

STUDY GUIDE:

Zscaler Digital Transformation Administrator (ZDTA) Certification

The logo consists of a dark blue rectangle with a lighter blue vertical bar on the left side. The text "Zscaler Digital Transformation Administrator" is written in white, sans-serif font on the dark blue background.

**Zscaler Digital
Transformation
Administrator**

Zscaler Digital Transformation Administrator	12
How to Use This Study Guide	12
About the ZDTA Exam	12
Exam Format	12
Audience & Qualifications	13
Skills Required	13
Recommended Training	13
Zero Trust Exchange (ZTE) Overview	14
The Need for Digital Transformation	14
The Need for a New Security Architecture	15
Why Legacy Security Models No Longer Work	16
The Flaws in Legacy Security Approaches	16
The Four-Step Attack Process in Legacy Security Models	16
The Need for Zero Trust Security	18
What is Zero Trust?	19
How Zero Trust Works in Practice	21
Private Application Access Without Public Exposure	21
Comparing Zero Trust to Legacy VPN Architectures	22
Secure Internet & SaaS Access (ZIA)	24
Zscaler Internet Access (ZIA): Secure and Reliable Connectivity	24
Secure Private App Access (ZPA)	26
Zscaler Private Access (ZPA): Secure and Seamless Private Application Access	26
How Private Access Works	26
Flexible Deployment Options	27
Why Organizations Choose ZPA	27
Who Uses Zscaler Services?	29
Network Operations (NetOps)	29
Security Operations (SecOps)	29
IT Operations & Administration	29
Executives & Business Leaders	29
Zscaler for Users Offerings	30
Zscaler for Users: Transforming Secure Access	30
Key Offerings of Zscaler for Users	30
Digital Experience Monitoring (ZDX)	31
Zscaler Digital Experience (ZDX): End-to-End Digital Experience Monitoring	31
What is End-to-End Digital Experience Monitoring?	31
Deep Insights for Cloud Applications & Collaboration Tools	31
Beyond Security: Full Visibility & Faster Troubleshooting	32
Core Skills	33
Identity Services	33
Identity Integration: Secure Authentication for the Zero Trust Exchange	33

Why Identity Integration Matters	33
Key Identity Integration Concepts	33
Connecting to an Identity Provider	35
SAML Authentication	36
What is SAML?	37
SAML Authentication Workflow	38
How SAML Authentication Works	38
Step-by-Step Authentication Process	38
Key Takeaways	39
SAML Authentication in Action	39
SCIM Authorization	40
What is SCIM	40
Resource Model and REST API Operations	42
Zscaler ZPA Support for SAML and SCIM	43
SCIM Capabilities	43
SCIM Data Management & Synchronization	44
Policy Considerations for SAML and SCIM Attributes	45
SAML Attribute Updates	45
SCIM Attribute Updates	45
Choosing Between SAML and SCIM for Policy Enforcement	45
SCIM Review	46
OpenID Connect (OIDC): Secure Authentication and Authorization	46
ZIdentity: Unified Identity Management for Zscaler Services	47
ZIdentity Admin Portal	47
Authentication Methods	47
Users, Groups, and Roles	47
User & Role Management	47
Administrative Roles	48
Service and Administrative Entitlements	48
Policies and Audit Logs	48
Admin Sign-On Policies	48
Audit Logs & Compliance	48
Key Benefits of ZIdentity	49
Connectivity Services	50
Connectivity Services Basics	51
Types of Tunnels in Secure Connectivity	51
Benefits of Tunneling	52
What is a PAC File?	53
How PAC Files Work	53
Types of PAC Files in Zscaler	53
1. Forwarding Profile PAC Files	53

2. App Profile PAC Files	53
How do System PAC files work?	54
How Traffic is Routed Using a PAC File	54
Optimizing Traffic Forwarding with Zscaler	54
The Role of PAC Files in Zscaler Security	55
Zscaler Client Connector	56
Zscaler Client Connector: Secure, Seamless Connectivity	56
Seamless User Experience	56
Key Features & Capabilities	57
Security & Compliance	57
Traffic Forwarding & Connectivity	57
Deployment & Management	57
User Navigation & Support	57
Why Zscaler Client Connector?	58
Traffic Forwarding Modes	58
Recommended Forwarding Mechanism: Zscaler Tunnel	58
Legacy & Alternative Forwarding Modes	59
ZIA Forwarding Profiles and Proxy Configuration	60
Trusted Network Detection and Forwarding Policy Decisions	61
Forwarding Policy Actions Based on Network Conditions	62
Connection Timeout and Fallback Behavior	62
System Proxy Settings and GPO Considerations	63
Summary: Forwarding PAC vs. Tunnel Mode	63
Application Profile	64
Key App Profile Features	64
Key Application Profile Configurations	65
Business Continuity & Supportability	66
Zscaler Client Connector Considerations	66
Client Connector ZIA Enrollment	67
Client Connector ZPA Enrollment	68
Client Connector Refresh Intervals	69
Device Posture and Posture Test	71
How Device Posture Enhances Zero Trust Security	71
Device Compatibility & Capabilities	72
Installing Zscaler Client Connector	73
Automating Installation Options for Zscaler Client Connector	76
Key Installation Parameters for Windows and macOS	76
Customization and Deployment Tools	78
Summary of Zscaler Client Connector	81
App Connectors	82
Connections to Private Access App Connectors	82

Provisioning Keys	83
Benefits of App Connector Provisioning Keys	83
Deploying App Connectors in Various Environments	84
Key Considerations for Deployment:	84
Best Practices for App Connector Deployment	84
Connectivity and Routing Requirements	85
Understanding App Connector IP Addressing	85
Impact on Active Directory and Network Policies	85
Example: Deploying App Connectors in a Zero Trust Architecture	86
Platform Services	90
Zscaler's Platform Services	91
Zscaler's Platform Services Suite	92
Device Posture	92
What is Device Posture?	92
Where to Access Device Posture in Zscaler?	92
Key Features of Device Posture in Zscaler	93
Device Posture for Enhanced Policy Access Control	94
BYOD vs. Corporate Devices	94
Key Components of Device Posture	94
Ensuring Device Security Before Access	95
SAML Response to Authentication: Strengthening Access Control	95
Understanding SAML Response Attributes	95
How Zscaler Uses SAML Responses	96
Trusted Networks: Strengthening Access Control	97
What Are Trusted Networks?	97
Defining Trusted Network Criteria with Zscaler Client Connector	97
Steps to Configure Trusted Networks in Zscaler Client Connector	98
Browser Access: Secure Application Access Without Client Installation	99
When to Use Browser Access	99
How Browser Access Enhances ZPA	99
TLS/SSL Inspection	101
Understanding TLS Inspection	101
SSL vs TLS: Understanding the Difference	103
Zscaler and TLS Decryption	104
Why is TLS Decryption Important?	104
The Growth of Encrypted Traffic & Threats	104
Zscaler ThreatLabz & Encrypted Threat Reports	105
TLS Inspection Pillars and Functionalities	105
TLS Inspection in the Zero Trust Exchange	106
SSL Inspection as a Forward Proxy in Zscaler Internet Access	107
SSL Inspection as a Reverse Proxy in Zscaler Private Access	108

How ZIA SSL Inspection Works	109
Conclusion: Why ZIA SSL Inspection Matters	112
A Five-Phase Approach to Deploying TLS Inspection	113
Conclusion	122
TLS Version and Cipher Visibility	123
Extended SSL Cipher Visibility	123
Policy Framework	124
What is the Policy Framework?	124
Policy Decisions & Enforcement	124
User Authentication and Policy Configuration in Zero Trust Exchange	125
Policy for Zscaler Internet Access	127
Policy Framework and Operational Flow in ZIA	127
Traffic Forwarding and Integration	129
Structured Rules and Criteria in Web Proxy Configuration	130
Bandwidth Control and Traffic Prioritization	131
Security Policy and Firewall Rules in ZIA	132
Policy Configuration and Actions in Network Address Translation (NAT) and Intrusion Prevention System (IPS)	134
Policy for Zscaler Private Access (ZPA) Policy Framework	136
Operational Flow & Policy Evaluation	136
Policy Criteria & Order of Operations	136
Types of ZPA Policies	137
Analyzing Access Policy Criteria for ZPA	138
Zscaler Digital Experience Policy	139
Access Control	141
Access Control Overview	143
The challenge of legacy firewalls	143
Why Legacy Firewalls Fall Short	143
The Risks of Legacy Firewall Architectures	143
How Zscaler Solves These Challenges	144
Zscaler's Access Control Services Suite	146
Cloud App Control, URL Filtering, and File Type Control	146
What is Cloud App Control and URL Filtering?	146
How Do They Work Together?	146
Why is URL Filtering Important?	147
Cloud App Control and URL Filtering Use-Cases	148
Advanced Use Cases	149
How is Zscaler Cloud App Control and URL Filtering Different?	150
Cloud App Control and URL Filtering Policies & Criteria	152
Granular Policy Criteria	152
Policy Actions	152

Visibility & Dashboards	153
Best Practices for Policy Configuration	153
File Type Control	155
Tenant Restriction	156
Bandwidth Control	157
Policing vs. Shaping: Key Differences	157
Configuring Bandwidth Control	159
Defining Bandwidth Classes	159
Creating Bandwidth Control Rules	159
Bandwidth Control Use-Cases	161
Prioritizing Productivity Apps	162
Limiting Bandwidth for Non-Productivity Apps	163
Enhancing Office 365 & Collaboration App Performance	164
Visibility & Reporting	165
Microsoft 365 (M365) Deployment with Zscaler	167
Challenges of Traditional Microsoft 365 Deployment	168
Microsoft 365 Network Connectivity Principles	169
Optimizing Microsoft 365 with Zscaler	171
M365 Deployment Best Practices	175
Traffic Forwarding and Secure Access	175
Optimizing Remote Work and Microsoft Teams	175
Enterprise Connectivity Principles	176
Addressing Regulatory and Compliance Needs	176
Teams Traffic Optimization for Inspected Deployments	176
Standard vs. Inspected Deployment Options	176
Review: Key Takeaways on Microsoft 365 Deployment with Zscaler	177
Challenges in Microsoft 365 Deployment	177
Microsoft 365 Connectivity Principles	178
Optimizing Microsoft 365 with Zscaler	178
Best Practices for M365 Deployment	178
Segmentation & Conditional Access through Policies	179
Private Application Access	179
Three Pillars of Secure Private Application Access	179
Modern Segmentation with Zero Trust	180
The Flaws of Legacy Segmentation	180
Zero Trust Segmentation with Zscaler	181
Three Core Segmentation Approaches	182
Application, Application Segment, and Segment Group	183
Application Segments and Segment Groups	183
Deploying App Connectors for Application Segments	183
Mapping App Connectors to Server Groups	183

Defining Application & Server Group Mapping	184
Access Policy for Application Segments	185
Application Discovery	185
Firewall	187
Zscaler Cloud Firewall	187
Key Features of Zscaler Cloud Firewall	187
Granular Firewall Policy Controls	188
FQDN-Based Firewall Rules & DNS Resolution	189
Network Services vs. Network Applications	189
Cloud Firewall Use-Cases	191
Cloud-Gen Firewall Best Practices	193
Key Benefits of Zscaler Cloud Firewall	194
Cyberthreat Protection Services	197
What is Cybersecurity?	197
Cybersecurity Overview	197
The Need for Cybersecurity	199
Understanding the Attack Surface	199
Stages of a Cyberattack Framework	200
Types of Cyberattacks	201
Holistic Approach to Stopping a Cyberattack	202
A Layered Approach to Threat Protection	203
Mapping to the Cyberattack Framework	204
Zscaler Delivers Comprehensive Cyber Threat Protection	205
What Sets Zscaler Apart in Cyber Threat Protection?	205
Zscaler's Cyber Security Services Suite	208
Malware Protection	208
What is Malware Protection?	208
Types of Malware	208
Malware Delivery Mechanisms	209
Zscaler Malware Protection & Configuration	210
Advanced Threat Protection	211
What is Advanced Threat Protection (ATP)?	211
How ATP Enhances Security	211
Handling ATP Security Exceptions	211
Understanding Command and Control (C2) Channels	212
How Command and Control Works in a Phishing Attack	212
Why Attackers Use Command and Control Channels	212
Common Tools Used for C2 Attacks	212
Zscaler Advanced Threat Protection (ATP)	213
Core Capabilities of Zscaler ATP	213
Threat Mitigation Techniques	213

Newly Registered & Observed Domains	214
Newly Revived Domains	215
Botnet Protection and AI-Powered Command & Control (C2) Detection	215
Dynamic Page Risk Analysis in Advanced Threat Protection	217
AI-Powered Phishing Detection	218
Blocking Malicious Content, Exploits, and Evasive Threats	219
An Early Warning System for Enterprises	220
Zscaler Cloud Sandbox: AI-Driven Malware Detection and Prevention	222
How Does Cloud Sandbox Work?	222
Driving Threat Intelligence for SOC Teams	222
Cloud-Powered Protection at Scale	222
Intrusion Prevention System (IPS): Cloud-Based Threat Protection	222
How Zscaler IPS Works	222
Key Benefits of Zscaler Cloud IPS	223
How Zscaler Deception Works: Proactive Threat Detection & Attack Disruption	223
Identity Threat Detection and Response (ITDR)	225
Overview of Zscaler ITDR	225
The Growing Threat of Identity-Based Attacks	225
Why ITDR is Critical for Organizations	225
Key Benefits of Zscaler ITDR	225
Private AppProtection Overview	227
Application Segmentation and Attack Surface Reduction	227
Virtual Patching and Custom Security Controls	227
Browser Isolation Overview	228
How Browser Isolation Works	228
Cybersecurity Use Case: File Protection	228
Detection & Response	229
Zscaler Detection & Response Overview	229
How Zscaler Enables Detection & Response	229
Detection & Response Workflow	229
Conclusion: Zscaler's Detection & Response Capability	231
Data Protection Services	231
Zscaler Data Protection: Ensuring Secure and Compliant Cloud Data	233
The Need for Data Protection in a Cloud-First World	233
Challenges with Traditional Data Protection Approaches	233
Key Use Cases for Zscaler Data Protection	234
AI-driven Auto Data Discovery and Classification	236
Shadow IT and Generative AI Security	236
Inline Data Discovery	236
Endpoint Data Discovery	236
Cloud Data Discovery	237

Secure Data in Motion	238
Securing Data in Motion with Inline Data Protection	238
Protecting Data from Generative AI (Gen AI) Risks	239
Zscaler's Inline Data Protection Capabilities	239
Critical Use Cases for Inline Data Protection	240
Content Inspection for Advanced Data Protection	241
File Type-Based Data Protection	241
Predefined & Custom Dictionaries for Content Inspection	242
Boolean Logic for Advanced DLP Policies	242
Exact Data Match (EDM) for Enterprise Data Protection	243
How EDM Works:	243
Securing SaaS Data	245
Reduce Risks with a SaaS Security Platform	246
Top Out-of-Band Use Cases	246
How SaaS Security Posture Management (SSPM) Works	247
Secure Cloud Data, Endpoint Data, and BYOD	250
Secure Cloud Data with DSPM	250
Secure Endpoint Data: A Streamlined Approach to Endpoint DLP	252
Comprehensive Data Loss Control	252
Key Benefits of Zscaler Endpoint DLP	252
Securing Unmanaged Devices (BYOD) with Browser Isolation	253
The Challenge with Traditional Approaches	253
How Browser Isolation Works	253
Ideal Use Cases	254
Risk Management	255
Understanding Risk Management in Cybersecurity	255
Types of Cybersecurity Risks	255
Zscaler Comprehensive Risk Management Suite	256
Zscaler Risk360: Advanced Cyber Risk Quantification & Management	256
Key Benefits of the Risk360 Platform	256
Vulnerability Management: A Critical Component of Cybersecurity	258
Key Characteristics of Vulnerability Management	258
Zscaler Data Fabric for Security	259
Key Capabilities of the Data Fabric for Security	259
Unified Vulnerability Management (UVM)	261
Key Capabilities of Unified Vulnerability Management	261
Enhancing Security Posture with Zscaler UVM	262
External Attack Surface Management (EASM)	263
How Zscaler EASM Enhances Security	263
Key Benefits of Zscaler EASM	263
Proactive Defense with Zscaler EASM	263

Deception: Proactive Threat Detection & Disruption	264
How Zscaler Deception Works	264
Deception Stages & Benefits	264
Zscaler Deception: A Game-Changer for Cyber Defense	265
ITDR: Identity Threat Detection & Response	266
Why ITDR is Crucial	266
Key Benefits of Zscaler ITDR	266
Enhancing Identity Security with Zscaler ITDR	267
Breach Predictor: Preemptive Detection and Response (PreDR)	268
Key Benefits of Zscaler Breach Predictor	268
Empowering Proactive Cyber Defense	268
Zscaler Digital Experience	269
Understanding ZDX: Enhancing Digital Experiences	269
Introduction to Zscaler Digital Experience (ZDX)	271
Challenges with Traditional Monitoring Approaches	271
How ZDX Solves These Challenges	272
ZDX Digital Experience Scoring	273
ZDX Dashboard and Telemetry Data	274
Deployment and Activation	275
ZDX deployment steps:	275
Advantages of deploying ZDX:	275
Why ZDX is the Best Choice for Digital Experience Monitoring	275
How the ZDX Score Works	276
ZDX Architecture Overview	279
Application Monitoring in ZDX	280
Cloud Path and Network Probing	281
Traceroute-Like Command Line View	283
ZDX Features and Functionality	286
Visibility into SaaS & Private Applications	287
UCaaS Monitoring	289
Software & Device Inventory	291
Automated Root Cause Analysis & API Integration	292
ZDX Use Cases	294
ZDX Dashboard Overview	303
Performance Overview and Filtering Options	303
Key Dashboard Metrics	304
Visualizing Performance Issues	304
Zscaler Zero Trust Automation	306
Introduction to APIs	306
RESTful API	306
How APIs Work	306

API Client	306
API Request Components	306
Zscaler APIs	307
Zscaler Internet Access (ZIA) API	307
Zscaler Digital Experience (ZDX) API	307
Zscaler Private Access (ZPA) API	307
Zscaler Cloud & Branch Connector API	307
Zscaler OneAPI	308
Before OneAPI : Zscaler Automation Framework	308
Zscaler Zero Trust Automation	309

Zscaler Digital Transformation Administrator

How to Use This Study Guide

Welcome to the Zscaler ZDTA Study Guide, which will serve as your go-to resource in preparing for the ZDTA exam and receiving your ZDTA certification.

About the ZDTA Exam

The Zscaler Digital Transformation Administrator (ZDTA) is a formal, third-party proctored certification exam that indicates that those who have achieved it possess the in-depth knowledge to design, install, configure, maintain, and troubleshoot most Zero Trust Exchange implementations.

Exam Format

Certification name: Zscaler Digital Transformation Administrator (ZDTA)

Delivered through: Online Proctored

Exam series: Zscaler Digital Transformation

Seat time: 90 minutes

Number of items: 60

Format: Multiple Choice

Languages: English or Japanese

Exam Domain	Weight (%)
Identity Services	4
Basic Connectivity	20
Platform Services	15
Zscaler Digital Experience	10
Access Control	15
Cyber Security Services	20
Basic Data Protection	16

Audience & Qualifications

The ZDTA exam is for Zscaler customers, partners as well as all who sell and support the Zscaler platform. By taking the exam, you are demonstrating your deep understanding and knowledge needed to sufficiently drive operational success.

Candidates should have a:

- Minimum of 5 years working in both IT networks and cybersecurity
- Minimum of 3-6 mo experience with the Zscaler platform.

Skills Required

- Ability to professionally operate, and troubleshoot the Zscaler platform
- Ability to adapt legacy on-premises technologies and legacy hub-and-spoke network designs to modern cloud architectures.

Recommended Training

Zscaler recommends that you have first attended the Zscaler for Users (EDU-200) Users-Administrator course and hands-on lab, or have solid hands-on experience with ZIdentity, ZIA, ZPA and ZDX.

Zero Trust Exchange (ZTE) Overview

The Need for Digital Transformation

In today's **hybrid working environment**, organizations must rethink how they **secure users, applications, and devices** across any network. As cyber threats grow in sophistication and the risk of **data loss** increases, businesses must adopt new security strategies that not only protect their digital assets but also deliver a **seamless user experience**.

Zscaler's **Zero Trust Architecture** leverages the world's **largest security cloud** to simplify and accelerate digital transformation. By securing **users, workloads, and IoT/OT devices**, Zscaler enables organizations to **operate securely, efficiently, and productively**, ensuring that security is never a barrier to business agility.



Secure your Users



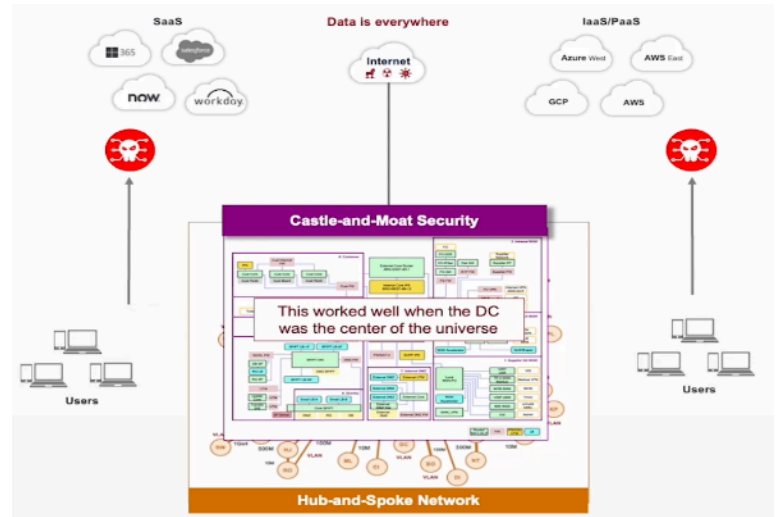
Secure your Workloads



Secure your IoT/OT

Why Legacy Security Models No Longer Work

Over the past decade, however, applications have moved to the **cloud**, and employees now work **remotely**—a trend accelerated by the **COVID-19 pandemic**. With users operating outside traditional network perimeters, organizations face an urgent need for **security transformation**. Every remote worker—whether in a **coffee shop, home office, or coworking space**—represents a **potential attack vector**. The challenge is clear: **how do you secure users when they are no longer inside the corporate network?**



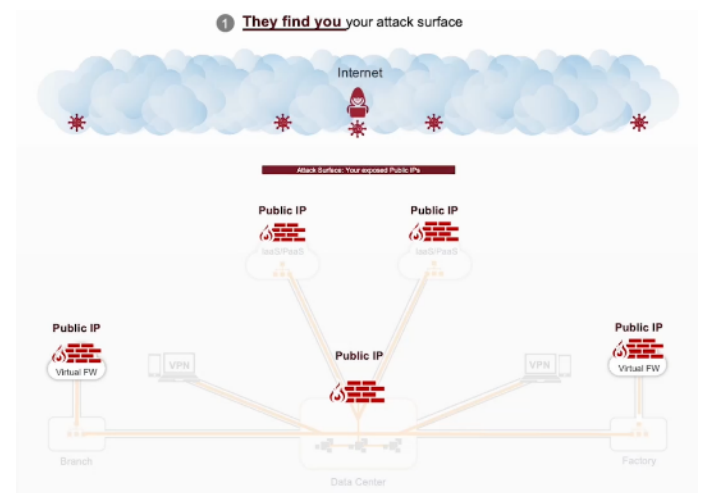
Traditional architectures rely on **routable networks**, extending **MPLS or private lines** between data centers and branch offices. When users started working remotely, companies simply extended these networks using **VPNs**. Now, with workloads shifting to **AWS, GCP, and Azure**, organizations are again extending their networks to **public cloud environments**—a practice that inadvertently creates more security risks.

The Flaws in Legacy Security Approaches

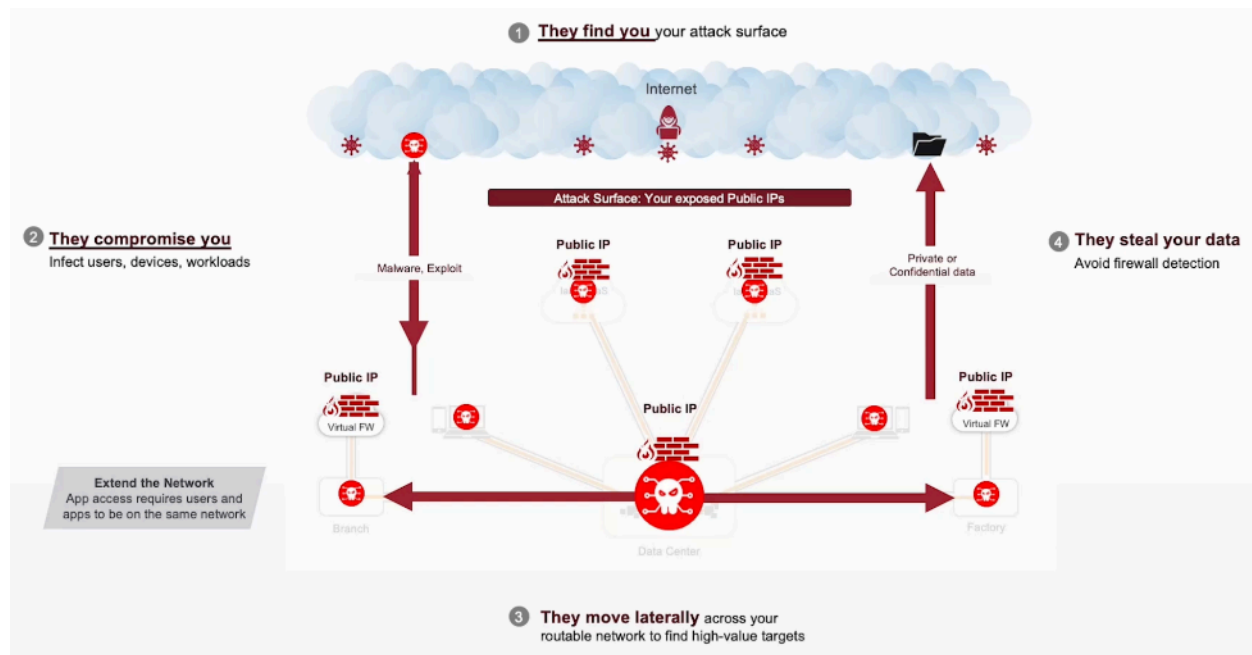
Legacy vendors often suggest deploying **virtual firewalls** in the cloud, but this approach is inherently flawed. **Virtual firewalls can be discovered, attacked, and subjected to DDoS (Distributed Denial-of-Service) attacks**, making them a weak link in security.

The Four-Step Attack Process in Legacy Security Models

Traditional security architectures expose businesses to a **four-step attack process** commonly exploited in major breaches like the **Colonial Pipeline attack**:



1. **They Find You** – Attackers scan the internet for vulnerable entry points, such as **exposed VPNs, misconfigured firewalls, or publicly accessible cloud workloads**. Any discoverable network presence increases the risk of an attack.
2. **They Compromise You** – Using **stolen credentials, phishing attacks, or unpatched vulnerabilities**, attackers infiltrate the network. A single set of compromised **VPN credentials** or an unprotected endpoint can provide them with the initial foothold they need.
3. **They Move Laterally** – Once inside, attackers navigate across the network, escalating privileges, bypassing security controls, and gaining access to **critical systems, databases, and applications**. Because traditional networks are **flat and routable**, attackers can freely explore without being detected.
4. **They Exfiltrate Your Data** – After identifying sensitive information, attackers extract **intellectual property, customer records, financial data, or trade secrets**, often using **encrypted channels** to evade detection. In some cases, they deploy **ransomware** or sell the stolen data on the **dark web**.



This attack lifecycle highlights the **critical flaws** in legacy security models. Without **Zero Trust principles**, organizations remain **exposed, easily discoverable, and susceptible to modern cyber threats**.

In traditional network architectures, a **single compromised VPN credential** grants attackers unrestricted access, allowing them to move laterally **undetected**. This **fundamental weakness** underscores why legacy security approaches are no longer sufficient in today's evolving threat landscape.

The Need for Zero Trust Security

Given these risks, organizations must shift away from **routable, discoverable networks** and embrace a **Zero Trust architecture**. Unlike traditional models, **Zero Trust eliminates the concept of implicit trust**—ensuring that users, devices, and applications are only granted access based on **strict identity verification and policy enforcement**.

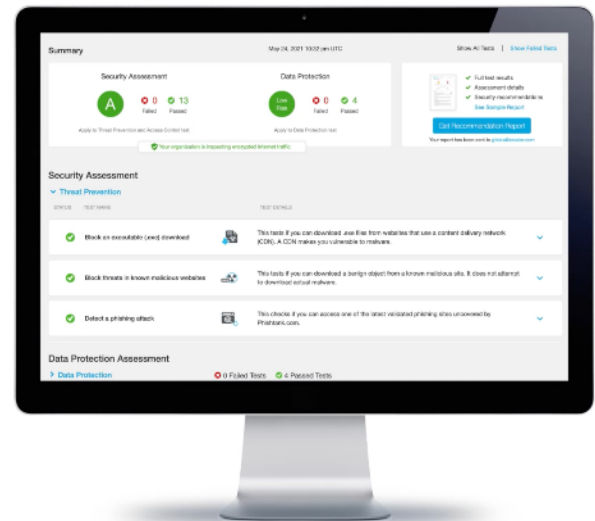
If you're wondering about **your organization's security posture**, visit **TestMyDefenses.com**. This tool helps assess whether your security controls can:

- ✓ Detect **known and unknown attacks**
- ✓ Prevent **data exfiltration**
- ✓ Block **source code leaks**
- ✓ Identify **zero-day exploits**

If you pass every test, you may be well-protected. However, if vulnerabilities exist, **Zscaler for Users** provides the **Zero Trust Exchange**—a modern security architecture designed to:

- **Eliminate VPN-based lateral movement**
- **Ensure secure, direct access to applications**
- **Block threats before they reach users or cloud workloads**
- **Protect against data exfiltration**

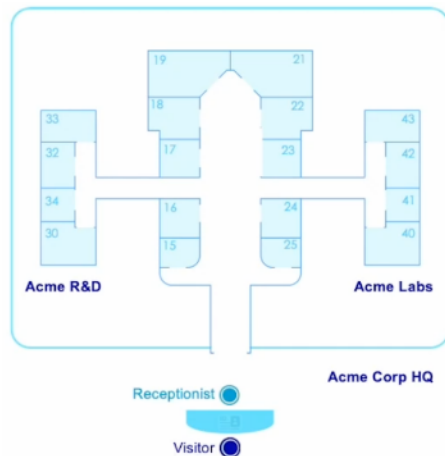
By adopting **Zscaler's Zero Trust Exchange**, organizations can **move beyond legacy security models**, enabling **fast, secure, and scalable digital transformation**.



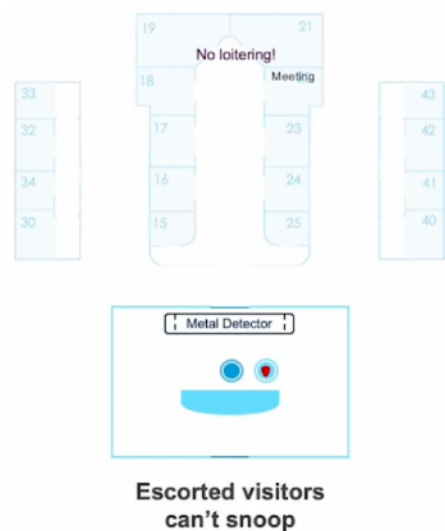
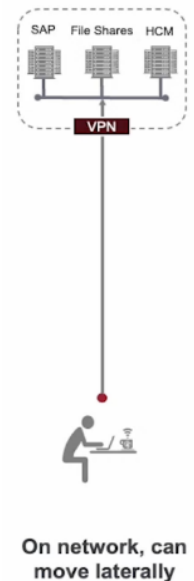
What is Zero Trust?

Zero Trust is about **connecting the right user to the right application**—not placing users on the network. To illustrate this, imagine visiting a corporate office.

Traditionally, when you arrive at a building, you see its **signage, entrances, and**

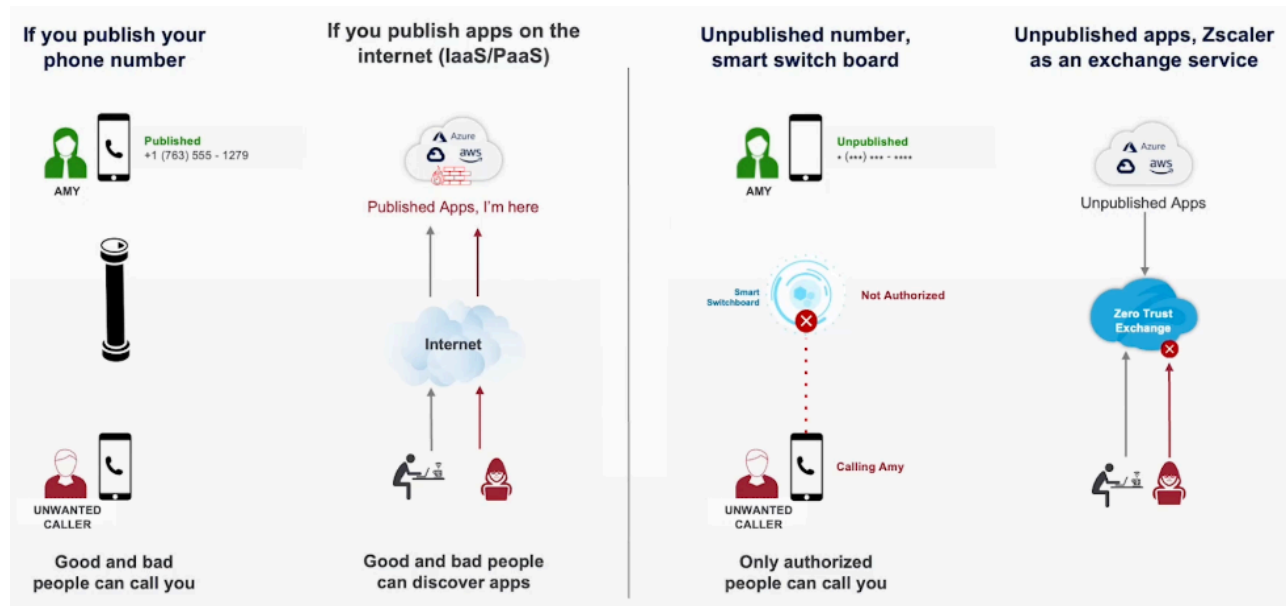


different wings—just like a public data center with AWS and Azure environments. The receptionist checks your ID (credentials and IP address), and once inside, you can **move freely**, explore different rooms, and even access sensitive information. This is akin to a **VPN-based security model**, where users are placed on the network and can conduct unauthorized activities, such as **scanning for vulnerabilities (Nmap scan), moving laterally, and exfiltrating sensitive data**.



With **Zscaler's Zero Trust Exchange**, access works differently. When you visit a building, you **can't see it**, and there's no visible sign or directory. A receptionist—acting as **Zscaler's security gateway**—validates your identity and **escorts you directly to your destination without exposing other areas**. You can only interact with the intended application, and **before exiting, security checks ensure that no sensitive data is exfiltrated**. This user-to-application model eliminates lateral movement and **prevents attackers from discovering and exploiting vulnerabilities**.

Another analogy involves **phone security**. Publishing your phone number in a public directory (the good old phone book) allows **anyone, including scammers, to call you**—just like a **public firewall makes your network discoverable and vulnerable**. In contrast, the **Zero Trust Exchange** functions as a **smart private switchboard**, ensuring that only **authorized contacts can connect**. Instead of broadcasting applications to the open internet, Zscaler ensures that only authenticated users **can request access based on predefined business policies**.



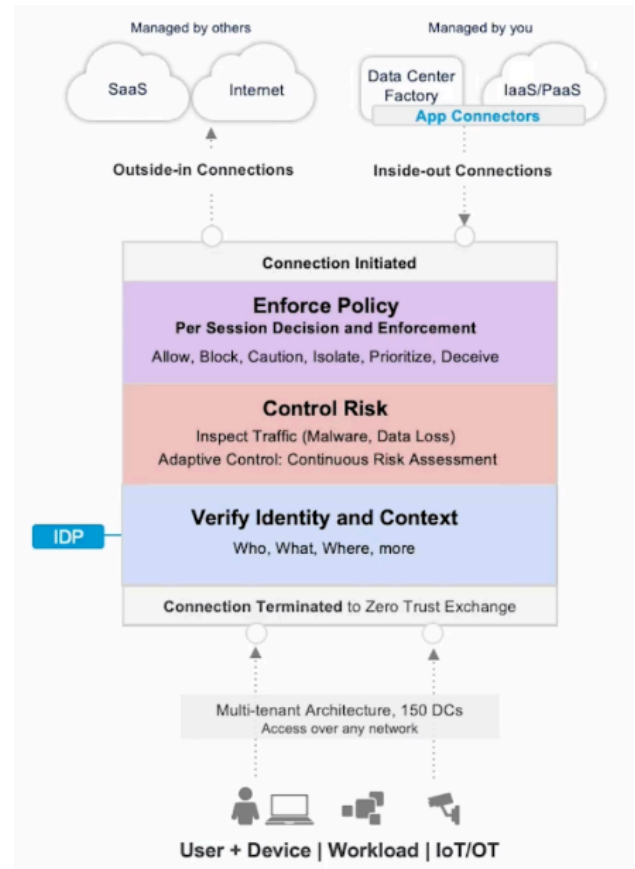
How Zero Trust Works in Practice

With **Zscaler's Zero Trust Exchange**, every request—whether from a **user, workload, or IoT/OT device**—is first **terminated at Zscaler**. At this stage, Zscaler evaluates the connection request by asking key questions:

- **Who is the user?**
- **Where are they connecting from?**
- **Where are they going?**
- **What is the context of the connection?**

Next, Zscaler **analyzes risk factors** by **inspecting SSL traffic** (since 90% of internet traffic is encrypted) and performing **data loss prevention (DLP) scans**. If the connection involves a sensitive private application, Zscaler enforces **data exfiltration controls**, ensuring that users cannot export confidential files.







Finally, based on security policies, Zscaler **decides whether to allow, block, or isolate the session**. If a **high-risk user** attempts to access a **sensitive application**, the session might be placed in **Cloud Browser Isolation**, allowing only **pixel rendering instead of full interaction**—preventing malware execution and data theft.



Private Application Access Without Public Exposure

For private applications, Zscaler deploys an **App Connector**, a lightweight virtual machine inside the organization's environment. Unlike traditional security models, which expose **public IP addresses**, the **App Connector establishes an inside-out connection only after the user's identity is fully validated**. This ensures that **applications remain invisible on the open internet**, eliminating the risk of direct attacks, such as **DDoS or credential stuffing**.

Comparing Zero Trust to Legacy VPN Architectures

<u>Zero Trust</u>	<u>Firewalls/VPN</u>
 Minimize Attack Surface No inbound connections, Apps Invisible	
 Prevent Lateral Movement Connect to apps, not networks	
 Prevent Compromise and Data Loss Proxy Architecture, SSL/TLS Inspection	

Unlike **VPNs and firewalls**, which extend **routable networks to remote users**, Zscaler follows a **true Zero Trust model**, granting **application-specific access without placing users on the network**. Traditional architectures rely on **pass-through security**, allowing threats to move freely and exposing **limited inspection buffers** that cannot fully analyze traffic or prevent data loss.

Example: Zero Trust Exchange in Action

Imagine you need to visit a high-security research facility. In a traditional security model (like a VPN), the facility's **building is visible**, its **entrances are clearly marked**, and **once you're inside, you can walk around freely**—even accessing areas beyond your intended destination. This unrestricted movement creates security risks, allowing **bad actors to explore, gather intelligence, and potentially steal sensitive data**.

Now, let's apply **Zscaler's Zero Trust Exchange** to the same scenario. Instead of a visible facility, the **building is completely hidden**—there's **no sign, no directory, and no way to locate it unless you're explicitly authorized**. When you request access, security **verifies your identity** before anything else. Rather than allowing you to roam the facility, a **designated escort (Zscaler) securely guides you directly to your specific meeting room**—without revealing the rest of the building.

Throughout your visit, security **continuously monitors your actions** to ensure compliance. Before you leave, an **exit screening checks for any unauthorized information or materials** to prevent data theft. This approach **eliminates the possibility of lateral movement**, ensuring that users can only access what they are explicitly authorized for—without exposing the broader environment.

This is the **fundamental difference** with **Zscaler's Zero Trust Exchange**—it **connects the right user to the right application without ever placing them on the network**. Unlike **legacy security architectures**, where attackers can infiltrate and explore freely, Zscaler ensures that **users can only access designated resources, remain invisible to unauthorized entities, and are continuously verified before, during, and after access**.

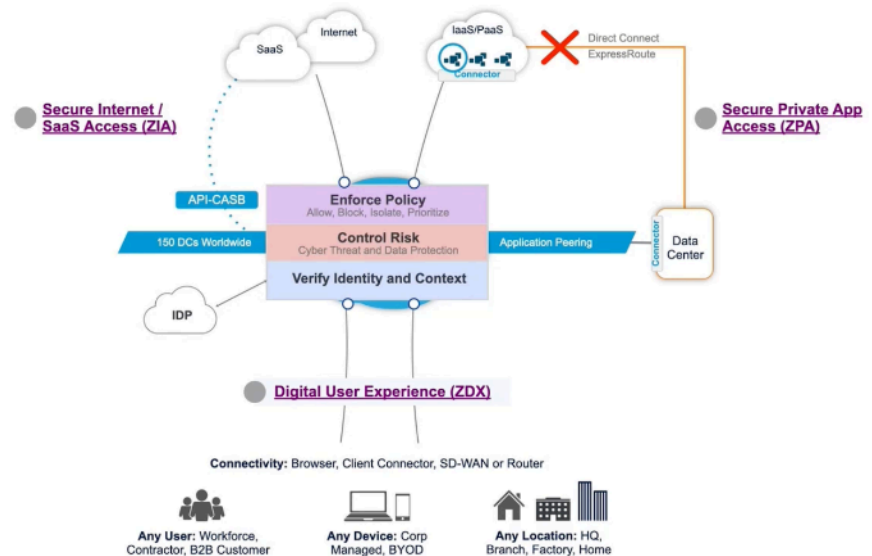
Organizations must **be cautious** when evaluating security vendors. Some claim to offer **Zero Trust** while still relying on **VPN-style access**, similar to comparing a **legacy gas-powered car** to an **electric vehicle**—both serve the same purpose, but one is fundamentally **more efficient, modern, and secure**. With Zscaler's **Zero Trust Exchange**, security is built **for the cloud era**, providing a **cleaner, more effective alternative to traditional network-based security models**.

Secure Internet & SaaS Access (ZIA)

Zscaler Internet Access (ZIA): Secure and Reliable Connectivity

Zscaler Internet Access (ZIA)

provides users with **fast, secure, and reliable** access to the internet and SaaS applications while ensuring protection against **advanced threats and data loss**. As a core component of **Zscaler for Users**, ZIA plays a foundational role in securing enterprise traffic by **inspecting, optimizing, and controlling** all internet-bound data. Since the majority of corporate traffic is directed to the public internet, securing this access is **essential** for maintaining a strong cybersecurity posture.



ZIA operates within the **Zscaler Zero**

Trust Exchange, where every **internet-bound connection** is **terminated, identity-verified, and risk-assessed** before access is granted. This process ensures that users securely connect to **internet and SaaS applications** without exposing the corporate network to external threats. By applying **Zero Trust principles**, ZIA eliminates the risk of lateral movement, reduces the attack surface, and ensures that security policies are consistently enforced across all users and locations.

Organizations adopt **ZIA** for three primary reasons. First, it delivers **best-in-class security** by leveraging AI/ML-driven **phishing and botnet detection, DNS security, and real-time traffic inspection** to detect and prevent cyber threats. Second, it provides **comprehensive data**

protection, securing **sensitive data in motion and at rest** with **100+ built-in data loss prevention (DLP) dictionaries** to enforce security policies effectively. Finally, ZIA enables **Zero Trust connectivity**, ensuring that **all sensitive traffic is routed through the Zero Trust Exchange**, where encrypted traffic is **inspected and controlled** to prevent unauthorized access and data exfiltration.

Reduces Cost and Complexity

Eliminates SWG, VPN Infrastructure, site-to-site VPNs



Immediate benefit

Secured 130,000 users in 6 weeks

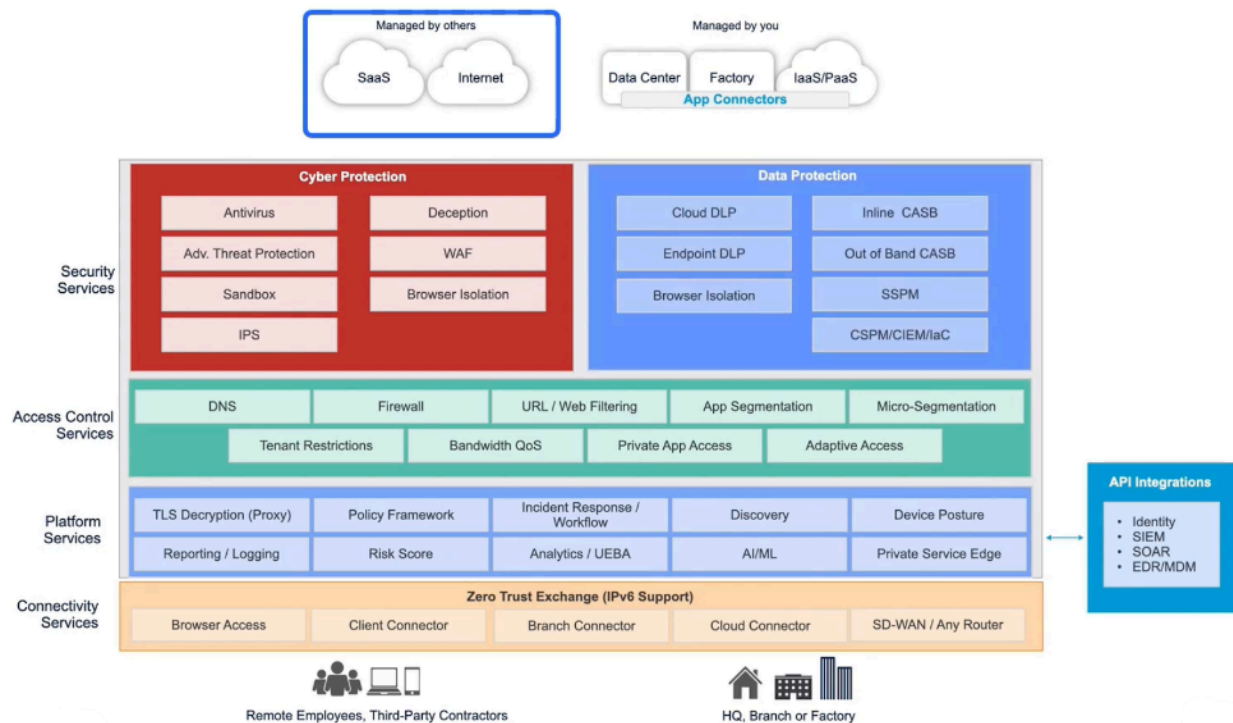
ZIA supports various **enterprise use cases**. It allows organizations to enforce

Zero Trust security for internet traffic, ensuring that all traffic is **fully inspected** for threats and compliance violations. It also enhances **UCaaS and SaaS performance** by enabling **local breakouts** for applications like **Microsoft 365 and Zoom**, reducing latency and improving the user experience. Additionally, **ZIA facilitates Zero Trust SD-WAN adoption**, allowing organizations to **replace legacy MPLS or private networks** while ensuring users can securely access the internet from **any location**, as if they were connected from a public network such as a **Starbucks Wi-Fi**. Furthermore, **ZIA secures workload-to-internet and IoT/OT-to-internet communications**, preventing unauthorized access and reducing attack surfaces across cloud environments and industrial systems.

By integrating **ZIA with the Zscaler Zero Trust Exchange**, organizations gain a **secure, scalable, and high-performance** model for **internet access**, ensuring seamless productivity without compromising security.

Secure Private App Access (ZPA)

Zscaler Private Access (ZPA): Secure and Seamless Private Application Access



Zscaler Private Access (ZPA) enables secure, seamless connectivity to **private applications, services, and OT devices** using the industry's only **next-generation Zero Trust Network Access (ZTNA) platform**. As part of **Zscaler for Users**, ZPA extends the **Zero Trust Exchange** to private application access, ensuring **secure, identity-based connections** without exposing applications to the public internet.

ZPA follows the same fundamental principles as **Zscaler Internet Access (ZIA)** but applies them in a private access context. Initially developed to secure internet access, Zscaler expanded its **Zero Trust capabilities** to **private applications**, recognizing that the same level of security and control was needed. Through **ZPA**, organizations can enforce **access control, security services, data protection policies, and digital experience monitoring** for private applications just as they do for internet-bound traffic.

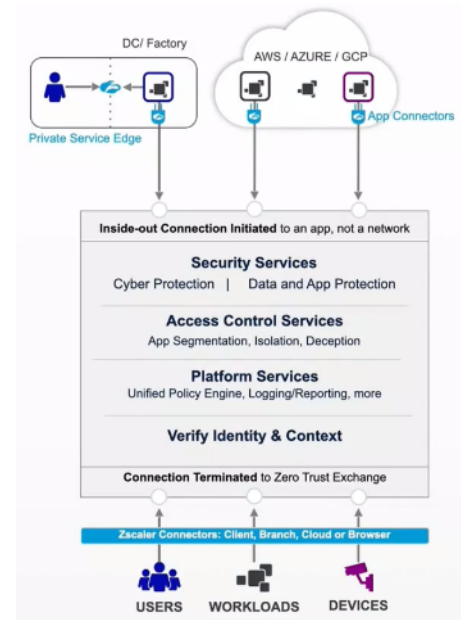
How Private Access Works

When a corporate user attempts to access a **private application**, ZPA **terminates the connection, verifies identity and context, and applies additional security controls** before establishing access. Unlike traditional VPNs, which **extend the corporate network** to remote users, ZPA creates an **inside-out connection** using an **App Connector**, ensuring that

applications remain **hidden from the open internet** and cannot be **discovered, attacked, or exploited**.

This **Zero Trust approach** provides a **more secure, flexible alternative** to legacy access solutions. By leveraging **ZPA**, organizations can:

- **Enable Zero Trust Application Access:** Users connect **directly to authorized applications** without being placed on the network, eliminating lateral movement risks.
- **Replace Legacy VPNs:** Many enterprises have replaced their **VPN appliances** with ZPA, reducing complexity, improving security, and simplifying remote access management.
- **Reduce Dependence on Virtual Desktop Infrastructures (VDI):** ZPA supports **remote desktop (RDP), SSH, and browser-based web applications**, allowing organizations to eliminate unnecessary **VDI deployments** while ensuring **secure remote access**.
- **Eliminate Public Exposure of Applications:** By deploying **App Connectors**, organizations can remove public IPs, preventing external attackers from discovering and targeting their private applications.



Flexible Deployment Options

ZPA can be deployed in **various environments**, including **on-premises data centers, private clouds, and edge locations**. Organizations that require **local processing** can implement **Private Service Edge**, which enables **Zero Trust private access without routing traffic through the public internet**. This ensures low-latency connections while maintaining **complete security and control** over private application access.

Additionally, **ZPA supports third-party users, contractors, and suppliers** who may require access to **corporate applications** from **unmanaged devices**. Instead of using traditional VPNs or direct network connections, ZPA **enforces the same security controls** for these external users, allowing **secure access to authorized applications** without **placing them on the network**.

Why Organizations Choose ZPA

Enterprises are adopting **ZPA** to **reduce risk, improve productivity, and lower costs** by eliminating the need for **multiple point products** like **VPNs, VDIs, and firewalls**. It enables

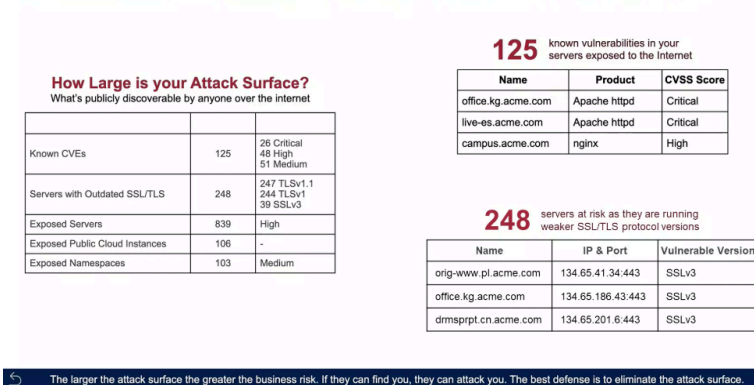
faster M&A integration, allowing newly acquired companies to **securely access applications** without complex **network integrations**.

ZPA also strengthens security by reducing the attack surface. Through **Zscaler's Attack Surface Reports**, organizations can **scan the open internet** to identify **publicly exposed servers**, **outdated SSL/TLS configurations**, and **known vulnerabilities (CVEs)**. By moving applications behind **ZPA**, businesses eliminate public IP addresses and make their applications **invisible to attackers**. This is critical in **mitigating zero-day threats**, as attackers start probing for vulnerabilities **within minutes** of a new exploit being discovered.

By **hiding private applications from the internet**, **ZPA ensures that organizations remain protected** even when zero-day vulnerabilities emerge, making **Zero Trust private access essential** for modern security architectures.

Example Attack Surface Exposure Assessment (Acme.com)

The tool only **queries public sources** for information. **No active traffic** is sent to your environment.



Who Uses Zscaler Services?

Zscaler's **comprehensive security and networking platform** is utilized by a wide range of professionals across various **IT, security, and business functions**. Here's a breakdown of the key roles that benefit from Zscaler's capabilities:

Network Operations (NetOps)

Professionals responsible for **network performance, reliability, and optimization** leverage Zscaler to ensure **secure, high-performance connectivity** across users, applications, and cloud environments.

- **Network Administrators** – Manage and maintain secure, scalable network infrastructure.
- **Network Analysts** – Monitor and analyze network traffic, ensuring optimal performance.
- **Network Engineers** – Design and implement network security and connectivity solutions.

Security Operations (SecOps)

Security professionals use Zscaler to **detect, prevent, and respond to cyber threats**, securing data, applications, and users.

- **Security Consultants** – Advise on security strategies and best practices.
- **Security Analysts** – Monitor security logs and investigate incidents.
- **Penetration Testers** – Assess vulnerabilities and test security defenses.
- **Threat Intelligence Analysts** – Analyze emerging threats and trends.
- **Threat Hunters** – Proactively identify and mitigate security threats.

IT Operations & Administration

IT teams depend on Zscaler for **secure digital transformation, system management, and user access control**.

- **IT Managers** – Oversee IT infrastructure and ensure compliance with security policies.
- **Systems Engineers** – Manage system configurations and integrations.
- **IT Architects** – Design secure, scalable IT environments.

Executives & Business Leaders

Business and technology leaders rely on Zscaler for **strategic security planning, compliance, and risk management**.

- **Chief Information Officers (CIOs)** – Drive digital transformation and cloud security strategies.

- **Chief Security Officers (CSOs)** – Oversee enterprise security and risk mitigation.
- **Compliance Officers** – Ensure regulatory compliance and governance policies are met.

By serving these diverse roles, **Zscaler empowers organizations to implement Zero Trust security, improve network performance, and enhance operational efficiency.**

Zscaler for Users Offerings

Zscaler for Users: Transforming Secure Access

Zscaler for Users provides a **comprehensive approach to securing corporate users** while optimizing network performance and **enabling seamless digital transformation**. By leveraging **Zscaler’s cloud-native architecture**, organizations can modernize the way **internet traffic flows to both SaaS and private applications**, ensuring security, visibility, and an enhanced user experience.

Key Offerings of Zscaler for Users

1. Secure Internet & SaaS Access

Zscaler Internet Access (ZIA) delivers **fast, secure, and reliable** internet and SaaS connectivity, ensuring that users are protected against **advanced threats and data loss** while maintaining high-performance access to cloud-based applications.

2. Secure Private Application Access

Zscaler Private Access (ZPA) provides **seamless, zero-trust connectivity** to private applications, services, and **OT devices**. As the industry’s **only next-gen Zero Trust Network Access (ZTNA) platform**, ZPA eliminates the need for **legacy VPNs**, reducing attack surfaces and ensuring **secure, direct access** without exposing applications to the open internet.

3. Digital Experience Monitoring

Zscaler Digital Experience (ZDX) empowers IT teams by **monitoring and optimizing** end-user digital experiences across applications, networks, and devices. By analyzing **performance metrics from the user’s perspective**, ZDX helps **quickly identify and resolve issues**, ensuring a consistently high-quality digital experience.

With **Zscaler for Users**, organizations can **enhance security, streamline access, and improve operational efficiency**—all while **enabling a seamless, high-performance digital workplace**.

Digital Experience Monitoring (ZDX)

Zscaler Digital Experience (ZDX): End-to-End Digital Experience Monitoring

Zscaler Digital Experience (ZDX) provides comprehensive **end-to-end digital experience monitoring** by analyzing performance from the **end user's perspective**. This ensures **optimized application, network, and device performance**, allowing IT teams to rapidly **identify and resolve issues** before they impact productivity.

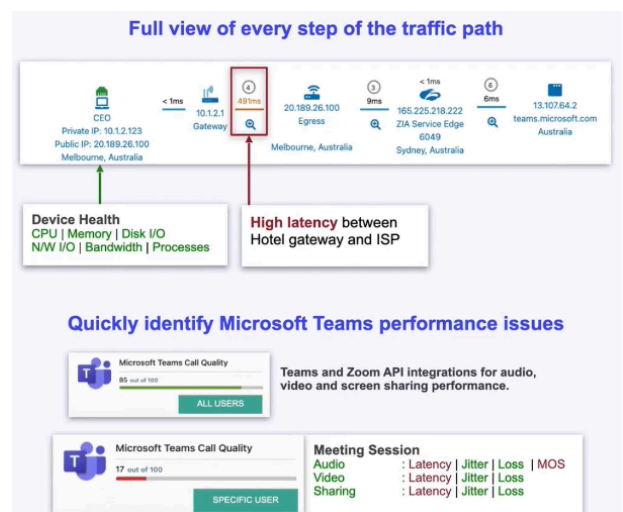
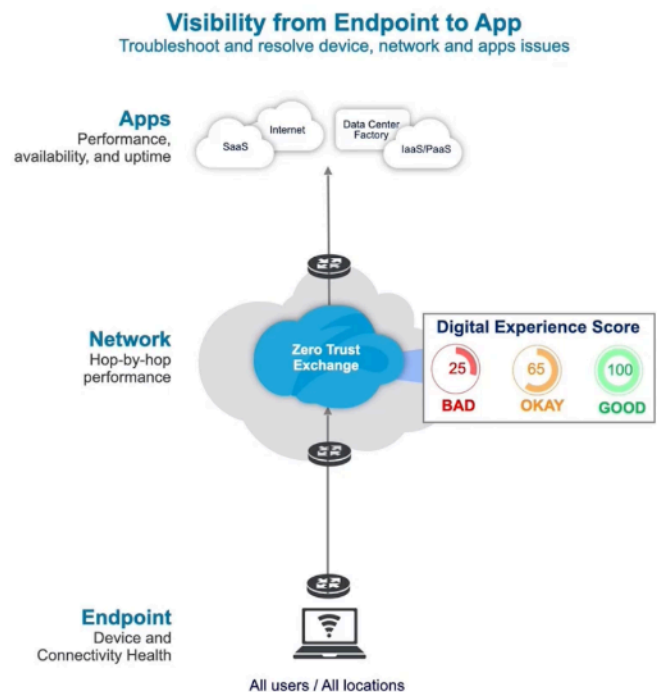
What is End-to-End Digital Experience Monitoring?

ZDX leverages the **Zscaler Client Connector** to provide **deep visibility** into network traffic, monitoring **everything from the user's device to the open internet**. With **150+ global points of presence** and **direct peering with major SaaS providers**, ZDX delivers **hop-by-hop visibility**, enabling IT teams to pinpoint performance issues at every layer, including:

- **Endpoint Issues:** Detect problems originating from the user's device.
- **Network Issues:** Identify latency, packet loss, or ISP-related disruptions.
- **Hop-Specific Problems:** Analyze where network bottlenecks occur.
- **Device Health:** Monitor CPU, memory, and overall system performance.
- **ISP and Gateway Issues:** Diagnose connectivity failures at the service provider or cloud gateway level.

Deep Insights for Cloud Applications & Collaboration Tools

ZDX also integrates with collaboration platforms like **Microsoft Teams and Zoom**, providing **granular meeting-level insights** into **audio and video quality**. IT teams can assess whether **performance issues** stem from the user's environment, network congestion, or external service disruptions.



Beyond Security: Full Visibility & Faster Troubleshooting

While Zscaler is known for **enhancing security, enabling direct-to-SaaS access, and preventing data loss**, **ZDX goes beyond** by offering **real-time visibility** into every aspect of digital performance. With **end-to-end diagnostics and actionable insights**, IT teams can:

- **Troubleshoot issues faster**
- **Diagnose root causes with precision**
- **Remediate problems proactively**

With **ZDX**, organizations gain a **powerful tool to optimize user experience, reduce downtime, and ensure seamless connectivity**—all within a **single, unified platform**.

Core Skills

Identity Services

Identity Integration: Secure Authentication for the Zero Trust Exchange

Understanding **identity integration** is essential for **authenticating users** to the **Zscaler Zero Trust Exchange (ZTE)** and ensuring that **user attributes are properly leveraged** for policy enforcement. This chapter will guide you through the fundamentals of **secure identity management** with Zscaler, helping you establish **trusted, seamless, and policy-driven access** for users.

Why Identity Integration Matters

In today's digital landscape, protecting **user identities** while ensuring **only authorized individuals access the right resources** is critical. Zscaler's **Identity Services** enable organizations to **securely manage user authentication and access** across cloud and private applications.

Key Identity Integration Concepts

1. Introduction to Identity Integration

- Learn how **Zscaler enhances secure connectivity** to both **internet and private applications** by integrating with **Identity Providers (IdPs)**.
- Understand how **dynamic access policies** are applied based on **user identity, device context, and real-time security posture**.

2. SAML Authentication

- Explore **Security Assertion Markup Language (SAML)** as a standard for verifying **user identities** across applications.
- Learn how **Single Sign-On (SSO) authentication** enhances security while providing a seamless access experience.

3. SCIM Authorization

- Understand **System for Cross-domain Identity Management (SCIM)**, a protocol designed to **automate user provisioning and ensure consistency** of identity information across multiple platforms.
- Learn how SCIM helps keep **user attributes up to date** and synchronized across identity and security ecosystems.

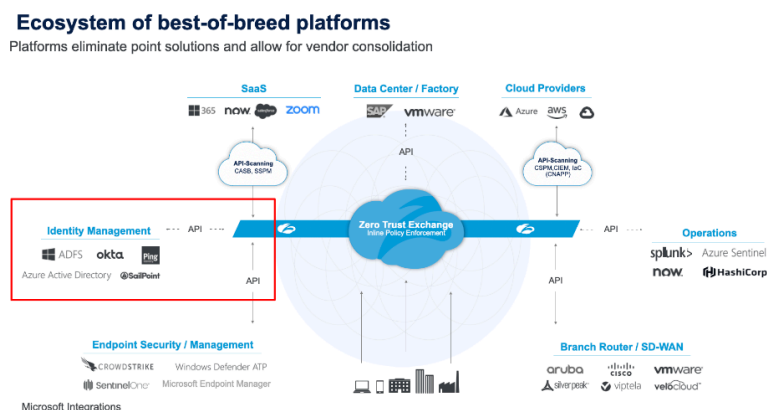
By the end of this chapter, you will be able to:

1. **Describe** the concepts of authentication and authorization
2. **Explain** the essentials of Security Assertion Markup Language (SAML) authentication, System for Cross-domain Identity Management (SCIM) authorization, and OpenID Connect (OIDC)
3. **Recognize** the importance of Identity Providers (IdPs) while connecting to the Zscaler Zero Trust Exchange
4. **Describe** ZIdentity
5. **Access** the ZIdentity landing page and admin portal
6. **Explain** the elements of the ZIdentity dashboard
7. **Add** ZIdentity Admin roles, users, user groups, user and session attributes, entitlements, and departments
8. **Assign** users and groups with administrative entitlement
9. **Describe** sign-on policies and audit logs

Connecting to an Identity Provider

Connecting to an Identity Provider is a fundamental step in securing access to the internet, SaaS applications, and private applications through Zscaler for Users. Before configuring identity integrations, it's essential to understand how Zscaler enables connectivity across different environments. Users can access applications either through **Direct Connect** or **ExpressRoute** at an Infrastructure as a Service (IaaS) provider or a private data center. Zscaler for Users facilitates secure access via a **browser or Zscaler Client Connector**, connecting users to the **Zero Trust Exchange** for verification, inspection, and policy enforcement.

When a user connects to the **Zero Trust Exchange**, the first step is identity and context verification. This process typically involves a **SAML-based identity provider**, although **LDAP or a hosted database** can also be used for Zscaler Internet Access (ZIA). Once user identity and context are established, Zscaler inspects the traffic, applies **data protection policies**, and enforces access controls such as **Allow, Block, Isolate, or Prioritize** based on user attributes and device posture. **Zscaler Internet Access (ZIA)** secures internet and SaaS applications, while **Zscaler Private Access (ZPA)** ensures seamless connectivity to private applications hosted in IaaS, PaaS, or private data centers. Additionally, **Zscaler Digital Experience (ZDX)** enhances visibility into user experience and device performance, helping IT teams diagnose and resolve performance issues.



The **Zero Trust Exchange** provides **connectivity services** specifically for Zscaler for Users, supporting browser-based access and **Zscaler Client Connector**, while also accommodating **Branch Connector, Cloud Connector, and SD-WAN connectivity**. Within the platform, Zscaler integrates with **identity providers (IdPs)** such as ADFS, Okta, PingOne, Auth0, OneLogin, and PingFederate, as well as **SIEM, SOAR, EDR, and MDM** solutions. Identity integration enables **SAML or LDAP authentication**, allowing security teams to apply policy based on **user identity, device posture, and session context**, while also generating access logs for reporting and compliance.

Once identity information is processed, **per-user and per-device access controls** can be enforced, including **URL filtering, application segmentation, tenant restrictions, and adaptive access** to private applications. Zscaler inspects content across the platform and applies **data protection policies** before routing traffic to public or private applications. Additionally, **ZDX** continuously monitors **network connectivity, latency, and application performance** to ensure a seamless user experience.

Zscaler integrates with multiple security partners to extend identity and access management capabilities. In the following sections, we will focus on **SAML and SCIM configurations** for **Zscaler Internet Access (ZIA)** and **Zscaler Private Access (ZPA)**, as well as the role of **CASB (Cloud Access Security Broker)**, **SSPM (SaaS Security Posture Management)**, and **CNAPP (Cloud-Native Application Protection Platform)** in securing SaaS applications. These integrations ensure that users gain **the right level of access under the right conditions**, reinforcing **Zero Trust security principles** across the enterprise.

SAML Authentication

After understanding Zscaler's approach to **identity integration** within the **Zero Trust Exchange**, let's explore **SAML (Security Assertion Markup Language)**—a critical protocol for enabling **secure, seamless access and identity federation** across applications and services.



Have you ever noticed how you can access multiple work applications without repeatedly entering your login credentials? This seamless experience is made possible by **SAML**, which ensures that **authentication and access control** work smoothly across different platforms. To understand how it functions, we need to explore its three key components and their roles in securing identity-based access.

What is SAML?

SAML (Security Assertion Markup Language) is a widely used protocol that allows different systems to communicate about **user authentication and authorization**. It acts as a **common language** between two entities—an **Identity Provider (IdP)** and a **Service Provider (SP)**—to securely verify users and grant access.

Think of SAML as having a **single key** that can unlock multiple doors instead of needing a separate key for each one. It works through three fundamental components:

1. **Service Provider (SP)**

The **Service Provider** is the application or service you are trying to access. It acts as a **gatekeeper**, ensuring that only authenticated users can enter. For example, **Zscaler Internet Access (ZIA)** or a corporate SaaS application like **Salesforce** or **Microsoft 365** would act as an SP. When a user attempts to log in, the **SP requests authentication** from the **IdP** to verify the user's identity.

2. **Identity Provider (IdP)**

The **Identity Provider** is responsible for verifying the user's identity and providing authentication. It acts as a **security checkpoint**, where users log in using credentials such as a **username, password, or multi-factor authentication (MFA)**. Examples of **IdPs** include **Okta, Ping Identity, Azure AD, and ADFS**. Once authentication is successful, the **IdP communicates with the SP** to confirm the user's identity.

3. **Security Assertion**

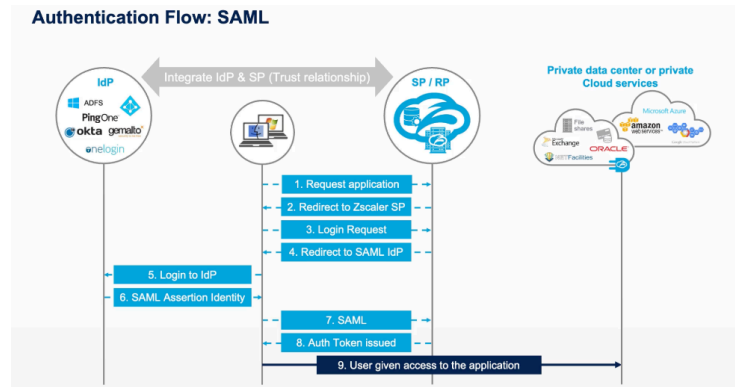
The **Security Assertion** serves as a **digital trust bridge** between the **SP and IdP**. Once authentication is completed, the **IdP generates a Security Assertion**—a secure token containing the user's attributes and permissions. The **SP verifies this assertion**, determines the level of access granted, and allows or denies entry based on the provided attributes.

Together, these components form the foundation of **SAML authentication**, enabling organizations to securely **manage user access across multiple applications without requiring repeated logins**. By implementing SAML, businesses ensure **efficient, scalable, and secure authentication**, reducing the risk of credential theft while **enhancing user experience**.

SAML Authentication Workflow

How SAML Authentication Works

SAML authentication operates through a structured process involving three key components: the **Identity Provider (IdP)**, the **user**, and the **Service Provider (SP)**—in this case, **Zscaler**. The applications users attempt to access could be **public SaaS applications** such as **Salesforce**, or **internal applications** secured through **Zscaler Private Access (ZPA)**.



Step-by-Step Authentication Process

- **User Requests an Application**

The authentication process begins when a user attempts to access an application. If they are **not yet authenticated**, they are **redirected to authenticate** at either **Zscaler Internet Access (ZIA)** or **Zscaler Private Access (ZPA)**.

- **SAML Authentication Request to Identity Provider**

Based on whether the application is public or private, Zscaler initiates a **SAML authentication request** to the **Identity Provider (IdP)**. This request informs the IdP that the user must authenticate and return a **SAML assertion** to validate the identity.

- **Identity Provider Challenges the User**

The **IdP verifies the request** and challenges the user to authenticate. The authentication method depends on the IdP's security policies and could involve:

- A **username and password**
- **Kerberos authentication**
- **Multi-Factor Authentication (MFA)**

Additionally, the **IdP can retrieve extra user attributes** and **group memberships**, embedding this information within the **SAML assertion**.

- **SAML Assertion Issued**

Once authentication is successful, the **IdP generates a SAML assertion**, **digitally signs it**, and **sends it back** to the **user's browser**. This assertion contains verified user details and is securely transmitted via an **automatic form POST using JavaScript**, ensuring a seamless experience.

- **Zscaler Validates the SAML Assertion**

Upon receiving the SAML assertion, **Zscaler verifies the digital signature** to confirm:

- The assertion is from a **trusted source**
- The data has **not been tampered with** during transmission

- **User Authentication Completion**

If the assertion is validated successfully, **Zscaler issues an authentication token** to the **Zscaler Client Connector** or a **cookie** to the user's browser, depending on the client type. The user is now **authenticated**, and their **application request is processed securely through the Zscaler Zero Trust Exchange**.

Key Takeaways

- **What initiates SAML authentication in Zscaler?**

The process begins when a user requests access to an application and is redirected to **authenticate through Zscaler Internet Access (ZIA) or Zscaler Private Access (ZPA)**.

- **What does the Identity Provider do after receiving the SAML request?**

The **IdP challenges the user to authenticate** based on its configured security policies (e.g., username and password, Kerberos, MFA). It may also **retrieve additional attributes** to include in the SAML assertion.

- **How does Zscaler handle a received SAML assertion?**

Zscaler **validates the digital signature** to ensure authenticity and integrity. Once verified, it **issues an authentication token** or a **cookie**, allowing the user to proceed with their request.

SAML Authentication in Action

- **Security & Convenience** – Enables **Single Sign-On (SSO)**, reducing the need for multiple logins while maintaining strong security controls.
- **Seamless Authentication** – Uses **SAML assertions** to securely **transmit authentication details** from the **IdP to Zscaler**, ensuring efficient access management.
- **Identity Federation** – Supports **federated identity management**, allowing users to authenticate once and securely access multiple applications.
- **Zero Trust Implementation** – Works alongside **Zscaler's Zero Trust Exchange**, ensuring that user access is dynamically authenticated and policy-enforced.

SCIM Authorization

Now that you have an understanding of SAML authentication and its workflow, let's take a look at the next identity integration, SCIM, which works to provide authorization and revoke access for disabled users.

What is SCIM

While **SAML** facilitates secure authentication and authorization by exchanging user identity data between **identity providers (IdPs)** and **service providers (SPs)**—enabling **Single Sign-On (SSO)**—**SCIM (System for Cross-domain Identity Management)** goes a step further. It provides a **standardized framework for managing user identities** across multiple systems, ensuring that **user attributes remain consistent and up-to-date**. SCIM automates the **provisioning, updating, and deprovisioning** of user accounts, reducing manual administrative work and minimizing security risks associated with outdated or incorrect user information.



How Does SCIM Work?

Consider **ZS Innovations**, a rapidly expanding company. As the company hires new employees, the **IT department** must create user accounts across various platforms, such as:

- **Email services** (e.g., Microsoft Office 365)
- **Customer Relationship Management (CRM) systems** (e.g., Salesforce)
- **Identity providers (IdPs) for Single Sign-On (SSO)**

With **SCIM**, user provisioning is automated. When a new employee joins, **SCIM-enabled identity providers** synchronize their user information across all relevant systems **in real time**, ensuring that employees have immediate access to the resources they need. Similarly, if an employee changes roles or leaves the company, SCIM ensures that **access permissions are updated or revoked automatically**, maintaining security and compliance.

Without SCIM



Without **SCIM**, the IT department must manually create and update user accounts across multiple systems. This process is **time-consuming, error-prone, and inefficient**, requiring repeated updates whenever an employee **joins, leaves, or changes roles** within the company. Manual management increases the risk of **inconsistent data, outdated permissions, and security vulnerabilities**, making it challenging to maintain accurate user access across all platforms.

With SCIM



When a new employee is added to the company's primary directory, **SCIM automates the provisioning process** by synchronizing user information across all connected systems, such as **Office 365, Salesforce, and the SSO provider**. This ensures that user accounts are **created, updated, or deactivated** consistently and efficiently, eliminating manual effort and reducing the risk of errors.

Resource Model and REST API Operations

There are two main components of SCIM: the **Resource Model** and **REST API operations**. These components provide a blueprint for how user and group information is structured and manipulated across different systems.

RESOURCE MODEL	REST API - OPERATIONS
<p>What is the Resource Model?</p> <p>The Resource Model is the framework that standardizes how user and group data is defined and organized, which is vital for consistent communication across various platforms.</p>	<p>What are REST API Operations?</p> <p>REST API Operations are the actions that can be performed using SCIM, such as adding, retrieving, modifying, or deleting user information, to keep systems in sync.</p>
<p>How the Resource Model Works</p> <p>When SCIM is enabled:</p> <ul style="list-style-type: none">• Standard Schema: It sets up a consistent framework for defining resources such as users and groups, ensuring that all systems understand the data in the same way.• Complex Types Support: The model accommodates a range of data complexities, from basic attributes to more detailed sub-attributes and multi-valued attributes, to address diverse organizational needs.• JSON Encoding: Information is encoded in JSON, making it easy to handle and exchange data across different web technologies.	<p>How REST API Operations Work</p> <p>With REST API, the following operations are essential for interacting with user and group resources within a SCIM-enabled system:</p> <ul style="list-style-type: none">• Create: Establish new user or group records.• Read: Access and retrieve details about existing resources.• Update: Modify attributes of users or groups as required.• Delete: Remove users or groups when they are no longer needed.• Search: Locate resources quickly based on specific criteria.• Bulk: Perform actions on multiple resources at once, streamlining management tasks.

Zscaler's ZPA supports both SAML and SCIM for multiple directories including the following:



Zscaler ZPA Support for SAML and SCIM

Zscaler Private Access (ZPA) supports both **SAML** and **SCIM** for seamless integration with multiple directories. This enables secure authentication and automated user management across various identity providers.

SCIM Capabilities

SCIM facilitates the **addition, deletion, and updating of users**, allowing organizations to apply policies based on **SCIM user or group attributes**.

For instance, when a user's access needs to be revoked—whether due to account deletion or deactivation in the directory—SCIM automates this process by:

- **Consuming** the updated user information
- **Automatically disabling** the user within Zscaler
- **Revoking access** across the platform

This ensures efficient and secure identity lifecycle management while reducing the need for manual intervention.

SCIM Data Management & Synchronization

SCIM ensures **consistent and secure identity management** by synchronizing user and group information across multiple systems. This process streamlines identity lifecycle management, automates updates, and reduces manual administrative overhead. Let's explore how SCIM facilitates seamless data synchronization and management across different platforms.

SCIM DATA MANAGEMENT	SCIM SYNCHRONIZATION
<p>What is SCIM Data Management?</p> <p>SCIM Data Management is the process that keeps user identity data synchronized and consistent. It's how we make sure that the information about users in your organization is the same everywhere it needs to be.</p>	<p>What is SCIM Synchronization?</p> <p>SCIM Synchronization is the mechanism that automatically updates user and group information across different systems to ensure everything is current and accurate.</p>
<p>How SCIM Data Management Works</p> <p>With SCIM enabled, the system generates protected, view-only lists within ZPA, comprising:</p> <ul style="list-style-type: none">• SCIM Users: A register of individual user identities within the organization.• SCIM Groups: Groupings that categorize users based on roles, departments, or access rights.• SCIM Attributes: Specific characteristics or data points associated with users and groups. <p>In this setup, users are managed centrally from the source directory or Identity Provider (IdP). Any additions or changes to users, groups, or attributes in this central location are then automatically synced and updated within ZPA. This mechanism ensures that user management is streamlined and that changes are reflected across all systems without delay.</p>	<p>How SCIM Synchronization Works</p> <p>This synchronization is a regular process that uses the API to refresh data:</p> <ul style="list-style-type: none">• Automatic Updates: The system is set to sync every approximately 40 minutes.• Manual Triggers: Administrators can initiate a sync at any time to immediately reflect any urgent changes.• Event-Driven Updates: Synchronization is prompted when specific events occur, such as:<ul style="list-style-type: none">○ A user is added to or removed from a group linked to the ZPA service.○ A user is directly assigned or unassigned from the ZPA service.○ A user is completely removed from the source directory.○ Changes are made to user attributes within the source directory.

Policy Considerations for SAML and SCIM Attributes

When determining policy based on **SAML and SCIM attributes**, it's essential to understand their differences and how they impact identity management and access control.

SAML Attribute Updates

SAML attributes are **received during authentication** and remain static until the user reauthenticates. To reflect updated SAML attributes, the user must **go through a new SAML authentication event**. These attributes are typically pulled from the identity provider (IdP), but they can also include contextual authentication details, such as the authentication method used or whether the user's device meets corporate security posture requirements.

SCIM Attribute Updates

Unlike SAML, **SCIM operates independently from authentication events** and enables **real-time or ongoing updates** of user attributes. If a user's group membership changes in the IdP, SCIM immediately synchronizes that change to Zscaler, whereas SAML would require the user to log in again for the update to take effect.

Choosing Between SAML and SCIM for Policy Enforcement

- **SAML Attributes**
 - SAML Attributes are static
 - Only applied on authentication
 - Only changed on re-authentication
 - Can include Device and Authentication attributes
- **SCIM Attributes**
 - SCIM Attributes are dynamic
 - User & Group specific
 - They will be updated after a change in the source directory
 - Frequency is IdP controlled
- **Both SAML and SCIM Attributes**
 - The best of both worlds

The screenshot shows the 'Edit IdP Configuration' window. It has a blue header with a close button. The main content area is white with various configuration sections. The 'Status' section has 'Enabled' selected. The 'ZPA (SP) SAML Request' section has 'Signed' selected. The 'HTTP-Redirect' section has 'Disabled' selected. The 'Single Sign-On' section has 'User' selected. The 'SAML Attributes for Policy' section has 'Enabled' selected and is highlighted with a blue box. The 'SCIM CONFIGURATION' section has 'SCIM Sync' set to 'Enabled' and 'SCIM Attributes for Policy' set to 'Enabled', both highlighted with blue boxes. The 'SCIM Service Provider Endpoint' is a URL. The 'Bearer Token' section has a 'Generate New Token' button. At the bottom are 'Save' and 'Cancel' buttons.

The choice between **SAML vs. SCIM** attributes for policy enforcement depends on the specific security requirements:

- **For group-based policies, SCIM** is preferable as it ensures continuous synchronization and immediate enforcement of changes.
- **For device trust-based policies, SAML** attributes should be used to see whether a user is accessing the system from a trusted or untrusted device.

SCIM Review

- **SCIM's Purpose:** SCIM extends beyond SAML by standardizing user identity management across multiple systems, ensuring **consistent and up-to-date user information**.
- **Automated Account Management:** SCIM automates the **creation, update, and deletion** of user accounts across platforms like email, CRM, and identity providers, reducing manual intervention and errors.
- **Core SCIM Components:** It includes a **Resource Model** for structuring user and group data and **REST API operations** for managing dynamic access rights.
- **Directory Integration and Policy Enforcement:** SCIM integrates with directories such as **Okta and Azure AD**, allowing **automated policy enforcement** based on changes in user attributes.
- **Data Management & Synchronization:** SCIM maintains a **single source of truth** for identity data, automatically synchronizing updates across all connected systems, minimizing inconsistencies, and ensuring security policies adapt to organizational changes.

By understanding the differences between SAML and SCIM attributes, organizations can **optimize their identity management strategy** and ensure the right level of security and access control for different user scenarios.

OpenID Connect (OIDC): Secure Authentication and Authorization

OpenID Connect (OIDC) is an **authentication protocol** built on the OAuth 2.0 framework, enabling **single sign-on (SSO)** and seamless identity verification across multiple applications. By allowing organizations to verify a user's identity and retrieve profile information, OIDC enhances security and user convenience.

Unlike traditional authentication methods, **OIDC does not store or transmit passwords**, reducing the risk of credential-based data breaches. Instead, it relies on secure token-based authentication, ensuring that users can access applications **without exposing their credentials**.

OIDC is often used alongside **OAuth 2.0**, an industry-standard authorization framework that enables users to **share access to their data with third-party applications** without sharing their login credentials. This approach is widely adopted across **technology platforms, social media services, and financial applications**, reinforcing **secure and scalable authentication** in modern digital environments.

ZIdentity: Unified Identity Management for Zscaler Services

ZIdentity is a **centralized identity service** designed to streamline **user authentication, identity management, and entitlement assignments** across Zscaler services, including **Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), and Zscaler Digital Experience (ZDX)**. By consolidating **identity data and role assignments** from multiple Zscaler platforms, **ZIdentity ensures seamless synchronization and consistency in access control**.

Administrators benefit from a **unified authentication experience**, allowing them to securely access all **Zscaler service admin portals** with a **single set of credentials**. This eliminates the need for multiple logins, improving **operational efficiency** while ensuring **secure access management**.

ZIdentity Admin Portal

The **ZIdentity Admin Portal** provides administrators with an intuitive interface to **configure ZIdentity accounts, manage user roles, and grant access** based on predefined permissions. Once set up, administrators can **send credentials to users**, enabling seamless and secure access to Zscaler services.

Authentication Methods

After configuring authentication preferences, users can sign in to the **ZIdentity Landing Page** using one of the following methods:

- **Password-based authentication**
- **Multi-Factor Authentication (MFA)**
- **Email One-Time Password (OTP)**
- **Security Key or Biometric Authentication**

MFA is enabled by default, ensuring enhanced security against unauthorized access. Users can authenticate using various **MFA options**, such as **SMS OTP, Google Authenticator (TOTP), or Fast Identity Online (FIDO) authentication**.

Users, Groups, and Roles

User & Role Management

- **User:** A unique account assigned to an individual.
- **User Group:** A logical collection of users with shared access needs, allowing for **efficient management of entitlements and permissions**.
- **Role:** Defines a user's **level of access and capabilities** within the system.

Administrative Roles

- **Admin Role:** Grants permissions to **manage specific areas**, such as **user accounts, policies, and configurations**.
- **Super Admin Role:** Provides **full control over the system**, including **managing admins, global settings, and high-level configurations**.

Service and Administrative Entitlements

Entitlements define the **level of access granted** to **Zidentity users**, ensuring they have the appropriate permissions within the system.

- **Service Entitlements:** Assigned to users who **require access to Zscaler services** but **do not need administrative capabilities**.
- **Administrative Entitlements:** Granted to users responsible for **managing administrative tasks**, such as **adding new admins, configuring policies, and overseeing user management**.

By using **user groups**, administrators can streamline **entitlement management** by **assigning multiple users** to specific Zscaler services based on **organizational requirements**.

Policies and Audit Logs

Admin Sign-On Policies

The **Admin Sign-On Policy** page provides an **overview of all configured sign-on rules**, defining whether **users are granted or denied access** to Zscaler services. These **policies help enforce security best practices and access control** based on predefined authentication conditions.

Audit Logs & Compliance

Audit logs maintain a **detailed record of user activities** within the **Zidentity Admin Portal**. They track **critical events**, including:

- **Configuration changes**
- **User management actions** (creating, updating, or deleting users)
- **Tenant management modifications**
- **Authentication setting adjustments**
- **Service assignment updates**

These logs provide **transparency and accountability**, ensuring **security teams can monitor access and detect anomalies efficiently**.

Key Benefits of ZIdentity

- **Seamless Single Sign-On (SSO):** Users can **access all subscribed Zscaler services** using a **single set of credentials**.
- **Stronger Security Controls: Enforced MFA** protects against **unauthorized access**.
- **Simplified Administration: Unified user and role management** through the **ZIdentity Admin Portal**.
- **Automated User Synchronization:** Supports **SAML Just-in-Time (JIT) provisioning** and **SCIM provisioning** for **automatic identity synchronization**.
- **IP-Based Admin Access Control:** **Restricts administrator access** based on **source IP addresses**.
- **Enhanced Visibility & Compliance:** **Audit logs track system activities**, ensuring **security transparency and regulatory compliance**.

By **centralizing identity management** and **strengthening authentication security**, **ZIdentity simplifies access, enhances security, and ensures seamless integration across Zscaler services**.

Connectivity Services

Understanding the various mechanisms available for **connecting to the Zero Trust Exchange (ZTE)** is essential for ensuring secure and efficient access. This chapter explores the different connection methods based on **use cases and locations**, providing insights into best practices for optimizing connectivity while maintaining security and performance.

By the end of this chapter, you will be able to:

1. **Identify** how Zscaler Zero Trust Exchange enforces secure connections across any network using Zscaler Client Connectors and App Connectors
2. **List** the key functionalities of the Zscaler Client Connector, including its role in forwarding traffic, verifying user and device identity, and managing secure connections within a Zero Trust architecture
3. **Describe** how Zscaler App Connectors securely connect users to applications through the Zero Trust Exchange
4. **Explain** the steps involved in the installation and enrollment of the Zscaler Client Connector to ensure seamless deployment

Connectivity Services Basics

Imagine a locked underground tunnel that only you have the key to—allowing you to send and receive data securely, away from prying eyes. This concept, known as **tunneling**, is a method used in networking to securely transfer data between networks without being detected.

Tunneling works by **encapsulating** your data inside a secure wrapper, protecting it from external threats. Data transmitted over a network is broken into smaller units called **packets**, each consisting of two parts: a **header**, which contains routing information, and a **payload**, which holds the actual data. In tunneling, the original data packet is wrapped inside another packet—a process known as **encapsulation**. This encapsulated packet moves through the network, appearing as normal traffic while remaining protected from interception.

When the packet reaches its destination, the outer layer is removed, and the **original data packet** is decrypted and delivered. This process of **encapsulation and decapsulation** ensures secure and private communication across networks, safeguarding data from unauthorized access and external threats.

Types of Tunnels in Secure Connectivity

Now that we've explored the basics of tunneling and how it secures data transmission, let's take a closer look at the different types of tunnels commonly used in network security. Each tunneling method has unique strengths in securely managing network traffic, and Zscaler leverages these methods to ensure seamless and protected connectivity. Understanding these tunneling mechanisms will help clarify their role in enhancing both security and efficiency.

HTTP Connect Tunnels: Securing Web Traffic

Think of **HTTP Connect tunnels** as dedicated pathways that securely route web traffic to its destination. They are commonly used to direct browsing activity through a proxy, ensuring that web requests reach the intended server while remaining protected. This method is particularly useful for organizations that require controlled and secure internet access for their users.

Secure Shell (SSH) Port Forwarding: A Secure Bridge

SSH tunnels create **encrypted pathways** between a client and a server over an unsecured network, such as the internet. For example, a remote worker might use an **SSH tunnel** to securely access files stored on their office computer from home without exposing sensitive data to external threats. This method is widely used for secure remote access and encrypted communication.

Generic Routing Encapsulation (GRE): A Flexible Data Tunnel

Developed by Cisco, **GRE** is a versatile tunneling protocol that allows different types of data—such as voice, video, or standard network traffic—to be encapsulated within a secure tunnel. Think of it as a **multipurpose conduit** that transports various types of

data across an IP network. Its flexibility makes it ideal for businesses needing scalable and adaptable solutions. **Internet Protocol Security (IPSec): A Locked Box for Data**

IPSec provides **end-to-end encryption** for data moving between two networks, ensuring that only authorized parties can access it. A common use case is securely connecting multiple office branches over the internet. With **IPSec tunnels**, data is encrypted and authenticated at each endpoint, preventing unauthorized interception and tampering.

DTLS/TLS Encrypted Tunnels: Real-Time Security for Communication

DTLS (Datagram Transport Layer Security) and TLS (Transport Layer Security) **encrypted tunnels** are designed for real-time data transmission, such as voice and video calls. These protocols ensure that data remains protected while minimizing latency, making them essential for applications where **speed and security** are equally important.

Zscaler Proprietary Microtunnels: A Specialized Secure Path

Zscaler's **proprietary microtunnels** are designed specifically for optimized security and efficiency within the **Zero Trust Exchange**. These microtunnels establish **dedicated, highly secure routes** for traffic within Zscaler's infrastructure, ensuring that data remains safe while moving through the cloud-based security framework.

By leveraging these tunneling methods, Zscaler provides organizations with **secure, high-performance connectivity**, safeguarding users and applications while maintaining flexibility in today's dynamic digital environment.

Benefits of Tunneling

Tunneling provides several key advantages in securing and optimizing network traffic, making it an essential technique for modern connectivity. Here are some of the primary benefits:

- **Easier Network Scaling** – Tunnels can be added or removed without disrupting existing connections or services, allowing networks to scale efficiently.
- **Enhanced Data Security** – Tunneling adds an extra layer of protection against interception and unauthorized access.
- **Supports Unsupported Protocols** – Some network hardware may not support certain protocols. Tunneling allows these protocols to function properly, ensuring compatibility with various applications.
- **Bypass ISP Firewalls** – In regions where certain services are blocked due to regulatory policies, tunneling can provide a way to bypass ISP restrictions and maintain connectivity.
- **Efficient Network Segmentation** – By separating different network segments, administrators can manage security policies and traffic more effectively without affecting overall network performance.
- **Secure VPN Creation** – Tunneling is a key component in establishing VPNs (Virtual Private Networks), enabling remote users to securely connect to internal resources over

public or private networks.

- **Reduced Latency & Improved Speed** – Certain tunneling protocols, such as **GRE** and **IPSec**, optimize data transmission by reducing unnecessary overhead, leading to lower latency and improved network performance.

By leveraging these tunneling benefits, organizations can **enhance security, improve network efficiency, and maintain seamless connectivity across multiple environments**.

What is a PAC File?

A **PAC (Proxy Auto-Configuration) file** is a **text file** that contains **JavaScript code** designed to guide web browsers and applications on how to route internet traffic. Its primary function is to determine whether web requests should be sent **directly to the destination server** or **through a proxy server** based on predefined rules.

How PAC Files Work

PAC files evaluate network conditions and apply routing rules based on specific criteria, such as:

- **Time of day** – Direct or route traffic differently based on working hours.
- **Day of the week** – Customize proxy usage for weekdays versus weekends.
- **Specific URLs** – Route selected websites through a proxy while allowing others to bypass it.
- **Domain names** – Apply different routing rules for corporate and public domains.

Types of PAC Files in Zscaler

PAC files are primarily written in **JavaScript** and are interpreted by web browsers and proxy-aware applications, used to define **when and how** traffic should be forwarded through Zscaler. However, in a **Zscaler environment**, there are two specific types:

1. **Forwarding Profile PAC Files**

- Processed by **browsers** and other **proxy-aware applications**.

2. **App Profile PAC Files**

- Not processed by browsers.
- Used exclusively for **forwarding traffic through Zscaler Client Connector**.
- The **Zscaler Client Connector** interprets these files but does not support the full syntax of browser-based PAC files.

By leveraging PAC files, organizations can efficiently manage **traffic routing, optimize performance, enforce security policies, and control access to specific resources** based on dynamic conditions.

How do System PAC files work?

Browsers only need the **URL of a PAC file** to fetch and execute the **JavaScript-based rules** within it. PAC files can be hosted on a **local workstation, an internal web server, or an external server** beyond the corporate network. The **Zscaler service** provides a **default PAC file** that leverages **geolocation technology** to direct traffic to the **nearest Internet & SaaS Public Service Edge**. Additionally, organizations can **upload custom PAC files** to the Zscaler platform for **greater control over traffic routing**.

How Traffic is Routed Using a PAC File

When a user opens a browser, the following sequence occurs:

1. **Fetching the PAC File:**
 - The browser is **pre-configured** with the URL of the **Zscaler default PAC file**.
 - Upon startup, the browser **requests** the PAC file from the Zscaler service.
2. **Determining the Nearest Service Edge:**
 - The Zscaler platform uses **geolocation technology** to identify the closest **Service Edges**.
 - The **Service Edge IP addresses** are dynamically inserted into the PAC file.
3. **Executing the PAC File Instructions:**
 - The browser **processes the PAC file** and follows its routing instructions.
 - Web traffic is forwarded to the **primary Service Edge** for security inspection and policy enforcement.

Because **the browser itself** is responsible for retrieving and applying the PAC file, web traffic is consistently routed through **Zscaler's security infrastructure, regardless of the user's network location**.

Optimizing Traffic Forwarding with Zscaler

For **optimal security and seamless user experience**, Zscaler recommends using a combination of:

- **Tunneling protocols** (e.g., GRE, IPsec, or Z-Tunnel)
- **PAC files** for browser-based traffic routing
- **Surrogate IP** for consistent user identification
- **Zscaler Client Connector** – a lightweight endpoint agent that securely directs traffic to Zscaler from any network

The Role of PAC Files in Zscaler Security

PAC files serve as a **key integration point** for **Zscaler's security services**, ensuring that:

- **Web traffic is routed efficiently and securely**
- **Corporate policies are enforced** for all users
- **Security inspection and filtering** apply regardless of the user's location

By leveraging **PAC files within the Zscaler platform**, organizations can achieve **secure, policy-compliant web access** while optimizing performance and user experience.

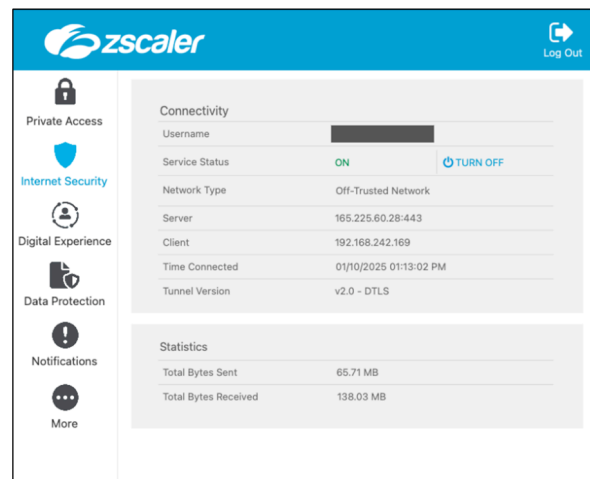
Zscaler Client Connector

Zscaler Client Connector: Secure, Seamless Connectivity

Zscaler Client Connector is a **lightweight application** installed on user devices to ensure secure and policy-compliant access to the internet and internal applications, even when users are off the corporate network. It automatically forwards all traffic through **Zscaler Internet Access (ZIA)** for secure browsing and SaaS access, **Zscaler Private Access (ZPA)** for seamless connection to private applications, and **Zscaler Digital Experience (ZDX)** for monitoring and troubleshooting performance issues. Additionally, **Zscaler Endpoint Data Loss Prevention (DLP)** safeguards sensitive data at the device level.

Zscaler Client Connector

- Lightweight client installed on user devices used for enforcement of security policies and steers traffic to the Zero Trust Exchange
- Single client for secure access to Internet and Private Applications, endpoint DLP, User Experience monitoring and Active Defense
- Supported on all major platforms – Windows, macOS, Linux, iOS, Android and ChromeOS on Android
- Integrates with all market leading MDM and UEM platforms for rapid deployment
- Provides user identity and device context to the Zero Trust Exchange for ubiquitous enforcement of policies regardless of location



Seamless User Experience

Zscaler Client Connector ensures a **seamless user experience** by intelligently adapting to network conditions. It features **automatic network detection**, which recognizes whether a user is on a trusted or untrusted network and dynamically enables or disables **ZIA, ZPA, ZDX, and DLP** accordingly. Additionally, it includes **captive portal handling**, which detects Wi-Fi networks that require payment or policy acceptance before granting access. In such cases, the Client Connector temporarily disables its services until the user successfully connects, then re-enables them automatically. The **effortless setup** further simplifies user onboarding—users log in once, complete a **one-step device enrollment**, and instantly gain **secure access** to corporate resources without manual configurations or interruptions.

Key Features & Capabilities

Security & Compliance

- **Authentication Support:** Works with **SAML-based authentication**, two-factor authentication, and existing user credentials (excludes Kerberos). ZPA requires SAML authentication.
- **Strict Policy Enforcement:** Prevents users from **logging out, disabling, or uninstalling** the app without an admin password.
- **SSL Inspection:** Automatically installs **Zscaler SSL certificates** for encrypted traffic inspection, ensuring compliance with security policies.

Traffic Forwarding & Connectivity

- **Trusted Network Detection:** Disables internet security services when connected to a corporate network, ensuring seamless traffic routing through existing security mechanisms.
- **Captive Portal Detection:** Temporarily pauses security enforcement on public Wi-Fi networks requiring login or payment before re-enabling services.
- **Zero Trust Private Access:** Eliminates the need for VPNs, providing **secure application access** without placing users on the corporate network.

Deployment & Management

- **Frictionless Deployment:** Supports modern **MDM/UEM solutions** (e.g., JAMF, SCCM) and allows **auto-updates** to keep client versions up to date.
- **Centralized Administration:** Managed via the **Zscaler Client Connector Portal**, where admins can configure policies, enforce security settings, and monitor updates.
- **3rd Party Integrations:** Works with **endpoint security solutions** like **CrowdStrike, Microsoft Defender, and VMware Carbon Black** for **context-aware security policies**.

User Navigation & Support

- **Intuitive Dashboard:** Users can view **connection status, security settings, and performance analytics** via dedicated ZIA, ZPA, and ZDX tabs.
- **Built-In Support Access:** Users can access support tools to assist their IT team or **Zscaler Support** from within the app.
- **Multi-Language Support:** The app **adapts to system language settings**, ensuring a **localized user experience**.

Why Zscaler Client Connector?

Zscaler Client Connector **simplifies and secures remote work** by ensuring **continuous security enforcement, seamless connectivity, and proactive monitoring** across all networks. Whether users are **working remotely, accessing SaaS applications, or connecting to private corporate resources**, Zscaler Client Connector **protects data, enhances user experience, and enforces security policies without disruption**.

Traffic Forwarding Modes

Zscaler Client Connector provides multiple **traffic forwarding mechanisms** to securely route user traffic through **Zscaler Internet Access (ZIA)**. These modes ensure authenticated, policy-enforced traffic forwarding, enhancing security and performance.

Recommended Forwarding Mechanism: Zscaler Tunnel

The **Zscaler Tunnel** is the **preferred** forwarding method, as it securely captures and encapsulates traffic at the network level before directing it through an encrypted tunnel to Zscaler's cloud security platform. This tunnel-based approach supports different methods:

1. Packet Filter-Based Tunneling (Windows Packet Filter)

- Captures and redirects network traffic at the packet level.
- Forwards traffic securely to Zscaler after policy validation.

2. Route-Based Mode

- Uses an additional **network adapter** to control traffic routing.
- Ensures **application-generated traffic** follows a defined security path.

3. Tunnel with Local Proxy

- Establishes a **loopback address** as an HTTP/HTTPS proxy.
- Configures system proxy settings to route browser and application traffic securely through **Zscaler cloud** via the local proxy.

All three of these methods establish **authenticated tunnels**, meaning that once a user is enrolled in Zscaler Client Connector, the tunnel is securely linked to their identity, ensuring that **user-based policies** are consistently applied.

ZIA : Forwarding Modes

Z-Tunnel – Packet Filter Based	Creates Packet Filters (Windows)	} Authenticated Tunnels
Z-Tunnel – Route Based	Creates Route Table Entries	
Tunnel with Local Proxy	Deploys System Proxy To Localhost	
Enforce PAC	No Client Connector forwarding (browser based auth), similar to GPO	
None	Client Connector is completely disabled (system settings only)	

Legacy & Alternative Forwarding Modes

For compatibility with older implementations, Zscaler Client Connector also supports additional forwarding options:

1. Enforced PAC Mode

- Implements a **PAC (Proxy Auto-Configuration) file** within the browser.
- Similar to **Group Policy Object (GPO)-based** configurations.
- Directs browser traffic through **Zscaler Internet Access (ZIA)** or legacy proxy servers.

2. None (No Configuration)

- Disables all forwarding mechanisms within **Zscaler Client Connector**.
- Relies on **existing browser settings or corporate proxy configurations** (e.g., GPO-defined settings).

Summary

By leveraging the right forwarding mode, **Zscaler Client Connector** ensures that user traffic is securely routed through **Zscaler's Zero Trust Exchange**, providing **seamless security, better policy enforcement, and optimized network performance**. While the **Zscaler Tunnel** is the preferred approach, organizations can select the forwarding mode that best suits their **security policies and deployment requirements**.

ZIA Forwarding Profiles and Proxy Configuration

Zscaler Client Connector supports multiple **tunnel modes** to forward traffic securely to **Zscaler Internet Access (ZIA)**. The **legacy Z-Tunnel 1.0** was limited to **HTTP CONNECT** traffic, while the **advanced Z-Tunnel 2.0** supports **multiple protocols** for enhanced inspection and security. Migrating to **Z-Tunnel 2.0** consolidates traffic into a single channel, enabling **real-time updates, notifications, and better security**.

ZIA: Forwarding Modes

Z- Tunnel 2.0	Z-Tunnel 1.0	Tunnel With Local Proxy	Enforce PAC	None
<ul style="list-style-type: none">• Secures ALL IP unicast traffic• Better protection and policy enforcement• Tunnel authentication, validation and integrity• Flexible include/exclude options• Real-time control channel• Excellent end user visibility• Uses Packet Filter (Windows) or Route based methods to intercept traffic locally• Supports Seamless SSO	<ul style="list-style-type: none">• Secures TCP 80/443 traffic• Utilizes lightweight HTTP CONNECT tunnels• Uses authenticated tunnels• Flexible include/exclude options• End user visibility to TCP 80/443 traffic only• Uses Packet Filter (Windows) or Route based methods to intercept traffic locally• Supports Seamless SSO	<ul style="list-style-type: none">• Secure ALL HTTP/HTTPS traffic (also on non-standard ports)• Utilizes lightweight HTTP CONNECT tunnels• Uses authenticated tunnels• Flexible include/exclude options• End user visibility to web traffic on any port from proxy aware apps• Uses a system proxy on localhost to intercept traffic• Supports Seamless SSO	<ul style="list-style-type: none">• Lightweight Proxy only solution• Proxy settings on OS enforced by Client Connector• Client Connector doesn't intercept and forward traffic• Traffic is forwarded based on installed system PAC• End user visibility to web traffic only• Supports browser based authentication only• No support for Postures, eDLP and MFA	<ul style="list-style-type: none">• No Client Connector based forwarding

Trusted Network Detection and Forwarding Policy Decisions

The **Zscaler Client Connector** automatically detects whether a device is on a **trusted** or **untrusted** network based on predefined **network criteria**. This detection allows administrators to enforce appropriate forwarding policies.

The following parameters determine trusted network identification:

- **Hostname & IP Matching** – Checks if a fully qualified domain name (FQDN) resolves to a specific IP.
- **DNS Server Detection** – Verifies if the primary DNS server matches the corporate configuration.
- **DNS Search Domain** – Confirms if the DHCP-assigned search domain matches what would be provided by the corporate DHCP server..
- **Network Range** – Matches the client's subnet with predefined trusted networks.
- **Default Gateway** – Identifies if the device's default gateway belongs to a corporate network.
- **DHCP Server** – Matches the assigned DHCP server IP to corporate infrastructure.
- **Egress IP Address** – Recognizes the public IP address used to access the internet.

The image shows a configuration interface for 'TRUSTED NETWORK CRITERIA'. It includes a section for 'Add Condition' with a dropdown menu showing 'Hostname and IP' and 'Pre-defined Trusted Networks'. Below this, there are fields for 'DNS Servers' (192.168.1.1) and 'DNS Search Domains' (localdomain). An 'Add Trusted Network' dialog box is open, showing a 'NETWORK DEFINITION' section with a 'Network Name' field and a 'TRUSTED NETWORK CRITERIA' section with a dropdown menu showing 'DNS Server', 'DNS Search Domains', and 'Hostname and IP'.

By combining these conditions, administrators can define **multiple trusted networks** (e.g., for data centers, branch offices, or specific locations). These trusted networks dictate **forwarding mode configurations**, ensuring that traffic is handled based on **network context**.

Forwarding Policy Actions Based on Network Conditions

Within the **ZIA Forwarding Profile**, administrators can define specific actions depending on whether the device is on a **trusted network**:

1. **Tunnel Mode (Recommended)** – Fully encapsulates traffic inside a **DTLS tunnel** to Zscaler, providing **complete visibility** and **policy enforcement**.
2. **Tunnel with Local Proxy** – Uses a loopback proxy to redirect browser traffic before encapsulating it in a secure tunnel.
3. **Enforce Proxy** – Directs traffic to a defined proxy server, using a **PAC file** for routing.
4. **No Forwarding (None)** – Allows traffic to bypass Zscaler and use existing network settings.

Best Practice: Use Z-Tunnel 2.0 to capture all traffic and forward it securely to **Zscaler via DTLS**. This mode provides the most **comprehensive security**, while allowing fallback to **TLS** if necessary.

Edit Forwarding Profile

FORWARDING PROFILE ACTION FOR ZIA

On Trusted Network

Tunnel Tunnel with Local Proxy Enforce Proxy None

Tunnel Version Selection

Z-Tunnel 1.0 Z-Tunnel 2.0

Advanced Z-Tunnel 2.0 Configuration

Z-Tunnel 2.0 Transport Settings

Primary Transport Selection

DTLS TLS

DTLS Connection Timeout (In Seconds)

9

TLS Connection Timeout (In Seconds)

5

MTU for Zscaler Adapter

Optional

Allow Fallback

TLS

Z-Tunnel 2.0 Setup Failure Behavior

Fallback to Z-Tunnel 1.0 and bypass non-web tra...

Redirect Web Traffic to Zscaler Client Connector Listening Proxy

Use Z-Tunnel 2.0 for Proxied Web Traffic

Connection Timeout and Fallback Behavior

To ensure uninterrupted connectivity, Z-Tunnel 2.0 includes **timeout and fallback mechanisms**:

- If a **firewall blocks UDP traffic**, Zscaler Client Connector **automatically switches** to a **TLS-TCP connection** to maintain security.
- Additional options exist to **redirect traffic** to a local listener for tunnel with local proxy configurations.

System Proxy Settings and GPO Considerations

Administrators can control how **proxy settings** are applied at the system level. When migrating from an **on-premises proxy**, previously **configured system proxies must be removed** to prevent conflicts.

Key **system proxy settings** include:

- **No Proxy (Recommended for Tunnel Mode)** – Prevents conflicts with system proxy settings.
- **Automatically Detect Settings** – Uses **WPAD (Web Proxy Auto-Discovery Protocol)** to dynamically retrieve proxy configurations.
- **Automatic Configuration Script** – Configures a **forwarding PAC file** to explicitly define traffic routing.
- **Use Proxy Server for LAN** – Sets a **hardcoded proxy** with an IP/FQDN and port assignment.
- **Execute GPO Update** – Forces **Group Policy Object (GPO) updates** to refresh proxy settings.

Configure System Proxy Settings

System Proxy Settings

Proxy Action Type ?

☒ Enforce ☐ Apply on Network Change ☐ Never

☐ Automatically Detect Settings

☐ Use Automatic Configuration Script ?

☐ Use Proxy Server for Your LAN ?

☐ Execute GPO Update

VPN Trusted Network ?

☒ Same as "On Trusted Network"

☒ Tunnel ☐ Tunnel with Local Proxy ☐ Enforce Proxy ☐ None

Off Trusted Network ?

☒ Same as "On Trusted Network"

☒ Tunnel ☐ Tunnel with Local Proxy ☐ Enforce Proxy ☐ None

It is critical to understand GPO behavior to prevent conflicts when applying **WPAD scripts, PAC files, or direct proxy settings**.

Summary: Forwarding PAC vs. Tunnel Mode

Understanding the role of a **forwarding PAC file** is essential in **Zscaler Client Connector**:

- **In Tunnel Mode (Z-Tunnel 2.0)**: The client should **not use a forwarding PAC file**. Instead, the client **natively intercepts traffic** and **tunnels it directly to Zscaler Zero Trust Exchange** over DTLS.

By leveraging **Z-Tunnel 2.0 with trusted network detection**, organizations **eliminate on-premise proxies**, improve **security enforcement**, and ensure **seamless traffic forwarding** within the **Zero Trust Exchange**.

Application Profile

Configuring **application profiles** for **Windows and Mac** devices is essential to ensure that traffic is securely managed through the **Zero Trust Exchange**. These profiles determine the **forwarding methods, tunneling protocols, and proxy settings** applied to different devices, ensuring seamless policy enforcement.

An **application profile** maps **forwarding profiles** to specific **users and devices** based on predefined criteria. Each **operating system**, including **Windows, Mac, iOS, Android, and Linux**, requires a tailored configuration. In this section, we focus on **Windows and Mac** devices.

The **application profile** determines the **forwarding profile**, which defines the **tunneling method**. When Z-Tunnel 2.0 is selected in the **forwarding profile**, the **application profile** ensures that traffic is securely routed through the tunnel. This configuration also defines **on- and off-trusted network behavior**, ensuring that **system proxy settings are not misconfigured**.

Key App Profile Features

App and IP Bypass

- **Global Bypasses:** Traffic is never forwarded to Zscaler Client Connector.
- **IP Bypasses:** Bypasses traffic received by Zscaler Client Connector, allowing direct communication.

DNS Management

- Determines how **DNS traffic** is handled by Zscaler Client Connector.
- Allows configuration of **DNS domain requests** that should be tunneled to Zscaler Internet Access (ZIA).

Notification and Logging Options

- Enables logging and alert notifications for **security events** and **policy enforcement**.
- **Anti-tampering & Client Version Rollback (Revert):** Prevents unauthorized modifications and allows rolling back to a previous Zscaler Client Connector version if needed.

The screenshot displays the 'TRAFFIC STEERING' configuration page in the Zscaler interface, specifically the 'App and IP Bypass' tab. The page is divided into several sections:

- GLOBAL BYPASSES:** Includes 'Process-Based Application Bypass' (with a version indicator 'v. 4.3.0+'), 'Source Port-Based Bypasses' (with 'v. 4.2.0+'), and 'VPN Gateway Bypass'. There are input fields for selecting bypasses and a 'Upload CSV' button.
- IP BYPASSES:** Includes 'Predefined IP-Based Application Bypass' and 'Custom IP-Based Application Bypass'.
- PASSWORDS:** A section for configuring various passwords, including 'Logout Password', 'Disable Password ZPA', 'Exit Password', and 'Uninstall Password', each with a version indicator.
- AUTHENTICATION:** Includes 'Machine Token' (with 'v. 3.2.0+'), 'Autopilot Machine Provisioning Key', and 'ZPA Machine Authentication' (with 'v. 3.4.0+').
- NOTIFICATION AND LOGGING:** Includes 'Log Mode' (set to 'Debug'), 'Log File Size in MB' (set to '100'), 'Use Zscaler Notification Framework' (checked), 'ZPA ReAuth Notification' (checked), and 'Advanced Notification time (in Mins)' (set to '30').

Advanced Configurations

- **No-default Route Networks:** Supports routing for networks without a default route.
- **Zscaler Firewall Options:** Enables inbound traffic control.
- **ZIA Reactivation Time:** Controls how quickly ZIA reactivates after a network change.
- **Data Protection:** Supports eDLP (Enterprise Data Loss Prevention) control.
- **Secure Client Connector with OTP:** Prevents users from disabling services by requiring a One-Time Password (OTP).
- **Authentication for ZPA Machine Tunnels:** Defines re-authentication criteria to enhance security.

Key Application Profile Configurations

1. PAC File URL Configuration

- Determines which **Zero Trust Exchange** node the client will use based on **geographic IP information**.
- The **PAC file** is later configured in the **Zscaler Internet Access (ZIA) Admin Portal** to specify which traffic should be forwarded or bypassed.

2. Override WPAD (Web Proxy Auto-Discovery Protocol)

- Prevents **Group Policy Object (GPO)** from enforcing **WPAD settings**.
- Ensures that the **WPAD configuration** defined in the **forwarding profile** takes precedence.

3. Restart WinHTTP (Windows-Specific Setting)

- Ensures that **Windows refreshes all proxy settings** when **Zscaler Client Connector** is established.
- Prevents legacy proxy settings from interfering with **Zscaler tunnels**.

4. Tunnel Internal Zscaler Client Connector Traffic

- Ensures that **health updates and policy traffic** remain within **Zscaler tunnels** rather than directly connecting to the **Zero Trust Exchange**.
- Maintains **consistent security and policy enforcement** across all sessions.

5. Cache System Proxy

- Stores the **system proxy state** before **Zscaler Client Connector** is installed.

- When **Zscaler Client Connector is uninstalled or disabled**, the original **proxy settings are restored**, ensuring business continuity.

6. **Zscaler Client Connector Revert**

- Allows **reversion to a previous version** of **Zscaler Client Connector** in case of an upgrade issue.
- Ensures that users can continue to function **without disruptions**, even if an update causes compatibility issues.

Business Continuity & Supportability

The **last two configurations (Cache System Proxy & Zscaler Client Connector Revert)** are particularly important for **business continuity**. If **Zscaler Client Connector** is uninstalled or an **update fails**, these settings ensure that users can continue working without **disruptions to their network connectivity**.

By correctly configuring **application profiles**, organizations ensure that **all traffic is securely forwarded**, policies are **enforced consistently**, and users can **operate without disruptions**, regardless of location or network conditions.

Zscaler Client Connector Considerations

When deploying **Zscaler Client Connector**, it is essential to understand key features and functions that impact its operation and security enforcement. These considerations ensure seamless integration and optimal performance across different use cases. Key aspects to focus on include:

- **ZIA Enrollment** – The process of registering **Zscaler Client Connector** for **Zscaler Internet Access (ZIA)** to enable secure internet and SaaS access.
- **ZPA Enrollment** – Configuring **Zscaler Client Connector** for **Zscaler Private Access (ZPA)** to securely connect users to private applications without exposing them to the open internet.
- **Refresh Intervals** – Defining how often **Zscaler Client Connector** updates policies, refreshes authentication tokens, and synchronizes settings with the **Zero Trust Exchange**.
- **Device Posture and Posture Tests** – Ensuring that endpoints meet security compliance requirements before allowing access, including device health checks, security software validation, and compliance enforcement.

By understanding and implementing these considerations, organizations can optimize **Zscaler Client Connector deployment**, ensuring **secure, seamless, and policy-compliant access** for users across all environments.

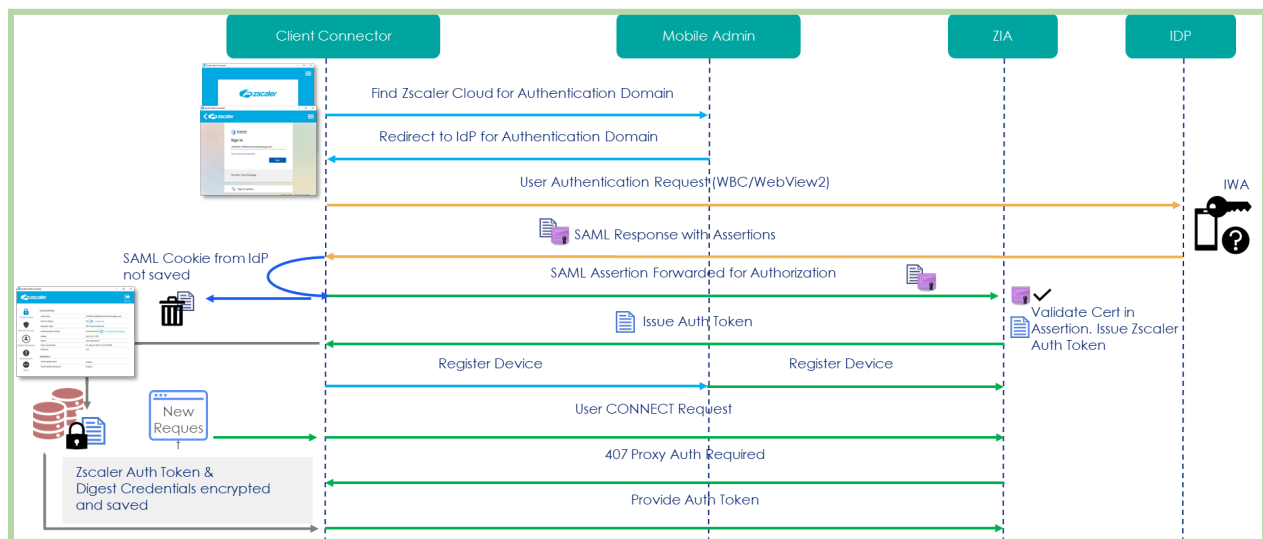
Client Connector ZIA Enrollment

ZIA enrollment in Zscaler Client Connector is a critical process that ensures **user authentication, policy enforcement, and secure traffic forwarding**. Enrollment is achieved through **SAML authentication** with an identity provider (IdP) such as **Okta, ADFS, or Azure AD**, allowing Zscaler to verify user identity and register the device within its security framework.

When a user launches **Zscaler Client Connector**, the first step is **authentication and enrollment**. The client contacts the **Zscaler Client Connector Portal** to determine the user's domain and identify the correct **SAML IdP** for authentication. The user is then redirected to their **SAML IdP** (e.g., **Okta, ADFS, Azure AD**) and signs in. After successful authentication, the **SAML response** is returned to **Zscaler Internet Access (ZIA)**, where it is validated.

If the authentication response is verified, **Zscaler Client Connector** receives an **authentication token**, which it then provides to the **Zscaler Client Connector Portal** for **device registration**. During this process, the portal **fingerprints the device**, registers it within the Zscaler system, and passes the device details to **ZIA**. At this point, **ZIA assigns client credentials** to the user, enabling the client to **authenticate traffic through the Zscaler platform**. This ensures that every request made through **Zscaler Internet Access** is properly **authenticated, inspected, and secured** according to organizational policies.

By completing **ZIA enrollment**, users gain **secure, policy-compliant internet and SaaS access**, while administrators maintain **visibility and control** over user activity, ensuring compliance with **Zero Trust principles**.



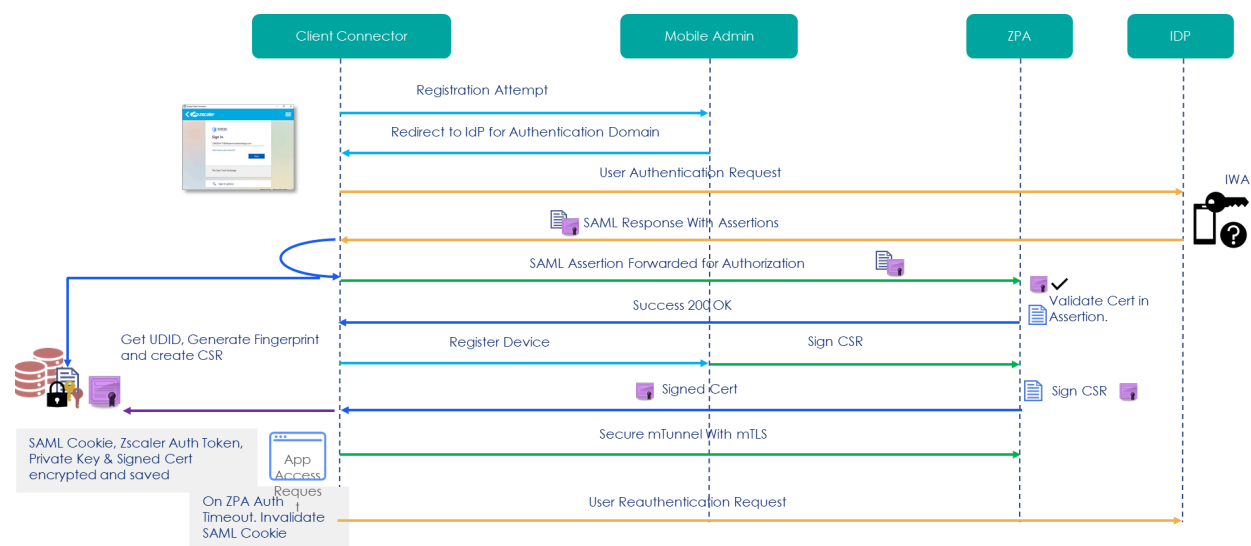
Client Connector ZPA Enrollment

Enrollment in **Zscaler Private Access (ZPA)** through **Zscaler Client Connector** is a distinct authentication process, separate from **Zscaler Internet Access (ZIA)**, though both use **SAML-based authentication**. This process ensures secure **device registration, tunnel creation, and policy enforcement** for accessing private applications.

When the **Zscaler Client Connector** is launched, it already recognizes the **user's domain** from the initial **ZIA enrollment**. The client initiates a **registration attempt**, followed by a second **SAML IdP authentication request**, as **ZIA and ZPA operate as independent SAML-reliant party trusts**. Since the user has already authenticated during **ZIA enrollment**, the **ZPA authentication** process is typically seamless, with the IdP recognizing the existing session. However, depending on the organization's security policies, an **additional multi-factor authentication (MFA) challenge** may be required.

Once authentication is completed, the **SAML response** is returned to **Zscaler Client Connector**, which uses it to **register the device** with the **Zscaler Client Connector Portal**. The portal then passes the **device registration details** to **ZPA**, which enables **certificate-based authentication and enrollment into ZPA**. At this stage, **Zscaler Client Connector establishes secure tunnels** to the **Zero Trust Exchange**, allowing users to access approved private applications securely.

Through **ZPA enrollment**, **Zscaler Client Connector** downloads the necessary **profile and settings**, ensuring that users can access only the **authorized private applications** based on their assigned **policies and entitlements**. This approach enforces **Zero Trust principles**, ensuring that users are securely connected to applications **without ever being placed on the network**, reducing **attack surface exposure** while improving **access control and security**.



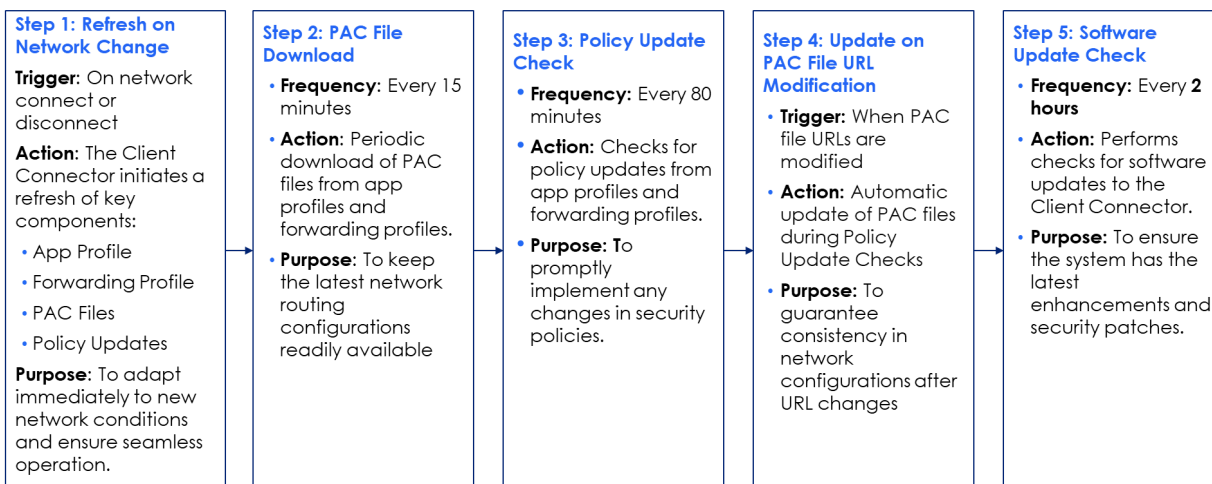
Client Connector Refresh Intervals

The **Zscaler Client Connector** continuously updates **applications, profiles, PAC files, and policies** to maintain security and optimize performance. Its **refresh intervals** are designed to dynamically adapt to **network changes**, ensuring that users remain compliant with the latest security configurations.

To achieve this, **Zscaler Client Connector** follows a structured process to fetch and apply updates, ensuring that all **security policies, access controls, and traffic forwarding settings** remain current. These updates help organizations respond to **changing network environments**, enforce **Zero Trust principles**, and protect users, applications, and data **seamlessly** across any location or device.

Client Connector Refresh Intervals

The Zscaler Client Connector ensures up-to-date information about applications, profiles, PAC files, and policies. Refresh intervals are designed to adapt to network changes and maintain security. The steps shown below detail the process of how the Zscaler Client Connector operates to keep systems secure and efficient.



Step 1: Refresh on Network Change

Trigger: On network connect or disconnect

Action: The Client Connector initiates a refresh of key components:

- App Profile
- Forwarding Profile
- PAC Files
- Policy Updates

Purpose: To adapt immediately to new network conditions and ensure seamless operation.

Step 2: PAC File Download

- **Frequency:** Every 15 minutes

- **Action:** Periodic download of PAC files from app profiles and forwarding profiles.
- **Purpose:** To keep the latest network routing configurations readily available

Step 3: Policy Update Check

- **Frequency:** Every 80 minutes
- **Action:** Checks for policy updates from app profiles and forwarding profiles.
- **Purpose:** To promptly implement any changes in security policies.

Step 4: Update on PAC File URL Modification

- **Trigger:** PAC file URL change in Policy Update
- **Action:** Download PAC file from new URL from the Policy Update
- **Purpose:** To guarantee consistency in network configurations after URL changes

Step 5: Software Update Check

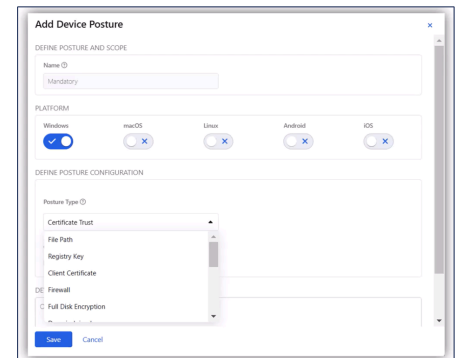
- **Frequency:** Every 2 hours
- **Action:** Performs checks for software updates to the Client Connector.
- **Purpose:** To ensure the system has the latest enhancements and security patches.

Device Posture and Posture Test

The **Zscaler Client Connector** employs **Device Posture** to evaluate the **trustworthiness and security** of devices attempting to access the **Zero Trust Network**. It performs security checks on key factors, including **certificate trust**, **domain-joining status**, **antivirus protection**, **disk encryption**, and **third-party endpoint security integrations**.

Device Posture

- Define device postures
- BYOD vs corporate devices
 - Domain joined, registry, file, certificate trust
 - Client certificate + non-exportable private key
- Device security
 - Anti virus
 - OS version
 - Disk encryption
 - Firewall
- Endpoint protection
 - Carbon Black, CrowdStrike, SentinelOne, Defender
- ZTA score



How Device Posture Enhances Zero Trust Security

Device Postures are powerful because you can also use them for Service Entitlement and App Profile selection!

1. Certificate Trust & Device Identity:

- Verifies if the device trusts an **internal root CA**, distinguishing between **corporate-managed** and **BYOD** devices.
- Checks for **client certificates** with **non-exportable private keys** to ensure device authenticity.

2. Security Compliance & Endpoint Protection:

- Confirms the presence of **antivirus software**, firewall settings, and whether **disk encryption** is enabled.
- Ensures the operating system is updated and compliant with security policies.

3. Integration with Third-Party Endpoint Security:

- Works with leading security providers such as **CrowdStrike**, **CarbonBlack**, **SentinelOne**, and **Microsoft Defender**.
- Leverages **CrowdStrike ZTA scores** and **Defender security insights** to **block compromised devices** from accessing applications.

Posture Check Support

Feature	Windows	macOS	Linux	iOS	Android/ChromeOS
OS Version	Yes	Yes	Yes	No	Yes
File Based Checks	Yes	Yes	No	No	No
Registry Key Checks	Yes	No	No	No	No
Firewall Status	Yes	Yes	No	No	No
Disk Encryption	Yes	Yes	Yes	No	Yes
AD Domain Join Status	Yes	Yes	No	No	No
Azure AD Domain Join Status	Yes	No	No	No	No
Process Status	Yes	Yes	Yes	No	No
Carbon Black Status	Yes	Yes	No	No	No
SentinelOne Status	Yes	Yes	No	No	No
Microsoft Defender Status	Yes	Yes	Yes	No	No
CrowdStrike Status	Yes	Yes	No	No	No
Anti-virus Status	Yes	Yes	Yes	No	No
Client Certificate	Yes	Yes	Yes	Yes	Yes
Server Validated Client Certificate	Yes	No	No	No	No
Client Certificate	Yes	Yes	Yes	Yes	Yes

Device Compatibility & Capabilities

- **Windows and Mac** devices support full posture checks, enabling deep security assessments.
- **iOS and Android** have limited posture-checking capabilities, such as verifying **disk encryption** but lacking **domain-joined status verification**.

By integrating **Device Posture into Zero Trust policies**, Zscaler ensures that **only secure, compliant devices** are granted access, reducing the risk of cyber threats and **unauthorized access** to sensitive applications.

High Level Steps for Client Connector Deployments

- 1 Determine how traffic will be forwarded (Z-Tunnel 2.0, 1.0 etc.)
- 2 Allow Client Connector processes on host AV/EDR
- 3 Configure host and on-premises firewalls to allow Client Connector traffic
- 4 Configure IdP authentication and optional SSO
- 5 Configure user notification, support and other settings in Client Connector Admin Portal
- 6 Configure Trusted Networks, Forwarding Profiles and optional Forwarding Profile PAC
- 7 Configure App Profiles, bypasses and optional App Profile PAC
- 8 Select a release and deploy using UEM/MDM or manually
- 9 Configure policy for ongoing Client Connector auto-updates



Installing Zscaler Client Connector

Administrators have the flexibility to define **policy settings** for managing updates and troubleshooting within **Zscaler Client Connector**. These policies help streamline the installation and maintenance process by enabling features such as **automated updates**, **packet captures**, and **log exports** for diagnostics and issue resolution. By configuring these settings, IT teams can ensure seamless deployment, enhance security, and simplify troubleshooting efforts across all connected devices.

Check for New Releases

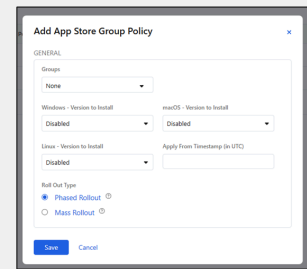
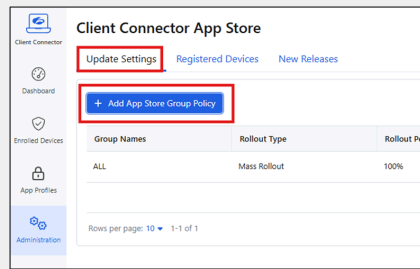


To access the Client Connector **installers**, follow these steps:

- Navigate to **Policy > Client Connector Portal**.
- Select **Administration** tab.
- Select **Client Connector App Store** from the left-side navigation pane.
- Select the **"New Releases"** tab.
- Here we can check if any new versions of the Client Connector are available for distribution. It lets us stay up-to-date with the latest releases and ensure we use the most recent and efficient version of the Client Connector software.

Once we're on the **"New Releases"** tab, we can check if any new versions of the Client Connector are available for distribution. It lets us stay up-to-date with the latest releases and ensure we use the most recent and efficient version of the Client Connector software.

Client Connector Updates by Group

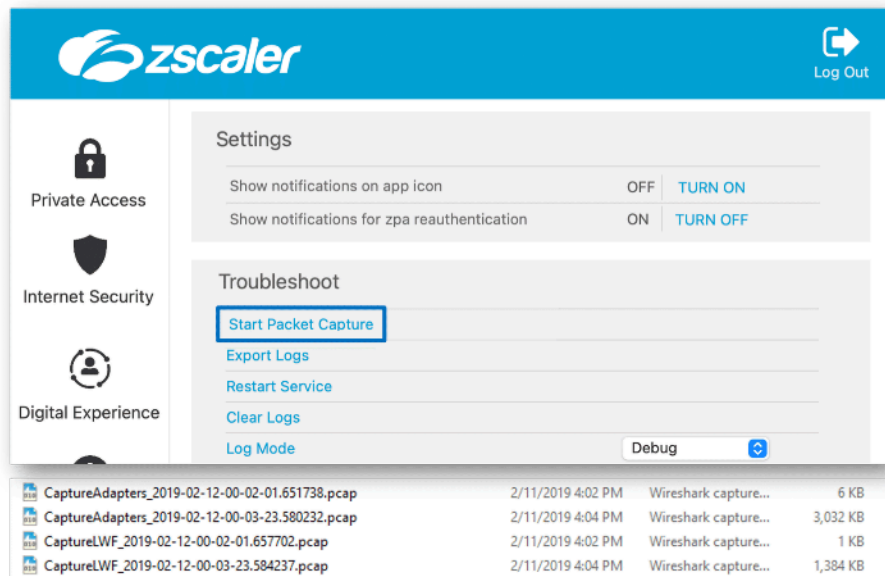


To manage Client Connector versions effectively, **accommodate testing by key groups**, and **reduce the load through staggered rollouts**, follow these steps:

- Assign Client Connector Versions to Specific Groups.
- Allows key groups internally to automatically get the latest version for testing before nominating this for other groups.
- Stagger Rollouts to Reduce Load.

By following these steps, we can effectively assign Client Connector versions to specific groups, facilitate testing by key groups, and reduce the load through staggered rollouts, ensuring a smoother and more efficient update process for our organization.

Full Packet Capture Support

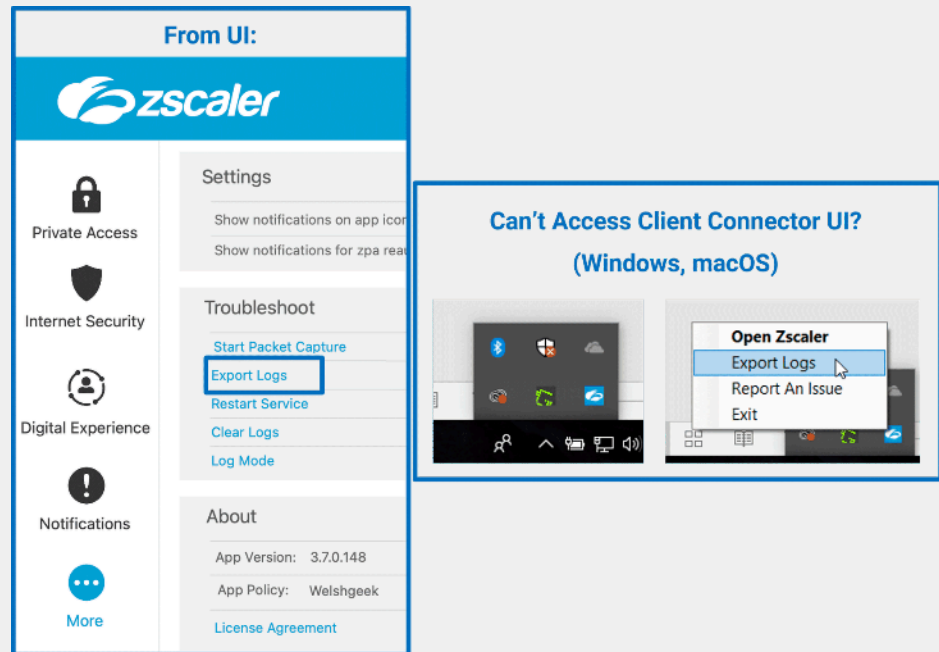


Built-in, System-Wide PCAPs (Includes LWF as Separate PCAP) Functionality:

- **Integrated Start/Stop Control:** Users can initiate or terminate PCAP capture easily.
- **Automatic Timeout:** Capture automatically stops after 5 minutes.

- **Aligned with Log Rotation:** Integration with standard log rotation procedures.
- **Eliminates Third-Party Tools:** Removes dependency on external packet capture software.
- **Admin Control:** This can be disabled by administrators for privacy management.

Exporting Logs



Access Control by Zscaler Administrator:

- The Zscaler administrator can deactivate access to these particular settings.
- Provides centralized control over configuration access.
- Enhances security and privacy management.
- Zscaler administrators can also remotely fetch logs without user interaction

Log Locations for Manual Log Collection

By accessing these directories, users can extract the logs and other pertinent data for analysis or troubleshooting purposes.

OS	Log Locations	Notes
Windows	C:\ProgramData\Zscaler\ %ALLUSERSPROFILE%\Zscaler\	Common logs and Machine Tunnel (ZPA) logs
	C:\ProgramData\Zscaler\log-[User SID] %ALLUSERSPROFILE%\Zscaler\log-[User-SID]	User specific logs
	C:\Users\[User Folder]\AppData\Local\Zscaler\ %LOCALAPPDATA%\Zscaler\	Client Connector UI logs
macOS	/Library/Application Support/Zscaler/	Common logs
	~/Library/Application Support/com.zscaler.zscaler/	User specific logs
Linux	/var/log/Zscaler/	Common logs Installer logs
	~/.Zscaler/Logs/	User specific logs

Automating Installation Options for Zscaler Client Connector

The **Zscaler Client Connector** supports multiple automated installation options across **Windows, macOS, and Linux**, allowing organizations to streamline authentication and enrollment. These options help automate the detection of **SAML Identity Providers (IdPs)**, redirect users for authentication, and ensure a **seamless Zero Trust security deployment**.

Key Installation Parameters for Windows and macOS

To simplify the installation process and eliminate manual user input, administrators can specify installation parameters such as **Cloud Name (-cloudName)** and **User Domain (-userDomain)**.

The **-cloudName** parameter tells the installer which Zscaler cloud environment the organization is using. This prevents users from manually selecting the correct Zscaler cloud during enrollment. Supported cloud names include ZscalerTwo, ZscalerCloud, and ZscalerNet, each corresponding to a specific Zscaler cloud environment.

The **-userDomain** parameter ensures that users are automatically redirected to the correct **SAML IdP** for authentication. This prevents users from needing to manually enter their organization's domain during setup. By specifying **-userDomain**, the client automatically associates the user with the correct authentication flow, ensuring a smooth enrollment process.

The **-strictEnforcement** parameter enforces strict security policies during installation. When enabled, it ensures that all **traffic forwarding rules and security policies** are strictly applied, preventing users from disabling Zscaler Client Connector or bypassing security controls. In this mode:

Requirements:

cloudName and **-policyToken** must be specified during installation to establish the correct cloud environment and policy enforcement.

Behavior:

- **PAC File Bypasses:** If the PAC file used in the **App Profile** contains bypass rules that match the **-policyToken** specified during installation, those specific

bypasses will still be honored.

- **Tunnel Mode Enforcement:** When running in **Tunnel Mode**, all traffic on **ports 80 (HTTP) and 443 (HTTPS)** will be blocked unless explicitly forwarded through Zscaler.
- **Tunnel with Local Proxy:** Traffic that adheres to the **PAC file's forwarding rules** will be blocked unless directed through Zscaler.
- **Control Traffic Forwarding:** Any **administrative or policy updates** initiated by **ZSATray or the Zscaler Client Connector UI** will still be securely forwarded.

Customization and Deployment Tools

For organizations that manage large deployments, these installation parameters can be embedded within software installation tools like **Microsoft Endpoint Configuration Manager (MECM)**, **Intune**, and **Jamf**. These tools enable automated distribution of the client across endpoints, ensuring users can securely connect without additional setup steps.

Install Client Connector : Windows .EXE Options

- Windows .EXE command line options

- File rename option, e.g. `example.com-Zscaler-windows-3.5.0.108-installer`

- Run the install executable file with the appropriate command line options...

```
<complete_path> --cloudName <zscaler_cloud> --deviceToken <device_token> --hideAppUIOnLaunch 1  
--mode unattended --policyToken <policy_token> --reinstallDriver 1 --strictEnforcement 1  
--unattendedmodeui <UI_mode> --userDomain <your organization's domain>
```

- Where: `<complete_path>` is the location of the installer .EXE file

<code>--cloudName</code>	: optional value	<code><zscaler_cloud></code> is the name of the Zscaler cloud to connect to
<code>--deviceToken</code>	: optional value	<code><device_token></code> is the device token for silent authentication to Zscaler IdP
<code>--hideAppUIOnLaunch</code>	: optional flag	<code>1</code> specifies Client Connector UI is to remain hidden
<code>--mode</code>	: optional flag	<code>unattended</code> to run in silent mode
<code>--policyToken</code>	: optional value	<code><policy_token></code> is the token of the App Profile to apply
<code>--reinstallDriver</code>	: optional flag	<code>1</code> specifies that the driver is to be reinstalled
<code>--strictEnforcement</code>	: optional flag	<code>1</code> specifies Client Connector enforcement option
<code>--unattendedmodeui</code>	: optional value	<code><UI_mode></code> available: <code>none</code> , <code>minimal</code> , <code>minimalWithDialogs</code>
<code>--userDomain</code>	: optional value	<code><your organization's domain></code> specifies the domain

[For a complete list of installation switches refer to Zscaler help article](#)

Additionally, **MST (Microsoft Transform) files** can be used alongside **MSI (Microsoft Software Installer) files** to customize the installation process.

MST files allow organizations to preconfigure settings within an MSI package, ensuring that the Zscaler Client Connector is deployed with the correct policies, authentication settings, and user experience preferences.

MSI files contain all the necessary installation instructions for deploying Zscaler Client Connector on Windows systems, standardizing the process and enabling scalability.

By leveraging **MST files with MSI deployment**, administrators can tailor the installation to match their organization's requirements while automating distribution through tools like **SCCM (System Center Configuration Manager, now called Microsoft Endpoint Configuration Manager)** or **Intune**.

Install Client Connector : Windows .MSI/.MST Options

Windows .MSI options

Edit the MSI installer file as necessary to apply options...

```
msiexec /i "<complete_path>" /quiet CLOUDNAME=<zscaler_cloud> DEVICETOKEN=<device_token>  
HIDEAPPUIONLAUNCH=1 POLICYTOKEN=<token_id> REINSTALLDRIVER=1 STRICTENFORCEMENT=1 USERDOMAIN=<your  
organization's domain> UNINSTALLPASSWORD=<password>
```

Where: <complete_path> is the location of the installer .MSI file

/quiet	: optional flag specifies deploying the Client Connector in silent mode
CLOUDNAME=	: optional value <zscaler_cloud> is the name of the Zscaler cloud to connect to
DEVICETOKEN=	: optional value <device_token> device token for silent authentication to Zscaler IdP
HIDEAPPUIONLAUNCH=	: optional flag 1 specifies Client Connector UI is to remain hidden
POLICYTOKEN=	: optional value <token_id> is the token of the App Profile to apply
REINSTALLDRIVER=	: optional flag 1 specifies that the driver is to be reinstalled
STRICTENFORCEMENT=	: optional flag 1 specifies Client Connector enforcement option
UNINSTALLPASSWORDCMDLINE=	: optional value <password> Uninstall Password from App Profile (MST only)
USERDOMAIN=	: optional value <your organization's domain> specifies the domain

[For a complete list of installation switches refer to Zscaler help article](#)

For **macOS**, the installer can be packaged into a **PKG file** for streamlined deployment, while Linux requires specific system prerequisites for proper installation. Organizations can also enforce **strict enforcement mode**, ensuring that all security policies remain applied without user tampering.

Install Client Connector : MacOS PLIST Support

- macOS deployment supports use of PLIST when deploying using a MDM/UEM
- When deploying using PLIST, the PKG download must be used
- Supports all install options switches
- A MDM/UEM is required to enable the following:

Trusted SSL inspection certificate in the macOS keychain
Custom Application-based bypass
Zscaler Firewall on macOS
Enable Full Disk Access for endpoint DLP on macOS

```
<?xml version="1.0" encoding="UTF-8"?>  
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-  
1.0.dtd">  
<plist version="1.0">  
  <dict>  
    <key>installation-parameters</key>  
    <dict>  
      <key>hideAppUIonLaunch</key>  
      <string>0</string>  
      <key>deviceToken</key>  
      <string></string>  
      <key>cloudName</key>  
      <string>zscaler</string>  
      <key>externalRedirect</key>  
      <string>>false</string>  
      <key>strictEnforcement</key>  
      <string>0</string>  
      <key>userDomain</key>  
      <string>customerdomain.com</string>  
      <key>launchTray</key>  
      <string>1</string>  
      <key>enableFips</key>  
      <string>0</string>  
    </dict>  
  </dict>  
</plist>
```

Install Client Connector : MacOS Options

MacOS install options

- File rename option, e.g. **example.com-Zscaler-osx-1.5.0.326-installer**

- Use Casper Suite or Tanium with the following installation command and options...

```
sudo sh $downloadLocation/Contents/MacOS/installbuilder.sh --cloudName $cloudNameValue --deviceToken $deviceTokenValue --hideAppUIOnLaunch --launchTray 0 --mode unattended --policyToken $policyTokenValue --reinstallDriver 1 --strictEnforcement 1 --unattendedmodeui $Uimode --userDomain $userDomainValue
```

- Where: `$downloadLocation` is the location of the unzipped installer app

```
--cloudName      : optional value $cloudNameValue is the name of the Zscaler cloud to connect to
--deviceToken    : optional value $deviceTokenValue device token for silent authentication to Zscaler IdP
--hideAppUIOnLaunch: optional flag 1 specifies Client Connector UI is to remain hidden
--launchTray     : optional flag 0 specifies Client Connector is not to run automatically
--mode           : optional flag unattended to run in silent mode
--policyToken    : optional value $tokenValue is the token of the App Profile to apply
--strictEnforcement: optional flag 1 specifies Client Connector enforcement option
--unattendedmodeui : optional value $Uimode available: none, minimal, minimalWithDialogs
--userDomain     : optional value $userDomainValue is the domain of your organization
```

[For a complete list is installation parameters refer to Zscaler help article](#)

Linux offers similar installation options to macOS but comes with additional prerequisites. Specific Linux distributions and versions must be supported, and certain libraries must be installed to ensure the **Zscaler Client Connector** functions properly and integrates with the user interface. Before installation, users must verify that their **Linux system meets the required specifications** and that all necessary dependencies are in place to ensure seamless operation.

Install Client Connector : Linux Options

Linux .run command line options

Install prerequisite dependencies (if necessary)...

```
sudo apt install net-tools libqt5dbus5 libqt5core5a libqt5sql5 libqt5sql5-sqlite libqt5webchannel5 libqt5webengine5 libqt5webenginecore5 libqt5webenginewidgets5 libqt5webkit5 libqt5webview5 libqt5widgets5 libnss3-tools libpcap ca-certificates -y
```

Run the install executable file with the appropriate command line options...

```
sudo <complete_path> --cloudName <zscaler_cloud> --deviceToken <device_token> --hideAppUIOnLaunch 1 --policyToken <policy_token> --strictEnforcement 1 --userDomain <your organization's domain> --enableFIPS
```

Where: `<complete_path>` is the location of the installer .run file

```
--cloudName      : optional value <zscaler_cloud> Zscaler cloud name to connect to
--deviceToken    : optional value <device_token> is the device token for silent authentication to Zscaler IdP
--hideAppUIOnLaunch: optional flag 1 specifies Client Connector UI is to remain hidden
--policyToken    : optional value <policy_token> is the token of the App Profile to apply
--strictEnforcement: optional flag 1 specifies Client Connector enforcement option
--userDomain     : optional value <your organization's domain> specifies the domain
--enableFIPS     : optional flag 1 to enable FIPS mode (defaults to 0)
```

Summary of Zscaler Client Connector

The **Zscaler Client Connector** is a lightweight application designed to provide secure connectivity within the **Zero Trust Exchange**. It ensures secure access by verifying user, device, and application identity while managing connections to the exchange.

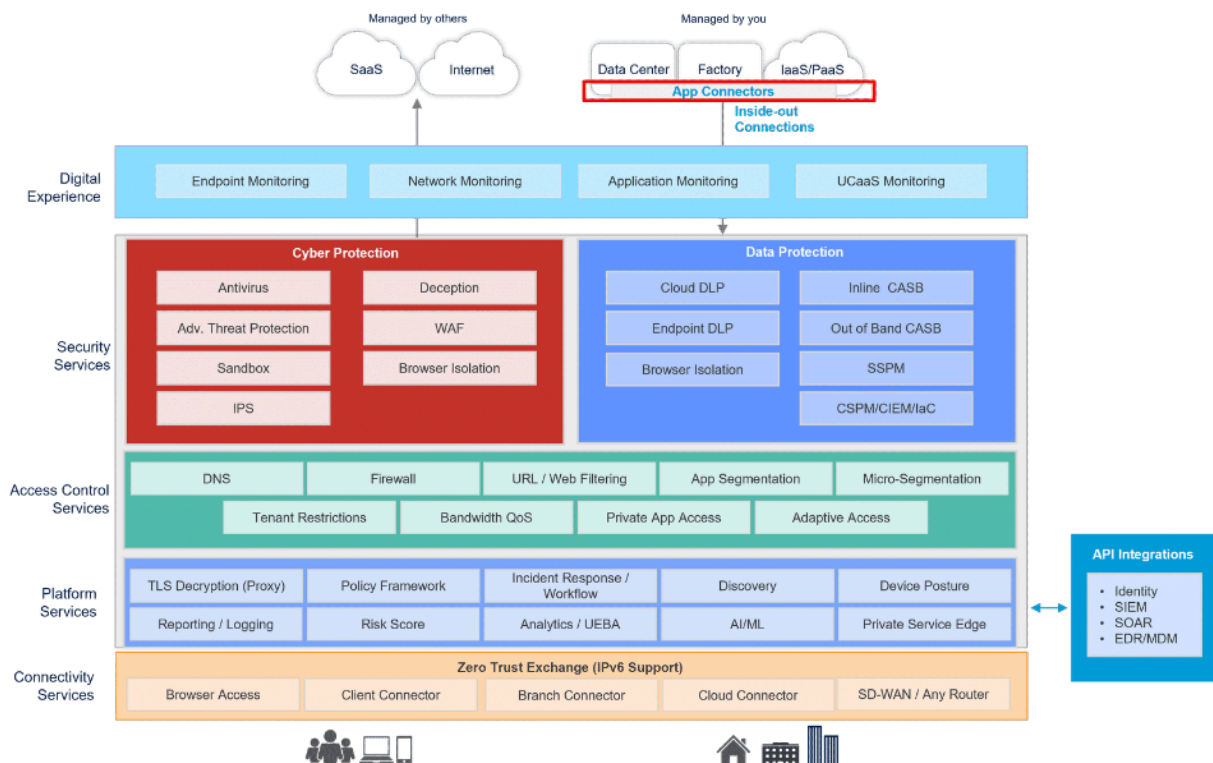
- **Unified Connectivity Services:** Zscaler Client Connector consolidates multiple user connectivity services on endpoint devices, streamlining access management and enhancing security by authenticating users and devices before granting access to applications.
- **Traffic Forwarding & Application Profiles:** The Client Connector establishes **secure tunnels** and applies user-based policies for traffic flowing to **Zscaler Internet Access (ZIA)**. Configuring **application profiles** optimizes traffic routing and ensures system stability.
- **Zero Trust Security Features:** Designed for **Zero Trust architecture**, the Client Connector connects users and devices to the **Zero Trust Exchange**, simplifying authentication, provisioning, and centralized administration while offering **flexible service management**.
- **Application Profile Setup:** Application profiles are essential for **Windows and macOS** devices. They define **traffic forwarding, tunneling protocols, and proxy settings**, ensuring smooth network performance and uninterrupted business operations.
- **Enrollment Process:** Users enroll in Zscaler Client Connector through authentication via a **SAML Identity Provider (IdP)**. Successful authentication generates an authentication token, which registers the device, applies security policies, and establishes secure tunnels for application access.
- **Security Refresh & Updates:** To maintain security, Zscaler Client Connector **periodically refreshes policies and configurations**, including applications, profiles, **PAC files**, and system policies. These updates occur at regular intervals and adapt to network changes, ensuring seamless operation. Additionally, **device posture checks** help assess and enforce security policies for both corporate and BYOD (Bring Your Own Device) endpoints.

By integrating **Zscaler Client Connector**, organizations enhance their **Zero Trust security framework**, ensuring **secure, policy-driven connectivity** while maintaining a **seamless user experience**.

App Connectors

An **App Connector** facilitates seamless communication between applications, services, and data sources, ensuring secure and efficient data exchange across systems without requiring extensive custom integrations.

In this chapter, we explore **Zscaler's App Connectors**, which enable **secure, Zero Trust access** by acting as an intermediary between users and private applications. These connectors ensure that users can **access applications securely** through the **Zero Trust Exchange**, without exposing them to the internet or requiring traditional network-based access methods.



Connections to Private Access App Connectors



App Connectors serve as a **secure and authenticated bridge** between an organization's internal servers and the **Zscaler Private Access (ZPA) cloud**. They establish outbound connections through the **firewall** to the **Zscaler cloud**, eliminating the need for inbound connections that could expose internal resources to threats. Once connected, the **ZPA cloud** facilitates **reverse connections**, allowing authorized users to securely access private applications without placing them on a publicly routable network. This architecture ensures seamless, **zero-trust application access**, enhancing security while simplifying connectivity.

Provisioning Keys

A **provisioning key** is a unique text string generated when adding a new **App Connector**. During deployment, you are required to enter this key, which serves as an **identifier** that allows the **ZPA cloud** to verify the **App Connector's authenticity** and complete the deployment process. Each provisioning key is linked to a specific **App Connector group**, ensuring that newly deployed **App Connectors** are assigned to the correct group for streamlined management and connectivity.

Benefits of App Connector Provisioning Keys

Provisioning keys play a critical role in **secure and scalable** App Connector deployment. They enable administrators to:

- Deploy **App Connectors** into a designated **App Connector group**.
- Set limits on the number of times a key can be used for deployment.
- Monitor the current **utilization count** of the key.
- Adjust the **maximum number of times** a key can be used.
- Select a **signing certificate** for enrolling App Connector certificates.

Optimized for Auto-Scaling

Provisioning keys are designed to **support auto-scaling**, allowing organizations to **deploy additional App Connectors** as needed, ensuring they can efficiently handle increased capacity demands. When generating a provisioning key, administrators can **define the maximum number of deployments** permitted with that key.

The **ZPA dashboard** tracks key usage, displaying the number of times a key has been used. Once a key reaches its usage limit, it can no longer be used for new **App Connector deployments**—unless the administrator modifies the key's **maximum usage count**. Additionally, multiple **provisioning keys** can be associated with a **single App Connector group**, offering greater flexibility in deployment strategies.

Next, let's explore **Zscaler's best practices** and **recommendations** for **deploying App Connectors** effectively.

Deploying App Connectors in Various Environments

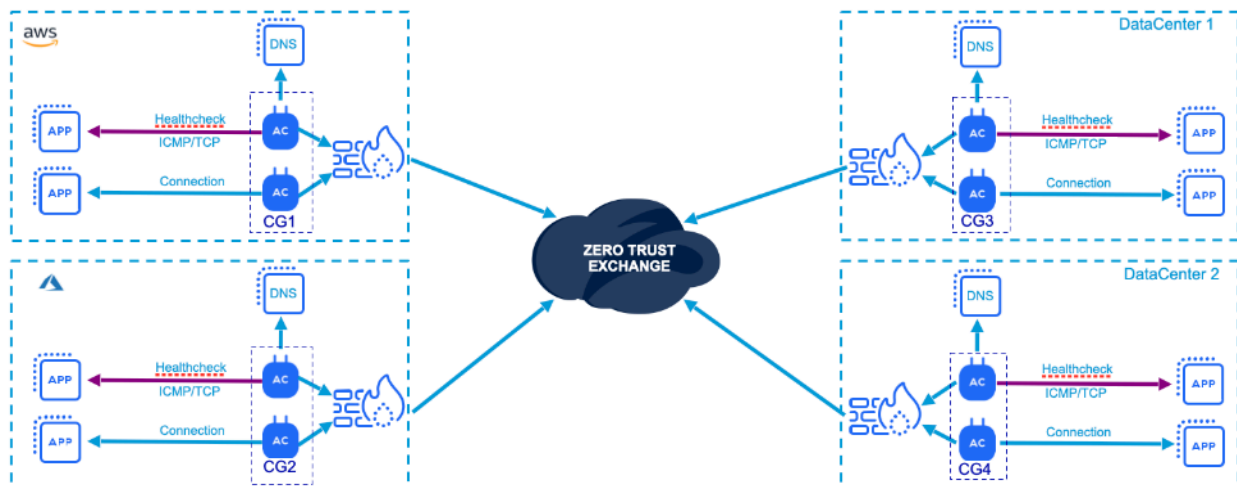
Deploying and configuring **App Connectors** across multiple data centers and cloud infrastructure environments is critical for establishing **secure, resilient, and high-performing** connections. Proper deployment ensures **fault tolerance, optimal routing, and seamless access** to private applications.

Key Considerations for Deployment:

- **Deploy App Connectors in pairs** to enhance resilience and prevent single points of failure.
- **Treat each deployment location as a separate connector group** to maintain efficient network segmentation.
- **Meet routing and Layer 4 connectivity requirements** to ensure seamless communication.
- **Properly configure applications such as Active Directory** to align with network policies.

Best Practices for App Connector Deployment

When deploying **App Connectors**, they should be placed in **data centers** and **Infrastructure-as-a-Service (IaaS) environments** such as AWS, Azure, or Google Cloud. Each **App Connector pair** is assigned to a distinct **connector group**, ensuring redundancy and failover support.



For example, if an organization has a **data center in London**, a **data center in New York**, an **AWS instance in US West**, and an **Azure instance in EMEA Central**, then:

- These are **four separate locations**, each requiring its own **connector group**.
- Each location should have **at least two App Connectors**, totaling **eight connectors across all locations**.

Connectivity and Routing Requirements

App Connectors must be **routable to both the internet and internal applications**. This involves:

- **Layer 4 connectivity requirements**, ensuring proper routing and network accessibility.
- **Meeting CPU and memory requirements**, which are detailed on the **Zscaler Help Center** and updated regularly.

For applications using **TCP**, App Connectors must be able to **open the necessary ports** to establish communication. For **UDP-based applications**, **ICMP (ping) must be enabled**, allowing the system to infer the application's health status.

- **UDP Health Checks:** Since UDP does not allow traditional health verification, Zscaler infers UDP application health using a **prior TCP check**.
- Example: If **TCP 389** is successfully connected, then a **UDP 389** request to the same server is assumed to be healthy.

Understanding App Connector IP Addressing

Any traffic that passes through an **App Connector** adopts the **source IP address of the App Connector**.

- A user accessing a private application via the **Zero Trust Exchange** first connects using **Zscaler Client Connector**.
- The request is **tunneled through the Zero Trust Exchange** to the **App Connector**.
- From the **App Connector to the private application**, the source IP seen by the **destination server** is the **IP address of the App Connector** rather than the user's original IP.

Impact on Active Directory and Network Policies

Certain applications, such as **Active Directory**, enforce policies based on the **client IP address**. Since the **App Connector's IP** is presented to the network:

- The **Active Directory Sites and Services configuration** must account for **App Connector IPs** to ensure proper **user authentication and policy enforcement**.
- This ensures that users are directed to the correct **domain controllers** for **authentication, GPO enforcement, and resource access**.

Example: Deploying App Connectors in a Zero Trust Architecture

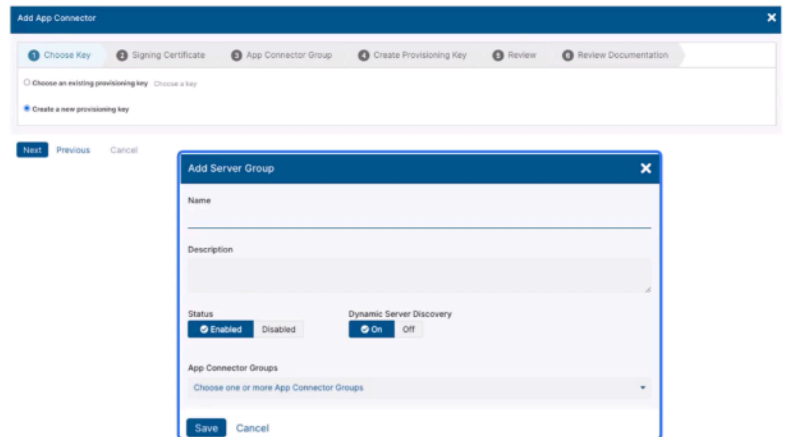
Deploying **App Connectors** in **Zscaler Private Access (ZPA)** is essential for **secure, policy-based connectivity** between users and private applications. This example outlines the **step-by-step process** for setting up App Connectors, provisioning keys, and mapping applications to ensure a **seamless Zero Trust implementation**.

Step 1: Generating a Provisioning Key

Provisioning keys serve as **unique identifiers** for **secure App Connector deployment** and **TLS connection generation** within ZPA. These keys are signed by an **intermediate certificate authority (CA)** and provide a **chain of trust** between users, applications, and ZPA.

Example: Creating a Provisioning Key

- An administrator logs into the **Zscaler Client Connector Portal** and navigates to the **Provisioning Keys** section.
- A new **provisioning key** is generated and securely stored.
- This key is later used to **deploy App Connectors** in different locations.

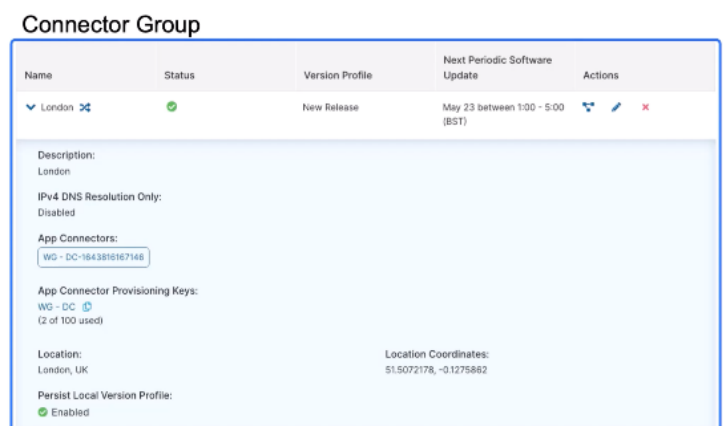


Step 2: Deploying App Connectors

App Connectors are installed in **data centers, cloud environments (AWS, Azure), or virtual private clouds (VPCs)**. Each location represents a **separate App Connector group**.

Example: Deploying App Connectors in Multiple Locations

- A company has **four infrastructure locations**:
 - **London Data Center**
 - **New York Data Center**
 - **AWS US-West**
 - **Azure EMEA-Central**
- Each location is assigned a **separate App Connector group**, with two connectors deployed per location for **redundancy**.



- The App Connectors **establish secure tunnels** to the **Zero Trust Exchange**.
- **Connectivity between locations** (such as data center-to-data center, AWS-to-data center) can be established using **ExpressRoute, Direct Connect, or site-to-site VPNs**.




Step 3: Assigning App Connectors to a Server Group

Each App Connector must be **linked to a server group**, which helps direct **user requests to the correct applications**.

Example: Mapping App Connectors to a Server Group

- The **London and New York App Connectors** are assigned to a “**Corporate Data Center**” server group.
- The **AWS and Azure App Connectors** are assigned to a “**Cloud Applications**” server group.
- **Each group has a localized DNS configuration**, ensuring low-latency name resolution.
- **Dynamic Server Discovery** is enabled, allowing **automatic DNS resolution** for applications.

Server Group

Name	Status	Dynamic Server Discovery	App Connector Groups	Actions
1. DC Discovery	✓	✓	London	  
Description DC Discovery Servers				






Step 4: Defining Application Segments

Applications must be mapped to **App Connectors** through **application segments**, which define **access rules and security policies**.

Example: Creating Application Segments

- The administrator creates an application segment for **Sales Applications** using the wildcard *.salesportal.company.net.
- Any request for an application matching this domain is **resolved through the assigned App Connectors**.
- **Health checks validate application availability**, ensuring seamless connectivity.

Application Segment

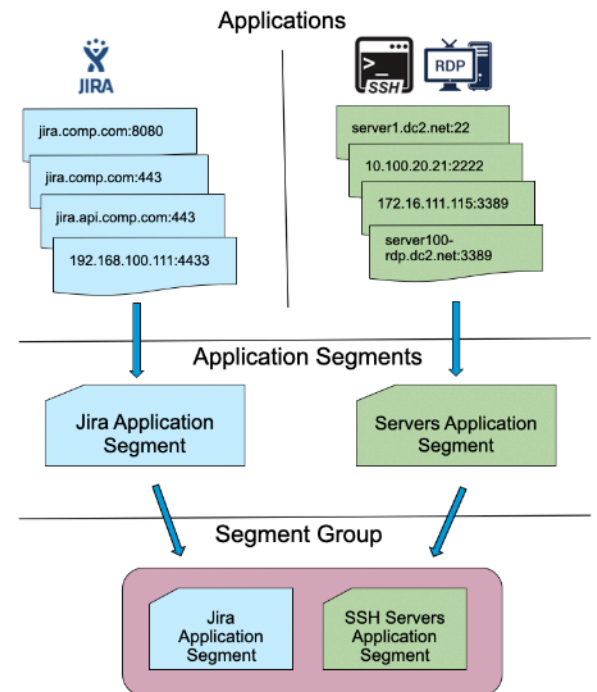
Wildcard	*.welshgeek.net	✓	On Access	    
Description				
Segment Group		Server Groups		
DC Apps		1. DC Discovery		
Double Encryption		Bypass		Client Connector can receive CNAME
✗ Disabled		Use Client Forwarding Policy		✓ Enabled
Source IP Anchor		ICMP Access		
✗ Disabled		✗ Disabled		

Step 5: Enforcing Zero Trust Access Policies

Once App Connectors are deployed and application segments are defined, the **Zero Trust Exchange** evaluates user access **in real-time**.

Example: User Requesting Access to an Internal Application

1. A sales employee attempts to access **salesportal.company.net**.
2. The request is sent to the **Zero Trust Exchange**, which checks **user identity, device security posture, and policies**.
3. The Exchange selects the **best App Connector** to service the request.
4. The App Connector **performs a DNS lookup and health check**.
5. If the application is available, the **connection is securely brokered**.



Step 6: Managing Source IP and Active Directory Integration

Since users do not connect **directly** to internal applications, the **App Connector's source IP** is used for network communication.

Example: Configuring Active Directory for App Connector Access

- The **App Connector's IP** is **registered in Active Directory** to ensure correct **user policy enforcement**.
- Group Policy Objects (GPOs) and authentication mechanisms recognize the **App Connector's IP** instead of the user's **local IP**.
- **Result:** Users can **seamlessly** access applications without **network exposure**.

Where Do All These Components Fit?

Within the **Zscaler Client Connector**, the client recognizes the assigned wildcard ***.domain.com** and requests access to an internal application. The request is then processed as follows:

1. **Querying the Zero Trust Exchange:**
 - The client queries the **Zero Trust Exchange** to check **whether access is allowed**.
 - The Exchange determines **which App Connector serves the application**.
2. **Evaluating Policy & Application Availability:**
 - The App Connector evaluates policy, performs a **DNS request**, and determines which **connector is best suited** for handling the request.
 - A **health check** is performed to verify that the application is available.
3. **Establishing a Secure Connection:**
 - If the application is accessible, the connection is **securely brokered** through the **Zero Trust Exchange**.
 - The client **egresses onto the network** via the **source IP address of the App Connector**.

This process ensures that **users securely access applications** without **direct exposure to the network**, maintaining **Zero Trust security principles**.

Conclusion

This **example** illustrates how organizations can **deploy App Connectors** to securely connect users to private applications. By leveraging **provisioning keys, server groups, and application segments**, companies can **eliminate network exposure** and ensure **policy-driven, Zero Trust access** to corporate resources.

Platform Services

This chapter provides a comprehensive overview of Zscaler's **Platform Services** within the **Zero Trust Exchange (ZTE)**, detailing their functionalities, interactions, and typical configurations. The content is divided into two key sections, designed to progressively build a deeper understanding of Zscaler's platform capabilities.

Platform Services Overview

The first section introduces **Zscaler's Platform Services**, which serve as the foundation of the **Zero Trust Exchange**. These services enable seamless **security, connectivity, and policy enforcement** across the ecosystem, supporting critical functions such as **traffic forwarding, identity integration, logging, and policy evaluation**.

Zscaler's Platform Services Suite

The second section delves deeper into **device posture evaluation**, a crucial aspect of **Zero Trust policy enforcement**. This includes assessing various **security parameters**, such as **domain join status, endpoint protection compliance, and third-party security integrations** like the **CrowdStrike ZTA score**.

By the end of this chapter, you will be able to

1. **Identify** the fundamental set of Platform Services Zscaler provides and how they apply to the Zero Trust Exchange
2. **Explain** what is device posture and features that make device posture an exceptional solution
3. **Describe** the TLS/SSL Inspection process
4. **Summarize** how to configure policies for ZIA, ZPA, and ZDX

Zscaler's Platform Services

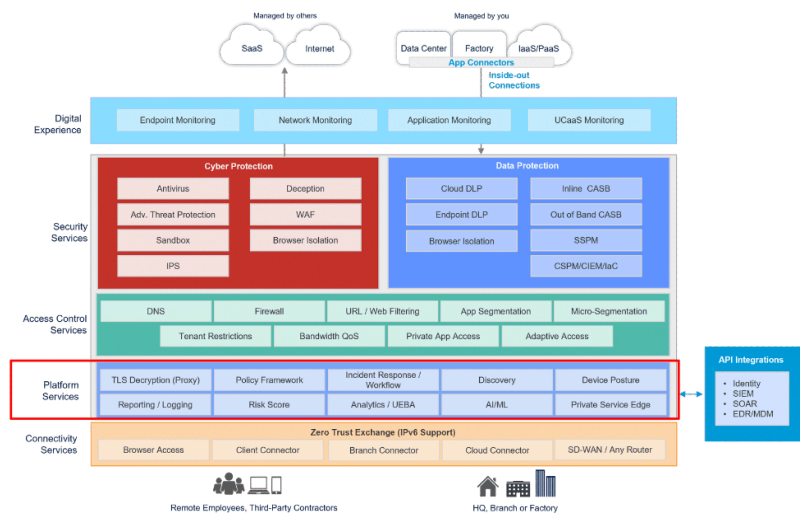
Included within Zscaler's holistic Zero Trust Exchange is the **Platform Services** suite, which contains a set of fundamental functionalities that are common across Zscaler's other service suites, including **Connectivity**, **Access Control**, **Security**, and **Digital Experience**.

Zscaler's Zero Trust Exchange architecture provides multiple options for establishing secure connections.

In this chapter, we will explore the key services within the **Zero Trust Exchange** that enable and support other security capabilities. These services play a critical role in enforcing **secure access, visibility, and policy controls** across the network. The topics covered include:

- **Device Posture** – Evaluating endpoint security and compliance to determine trust levels for access control.
- **TLS Inspection** – Decrypting and inspecting encrypted traffic to detect threats and enforce security policies.
- **Policy Framework** – Defining and applying policies that govern user access, data protection, and security enforcement.

Each of these components contributes to a **comprehensive Zero Trust security model**, ensuring **continuous monitoring and dynamic risk-based decision-making**.



Zscaler's Platform Services Suite

Device Posture

Device Posture ensures that a device meets a **minimum security standard** before being granted access to applications or data. This evaluation helps mitigate risks by verifying the security health of endpoints before they interact with corporate resources. In this section, we'll focus on the highlighted components within the **Zero Trust Exchange** that contribute to Device Posture enforcement.

What is Device Posture?

Device Posture refers to the **security status** of a computing device—such as a **laptop, smartphone, or tablet**—based on its **settings, configurations, and security controls**. It determines whether a device is **compliant, trusted, or at risk**, influencing its level of access to corporate applications and data.

By assessing various factors, Device Posture provides **real-time insights** into potential risks and vulnerabilities, ensuring that only secure devices can interact with critical business applications.

Where to Access Device Posture in Zscaler?

Device Posture is part of **Zscaler's Platform Services suite** and can be accessed through the following path in the **ZIA Admin Portal**:

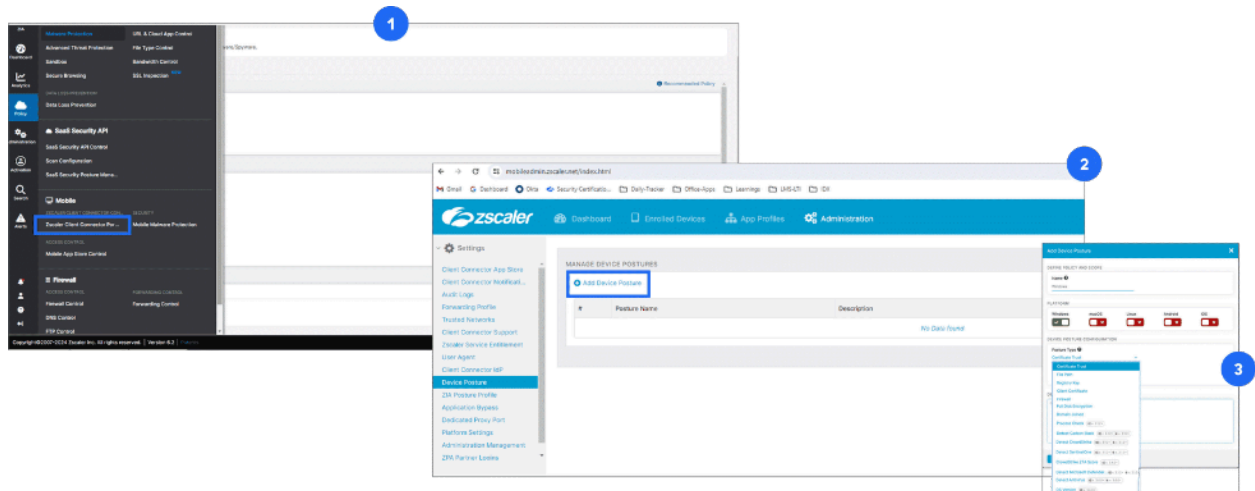
ZIA Admin Portal > Policy > Zscaler Client Connector > Administrator > Device Posture

Additionally, Device Posture integrates with other **Zero Trust Exchange** functionalities, including:

- **Browser Access** – Verifies security compliance before granting web-based application access.
- **Zscaler Client Connector** – Enforces security policies based on device posture checks.
- **Identity Integration** – Uses authentication methods to align security policies with user identity.

Key Features of Device Posture in Zscaler

Zscaler's **Device Posture** leverages four key functionalities to ensure robust security enforcement:



1. **Policy Access Control** – Enforces dynamic access policies based on real-time device security status.
2. **SAML Authentication Response** – Uses identity attributes to validate device trustworthiness during authentication.
3. **Trusted Networks** – Recognizes known corporate networks and applies appropriate security policies.
4. **Browser Access** – Ensures security compliance for users accessing applications via web browsers.

By incorporating these **security controls**, Zscaler's **Device Posture** strengthens endpoint security and ensures that only compliant devices can access **corporate applications and data** within the **Zero Trust Exchange**.

Device Posture for Enhanced Policy Access Control

Device Posture plays a crucial role in securing organizational networks and data by evaluating various **device configurations and security measures**. By assessing the security status of endpoints, **Device Posture enables dynamic policy enforcement** to ensure that only compliant and trusted devices gain access to corporate applications.

BYOD vs. Corporate Devices

Differentiating between **Bring Your Own Device (BYOD)** and **corporate-managed devices** is essential for **tailored access control**.

- **BYOD Devices:** Personal devices used for work, often lacking enterprise-grade security controls.
- **Corporate Devices:** Company-owned and managed endpoints with enforced security policies.

By identifying these distinctions, **Device Posture assessments** help enforce appropriate access policies, allowing secure access for corporate devices while restricting or limiting BYOD devices.

Key Components of Device Posture

Zscaler's **Device Posture** assessment evaluates multiple security attributes to determine device trustworthiness, including:

- **Domain Joined Status** – Confirms whether the device is part of the organization's domain network, ensuring centralized security management.
- **Registry, File, and Certificate Trust** – Checks for specific **registry keys, system files, and trusted certificates** to verify device integrity.
- **Client Certificate with Non-Exportable Private Key** – Ensures a **client certificate** issued by a trusted authority is present and that the **private key remains protected**, preventing unauthorized export.
- **Device Security Measures** – Evaluates essential security controls, such as:
 - Antivirus software presence and status
 - Operating system version compliance
 - Disk encryption enforcement
 - Firewall activation
 - Endpoint protection solutions (e.g., **Carbon Black, CrowdStrike, SentinelOne, Defender**)
- **CrowdStrike ZTA Score** – Measures the device's adherence to **Zero Trust security principles**, aiding in **real-time policy enforcement**.

Ensuring Device Security Before Access

Before granting access to **corporate applications and sensitive data**, the **Device Posture assessment** ensures that devices meet security requirements. This involves:

- **Verifying antivirus software is active and updated**
- **Checking OS version compliance**
- **Confirming disk encryption is enabled**
- **Ensuring firewall protections are in place**
- **Assessing endpoint protection solutions for threat defense**

In the next section, we will explore how **SAML authentication responses** further enhance security by integrating **identity attributes** into access control policies.

SAML Response to Authentication: Strengthening Access Control

Security Assertion Markup Language (**SAML**) is a widely used authentication protocol that facilitates the **secure exchange of authentication and authorization data** between an **Identity Provider (IdP)** and a **Service Provider (SP)**. In the context of Zscaler, **SAML responses play a critical role** in enforcing access policies based on user identity, device context, and security attributes.

Understanding SAML Response Attributes

When a user successfully authenticates, the **SAML IdP** issues an **XML-based assertion** that contains **key attributes** used by **Zscaler's Service Providers (SPs)** to implement access policies.

Example of Key SAML Response Attributes:

```
{
  "nameid": "mryan@welshgeek.net",
  "orgId": null,
  "idpEntityID": null,
  "idpid": null,
  "saml_attributes": {
    "http://schemas.microsoft.com/identity/claims/tenantid": "fe4036f5-76ad-4232-9bda-313544c3ad54",
    "http://schemas.microsoft.com/identity/claims/objectidentifier": "86dfb10-ca60-4dc8-b8e5-67e0bada8dd8",
    "http://schemas.microsoft.com/identity/claims/identityprovider": "https://sts.windows.net/fe4036f5-76ad-4232-9bda-313544c3ad54/",
    "http://schemas.microsoft.com/claims/authnmethodsreferences": [
      "http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password",
      "http://schemas.microsoft.com/claims/multipleauthn"
    ],
    "http://schemas.microsoft.com/2012/01/devicecontext/claims/ismanaged": "true",
    "http://schemas.microsoft.com/2014/09/devicecontext/claims/iscompliant": "true",
    "http://schemas.microsoft.com/2014/02/devicecontext/claims/isknown": "true",
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname": "Mark",
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname": "Ryan",
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name": "mryan@welshgeek.net",
    "memberOf": ["Group-OEB", "ADSyncAdmins", "CertificateAuth", "Internet-ZPA-Enabled", "Zscaler", "Private Access - ALL"],
    "Country/Country": "CN",
    "samlassertion": null
  }
}
```

- **NameID:** Identifies the authenticated user (e.g., email address).
- **IdP EntityID:** Identifies the **Identity Provider (IdP)** that authenticated the user.
- **SAML Attributes:**

- **Tenant ID** – Identifies the organization within Zscaler.
- **Object Identifier** – Maps the user's unique identity.
- **Identity Provider** – Specifies which IdP authenticated the user.
- **Authentication Methods** – Details how the user authenticated (e.g., MFA, password, certificate).
- **Device Context Claims** – Provides information about the user's device (e.g., managed or unmanaged).
- **User Name & Group Memberships** – Defines the user's role and group-based access permissions.
- **Country Information** – Specifies the user's geographical location.
- **SAML Assertion**: Encapsulates additional security data required for authorization.

How Zscaler Uses SAML Responses

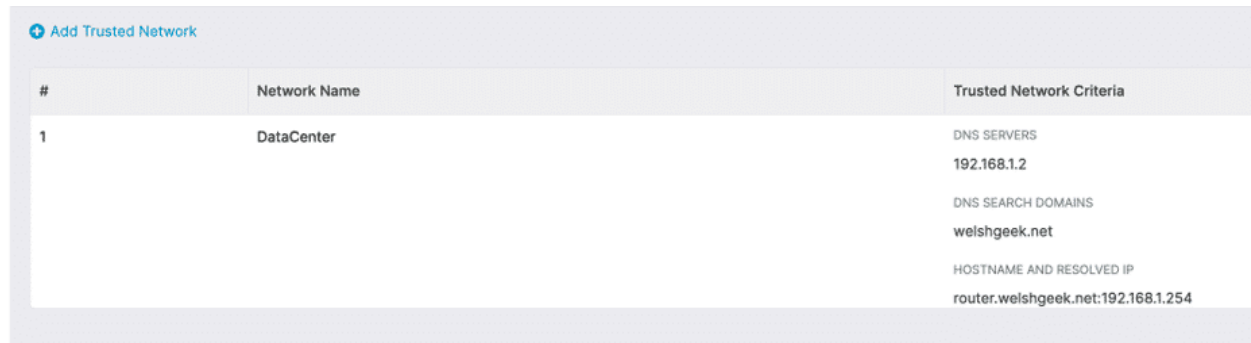
Zscaler's **SAML Service Providers (SPs)** for **Zscaler Internet Access (ZIA)** and **Zscaler Private Access (ZPA)** consume these attributes to enforce identity-based policies. Additionally, attributes synchronized from **ZIA's SAML SP to the Zscaler Client Connector Portal** are used for **entitlement management, policy enforcement, and seamless user access** to applications and resources.

Next: Trusted Networks – A Key Component of Device Posture

Now that we've explored how **SAML authentication responses enhance access control**, let's move on to the next essential feature: **Trusted Networks**, which further strengthens **Device Posture assessments** within the **Zero Trust Exchange**.

Trusted Networks: Strengthening Access Control

In today's **hybrid and remote work environments**, **trusted networks** play a vital role in implementing **effective access control policies**. As users connect from various locations, organizations need a mechanism to distinguish between **secure internal networks** and **untrusted external networks** to enforce appropriate security measures.



The screenshot shows a web interface titled "Add Trusted Network". It contains a table with three columns: "#", "Network Name", and "Trusted Network Criteria". There is one row in the table with the following data:

#	Network Name	Trusted Network Criteria
1	DataCenter	DNS SERVERS 192.168.1.2 DNS SEARCH DOMAINS welshgeek.net HOSTNAME AND RESOLVED IP router.welshgeek.net:192.168.1.254

What Are Trusted Networks?

A **Trusted Network** is a **secure and reliable network environment** that an organization designates as trustworthy. Users accessing resources from a **trusted network** may be granted different levels of access compared to those connecting from **untrusted or public networks**. This classification enables **dynamic policy enforcement**, ensuring that users receive appropriate access based on their network location.

Defining Trusted Network Criteria with Zscaler Client Connector

Zscaler Client Connector allows organizations to **define trusted networks** based on specific **network-related criteria**, ensuring security and policy enforcement. These criteria include:

- **DNS Server IP Addresses** – The IP addresses of DNS servers assigned to the client device.
- **DNS Search Domains** – The domains provided to the client device for **resolving internal resources**.
- **FQDN and IP Address Resolution** – Defining **Fully Qualified Domain Names (FQDNs)** and their corresponding IP addresses for validation.
- **Condition Match** – Defining whether a connection must meet **ANY or ALL** specified conditions to be classified as a **trusted network**.

Steps to Configure Trusted Networks in Zscaler Client Connector

To **set up and enforce trusted networks**, organizations typically follow these steps:

1. **Define DNS Server IP Addresses** – Specify the trusted **DNS servers** that client devices must use.
2. **Define DNS Search Domains** – Establish **search domains** that should be recognized within the network.
3. **Configure FQDN and IP Address Resolution** – Map **FQDNs** to specific **IP addresses** for validation.
4. **Set Condition Match** – Determine whether **ANY** or **ALL** conditions must be met for a network to be classified as **trusted**.

By implementing **trusted network policies** using **Zscaler Client Connector**, organizations can **enhance security, minimize unauthorized access, and enforce network-aware policies** while providing a seamless user experience.

Edit Trusted Network [X]

NETWORK DEFINITION

Network Name ⓘ
DataCenter

TRUSTED NETWORK CRITERIA

Add Condition ⓘ
Select [v] [Add Condition]

Condition Match
Any [v]

DNS Servers ⓘ
192.168.1.2 [X]

DNS Search Domains ⓘ
welshgeek.net [X]

Hostname ⓘ Resolved IPs For Hostname ⓘ
router.welshgeek.net 192.168.1.254 [X]

[Save] [Cancel]

Browser Access: Secure Application Access Without Client Installation

Browser Access enables secure user authentication and application access through a **web browser**, eliminating the need for users to install **Zscaler Client Connector** on their devices. This feature is particularly useful in scenarios where installing the **Client Connector** is not feasible or desirable.

When to Use Browser Access

Organizations may opt for **Browser Access** in cases such as:

- **Unmanaged or Unsupported Devices** – Providing access to applications on **operating systems** that are not currently supported by **Zscaler Client Connector**.
- **Third-Party Access** – Allowing **contractors, partners, or external vendors** to securely access applications without requiring device ownership or management by the organization.

How Browser Access Enhances ZPA

With **Browser Access**, organizations can:

- **Enable seamless access** to applications via any **modern web browser**, removing the need for **client installations, browser plugins, or additional configurations**.
- **Leverage existing Identity Providers (IdPs)** to authenticate users, including employees, **contractors, and third-party users**, without requiring them to maintain an **internet-facing application footprint**.

By integrating **Browser Access** with **Zscaler Private Access (ZPA)**, organizations can maintain **zero-trust security principles** while ensuring **secure, convenient, and policy-based access** for a diverse range of users.

Section Summary: Key Takeaways

Device Posture & Policy Access Control

Device Posture plays a crucial role in evaluating **security status** to enforce effective **policy-based access control**. It assesses key security factors such as **domain join status**, **registry checks**, **security configurations**, and **CrowdStrike ZTA scores** to determine device trustworthiness.

SAML Authentication Response

SAML enables **secure authentication** by facilitating the exchange of **identity and access attributes** between **Identity Providers (IdPs)** and **Service Providers (SPs)**. **Zscaler SAML SPs** use attributes like **NameID** and **IdP EntityID** to authenticate users and enforce access policies.

Trusted Networks

Zscaler Client Connector defines **trusted networks** based on **DNS settings**, **IP configurations**, and **FQDN resolutions**. These settings enhance **network security** by differentiating **trusted** and **untrusted** environments, allowing administrators to apply **dynamic access policies**.

Browser Access

Browser Access provides **secure authentication and application access via a web browser** without requiring **Zscaler Client Connector** installation. This is particularly useful for **unmanaged devices**, **contractors**, and **third-party users**, ensuring secure and seamless access to applications over **ZPA**.

Now that we've explored how **Device Posture** integrates with **connectivity and identity functionalities** within the **Zero Trust Exchange**, let's dive into our next **Platform Services** capability—**TLS/SSL Inspection**.

TLS/SSL Inspection

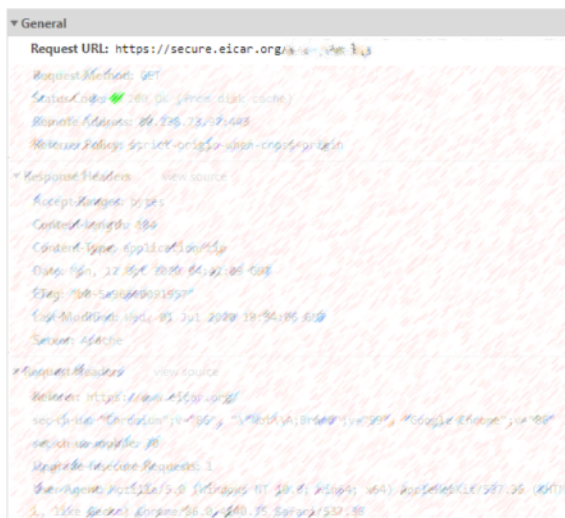
Understanding TLS Inspection

TLS Inspection, also known as **SSL Inspection**, is a critical cybersecurity measure that **decrypts and analyzes encrypted network traffic** to detect and prevent hidden threats. By intercepting **TLS-encrypted communications** between clients and servers, organizations can uncover potential risks, such as **malware infiltration, phishing attempts, or data exfiltration**, that may otherwise go undetected within encrypted connections.

One of the most significant distinctions in network security is the difference between an **encrypted HTTPS transaction** and a **decrypted HTTPS transaction**. While **encrypted traffic** ensures privacy, it can also **conceal malicious activity**, making inspection essential for enforcing security policies and safeguarding sensitive data.

Encrypted HTTPS Transaction

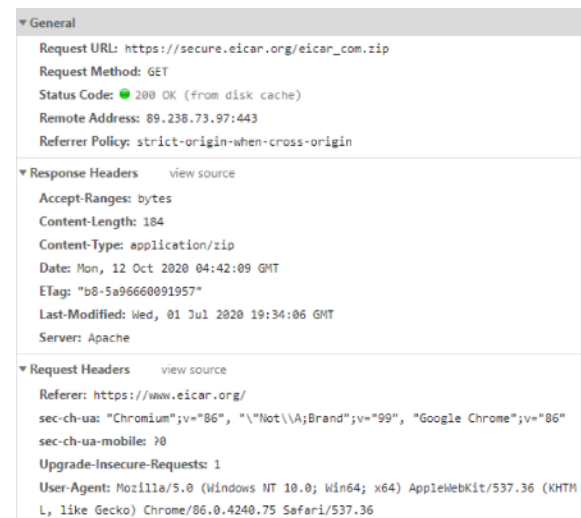
When an HTTPS transaction is encrypted, it becomes unreadable to anyone who tries to view it. However, the Server or Domain Name can still be seen without inspection during a TLS Handshake. This is the only piece of information that is visible to a viewer.



Decrypted HTTPS Transaction

When you decrypt an HTTPS transaction or TLS, the following becomes visible:

- HTTP Headers
- Request and Response Headers
- Full Request URL
- Request Method
- **All of the Payload**



Why SSL Inspection ?



2024 Zscaler, Inc. All rights reserved

1. **Network Visibility & Risk Control:** Gaining insights into user activity allows organizations to **enforce acceptable use policies, optimize network performance, and mitigate risks effectively**. By inspecting traffic and implementing adaptive controls, organizations can better manage potential threats.
2. **Compliance with Security Policies:** Many organizations have strict security policies that mandate **monitoring and controlling all inbound and outbound traffic**. Without SSL inspection, encrypted traffic remains unchecked, increasing the risk of policy violations and regulatory non-compliance.
3. **Preventing Data Loss:** SSL inspection helps **detect and prevent unauthorized data exfiltration** by monitoring encrypted traffic for **sensitive information leaks**. This ensures that confidential data, such as credit card numbers and proprietary documents, are not transmitted improperly.
4. **Enhanced Endpoint Security:** Even if a device is compromised, SSL inspection can **block malicious communication** between infected endpoints and external threat actors, limiting the impact of cyberattacks.
5. **Restricting Access to Specific Tenants:** Organizations can control access to designated **cloud service tenants** (e.g., **Microsoft 365, Google Workspace, or other SaaS applications**) to **prevent unauthorized access or data movement across instances**.
6. **Protection Against Encrypted Cyber Threats:** Advanced cyberattacks, such as **ransomware, phishing, and command-and-control (C2) communications**, often rely

on encrypted channels to evade detection. Since **most internet traffic is now HTTPS-encrypted**, traditional security tools struggle to inspect it. **SSL inspection decrypts this traffic, enabling security solutions to detect and block hidden threats.**

SSL vs TLS: Understanding the Difference

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols that **encrypt and secure data transmission between two endpoints**. However, there are key differences between them.

SSL was originally developed by Netscape in the mid-1990s, with **SSL 3.0 released in 1996**. Over time, **vulnerabilities in SSL**—such as its susceptibility to **man-in-the-middle attacks**—led to its deprecation. The **Internet Engineering Task Force (IETF) officially discontinued SSL in 2015** due to security weaknesses.

TLS was introduced as an improved version of SSL. **TLS 1.0 was released in 1999**, and the latest version, **TLS 1.3, was adopted in 2018**. TLS 1.3 enhances security by **removing outdated cryptographic algorithms and improving handshake efficiency**, making it the most secure version to date.

Why People Still Say “SSL”

Even though **SSL is no longer supported**, the term “**SSL**” is **still widely used** as a general reference to cryptographic protocols. Many still refer to “**SSL/TLS**” or “**SSL Inspection**” when discussing encrypted traffic, even though **TLS is the protocol currently in use**.

To maintain clarity:

- **“TLS” will be used to describe the actual protocol that secures communication.**
- **“SSL Inspection” remains the commonly used term for inspecting encrypted TLS traffic.**

Zscaler and TLS Decryption

As part of **Zscaler's Platform Services suite**, **TLS Decryption (or TLS Inspection)** plays a critical role in **Access Control, Cyber Protection, and Data Protection** by allowing organizations to **analyze and enforce security policies** on encrypted communications.

Why is TLS Decryption Important?

With **85–90% of all internet traffic now encrypted**, attackers increasingly use **TLS encryption to conceal threats**. Without decryption, organizations **cannot see inside encrypted traffic**, creating blind spots that **allow malware, phishing attacks, and data exfiltration to go undetected**.

To illustrate the importance of TLS decryption, consider this real-world example:

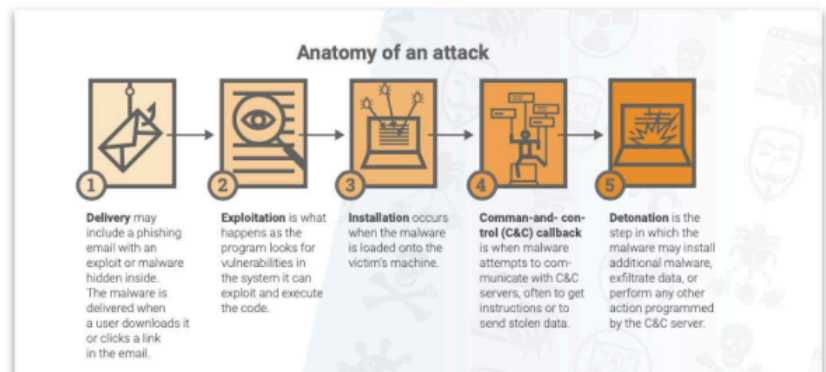
- **A user downloads a PDF from Google Drive using Google Chrome.**
- **Zscaler decrypts and inspects the file in real-time.**
- **If the file contains malware, Zscaler detonates and analyzes it before delivery.**
- **If the file contains sensitive data, Zscaler enforces data protection policies to prevent leaks.**

This inspection process ensures **malicious threats are stopped before they reach the user**, while also **protecting sensitive data from unauthorized sharing**.

The Growth of Encrypted Traffic & Threats

Several factors have contributed to the **explosive increase in encrypted internet traffic**:

- **Non-HTTPS websites now trigger security warnings, encouraging universal TLS adoption.**
- **Services like “Let’s Encrypt” have made it easy for any website to implement TLS encryption.**
- **Protocols such as HTTP/2 require TLS, further increasing encrypted traffic volumes.**



The Zscaler cloud identified and stopped 20 billion threats hidden inside encrypted traffic.

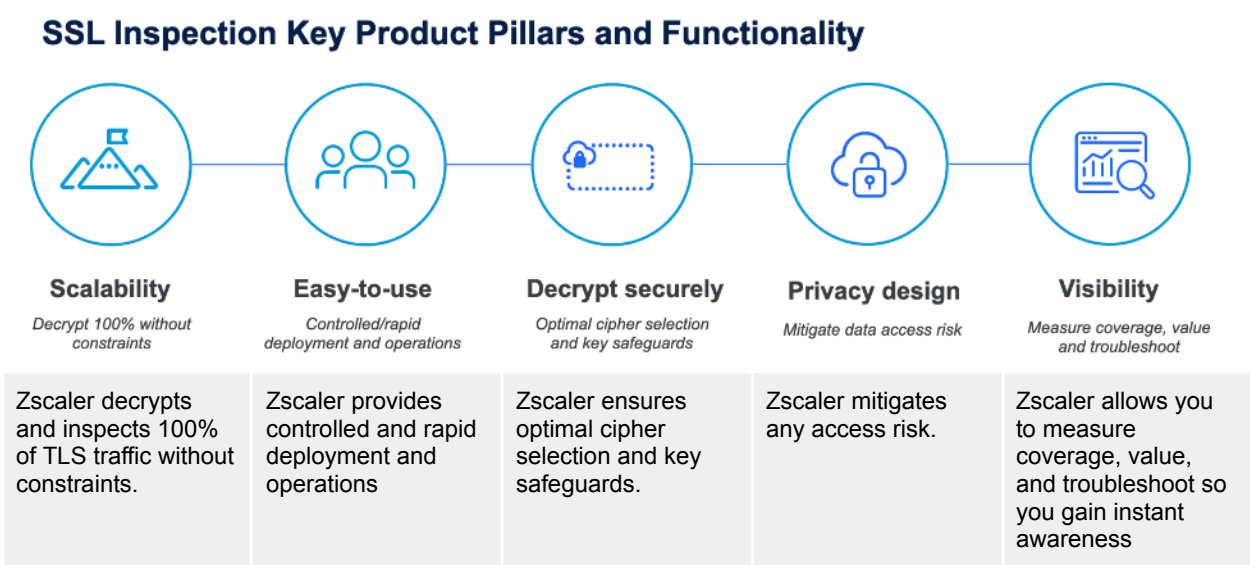
While TLS provides **critical privacy and security benefits**, it also **creates blind spots** that cybercriminals exploit. **Threat actors use encrypted channels to launch attacks, distribute malware, and exfiltrate sensitive data** without detection.

Zscaler ThreatLabz & Encrypted Threat Reports

Every year, **Zscaler ThreatLabz publishes “The State of Encrypted Attacks” report**, revealing a **year-over-year increase in threats hidden within encrypted traffic**. This underscores the need for **effective TLS inspection to prevent sophisticated attacks** while maintaining privacy and security.

TLS Inspection Pillars and Functionalities

Zscaler understands that achieving a **strong security posture and full visibility** into **applications and threats** is only possible with **comprehensive TLS Inspection**. To support this, Zscaler has established **key TLS Inspection pillars and functionalities** designed to **enhance security, enforce compliance, and prevent encrypted threats** from bypassing detection.



TLS inspection within the **Zero Trust Exchange** plays a crucial role in **access control**, **compromise prevention**, **data loss protection**, and **SSL inspection** across **Zscaler Internet Access (ZIA)** and **Zscaler Private Access (ZPA)**. This includes **SSL interception**, **certificate validation**, and security enforcement in both **forward and reverse proxy** scenarios.

The diagram illustrates the three pillars of Zero Trust:

- Control Access**: Represented by a shield icon with a flame. It includes URL Filtering, Cloud Firewall, Bandwidth Control, and DNS Security.
- Prevent Compromise**: Represented by a person icon with a shield. It includes Malware Protection, Cloud Sandbox, Advanced Threat Protection (IPS), and Cloud Browser Isolation.
- Prevent Data Loss**: Represented by a database icon with a lock. It includes Inline DLP, Granular App Controls, Tenancy Restrictions, and File Type Controls.

A central cloud icon labeled "SSL Inspection at Scale" is connected to all three pillars. A red arrow points from the cloud to the "Prevent Data Loss" pillar. Below the cloud, a blue bar contains binary code (0s and 1s) and a padlock icon. In the bottom right corner, there is a red box with a skull and crossbones icon, indicating a security threat or breach.

Zscaler categorizes sites based on their security risk levels. **Trusted sites** are granted access with minimal restrictions, while **high-risk sites** may require **conditional access**, additional security measures, or be **denied entirely**. URL filtering, cloud firewall policies, and contextual security checks allow organizations to enforce precise access controls on web traffic.

TLS inspection plays a key role in preventing compromises by analyzing **traffic payloads**. Security features such as **malware inspection**, **Advanced Threat Protection (ATP)**, **Intrusion Prevention System (IPS) signatures**, and **cloud sandboxing** help identify and block threats before they reach users. Additionally, TLS inspection enables detection and disruption of **command-and-control (C2) traffic**, preventing compromised devices from communicating with malicious servers. Zscaler also leverages **session isolation** to safeguard users and web applications from potential attacks.

Data Loss Protection (DLP) and Application Controls

Inline DLP scanning ensures that sensitive information is not leaked or exfiltrated, either accidentally or through malicious intent. Granular **application controls** extend beyond simple URL filtering, allowing enforcement of security policies based on **full URIs, file types, and tenancy restrictions**. For example, Zscaler can limit access to specific **Microsoft 365 tenants**, preventing unauthorized data sharing across multiple instances. Additionally, sandboxing ensures that potentially harmful files are **analyzed before execution**, adding an extra layer of security.

Scalability and Performance

The **Zscaler Zero Trust Exchange** is built to **handle 100% SSL traffic**, ensuring **real-time decryption and inspection** at scale. By **dynamically generating intermediate certificates** at high speed, Zscaler maintains security without degrading user experience. This enables organizations to enforce **consistent, high-performance security policies** across all users and locations, securing encrypted traffic **without bottlenecks or blind spots**.

SSL Inspection as a Forward Proxy in Zscaler Internet Access

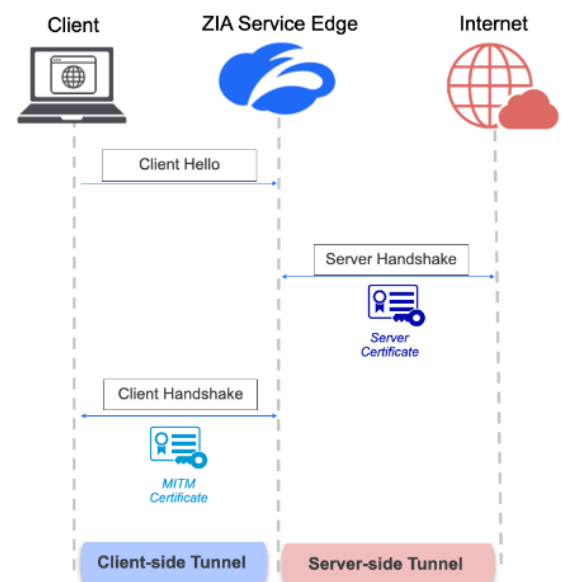
In **Zscaler Internet Access (ZIA)**, acting as a **forward proxy**, **SSL inspection** is performed using a **man-in-the-middle (MITM)** approach to analyze encrypted traffic securely.

When a **client requests access to a website**, the **Zscaler Service Edge** intercepts the request and establishes a connection with the destination **web server** on the client's behalf. Upon receiving the **server certificate**, Zscaler performs **validation checks** to ensure:

- The certificate is **signed by a trusted certificate authority (CA)**
- The **certificate's expiration date** is valid
- The **issuer information** is legitimate
- The **certificate contents** comply with security policies

Once validated, Zscaler **dynamically generates a certificate on the fly**, signed by a trusted **Zscaler root CA**, and presents it to the **client device**. From the client's perspective, it appears as though they are communicating directly with the web server. However, Zscaler acts as an **intermediary**, decrypting and inspecting the traffic before securely forwarding it to the actual destination.

This **man-in-the-middle (MITM) SSL inspection** allows organizations to **enforce security policies, detect threats, and prevent data loss** within encrypted communications while maintaining trust and security compliance.



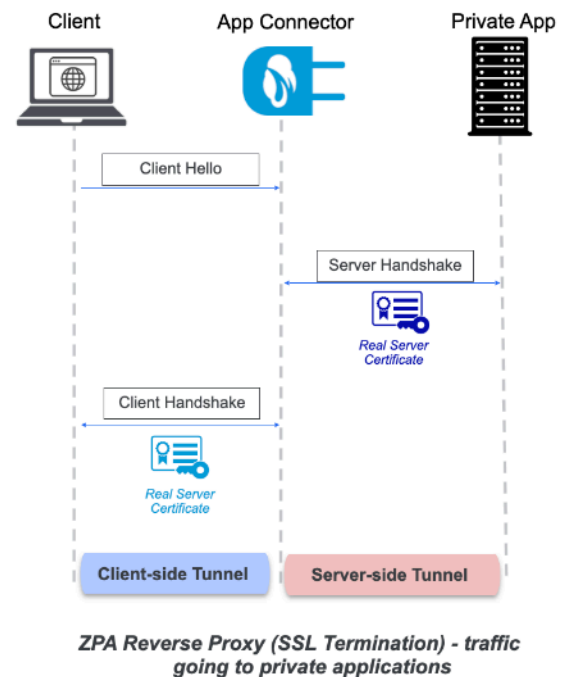
ZIA Forward SSL Proxy (MITM) - traffic going to the Internet

SSL Inspection as a Reverse Proxy in Zscaler Private Access

In **Zscaler Private Access (ZPA)**, SSL inspection functions differently compared to **Zscaler Internet Access (ZIA)**. Instead of acting as a **forward proxy**, **ZPA operates as a reverse proxy**, effectively becoming the **web server** that the user connects to.

When a **user attempts to access an internal application**, the **ZPA Service Edge** intercepts the request and establishes an **SSL handshake** with the client. This involves:

1. **Client Hello Request:** The user's device initiates a connection request to ZPA, believing it is the destination web server.
2. **Connection from App Connector to Application:** The ZPA **App Connector**, deployed in the private environment, reaches out to the actual application server to establish a secure connection.
3. **Retrieving the Service Certificate:** The **real service certificate** from the private application is provided to the **App Connector**.
4. **Certificate Presentation to Client:** The App Connector (or the ZPA Service Edge) presents a valid service certificate back to the **client device**.

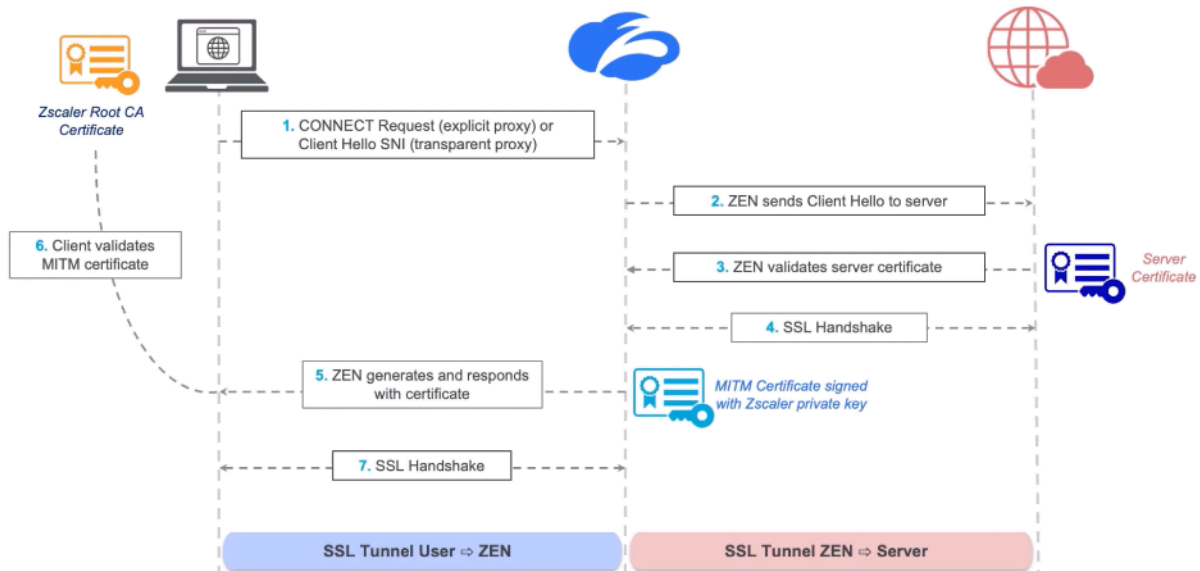


Depending on the configuration, the certificate presented to the client may either be:

- The **original certificate** from the application server.
- A **certificate uploaded to the ZPA platform**, allowing Zscaler to securely proxy and control access to private applications.

Let's dig in a little bit deeper into how Zscaler Internet Access SSL inspection works.

How does ZIA SSL Inspection/SSL Proxy Work?



How ZIA SSL Inspection Works

SSL inspection in **Zscaler Internet Access (ZIA)** enables **deep packet inspection of encrypted traffic**, ensuring visibility into threats and policy enforcement while maintaining a secure connection. Here's how it works step by step:

Step 1: Client Request to the Proxy

- A user initiates a **connection request** through their browser or application.
- In an **explicit proxy setup** with a **PAC file**, the request uses the **CONNECT method**, such as `CONNECT www.google.com`.
- In a **transparent mode** using **Zscaler Client Connector**, the client first **resolves the domain via DNS**, establishes a **TCP 443 connection**, and sends a **Client Hello** as part of the SSL handshake.
- The **Client Hello** includes the **Server Name Indication (SNI)**, which identifies the intended destination website.

Step 2: ZIA Service Edge Intercepts the Request

- The **ZIA Public or Private Service Edge** (previously known as ZEN) intercepts the **Client Hello** and extracts the **Fully Qualified Domain Name (FQDN)** being accessed.
- The Service Edge then initiates its own **Client Hello** to the destination web server.

- It completes the **SSL handshake** and retrieves the **server's certificate** from the target website.

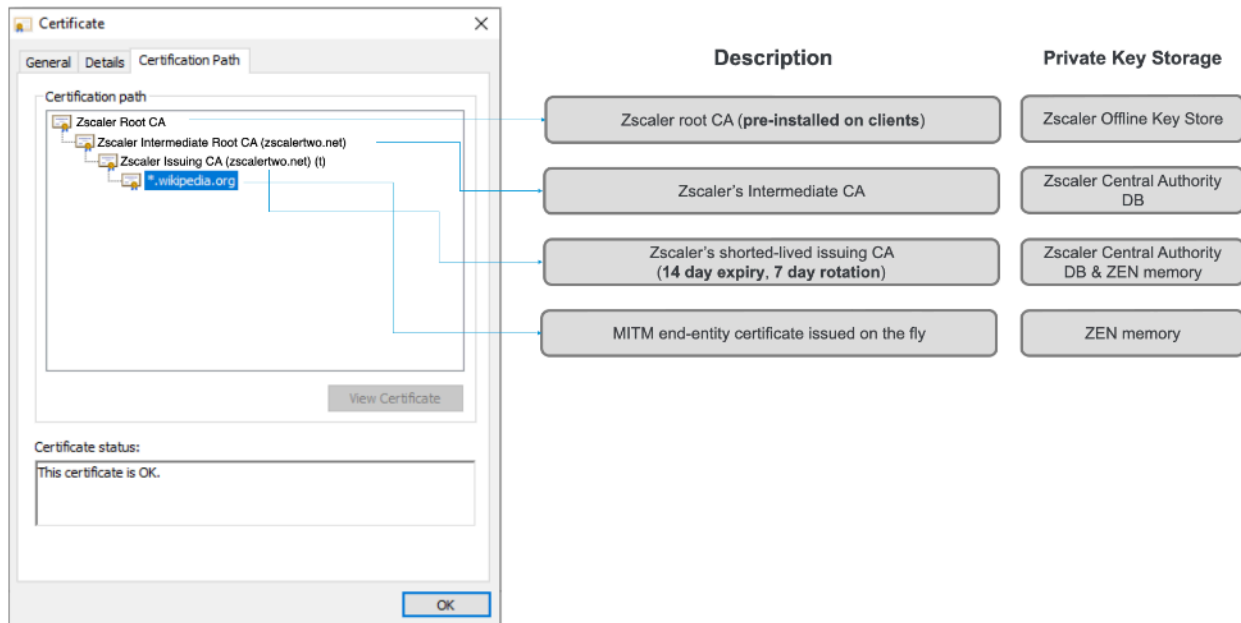
Step 3: Certificate Validation & Policy Enforcement

- **Zscaler validates the certificate** received from the web server by checking:
 - Whether it is signed by a **trusted Certificate Authority (CA)**.
 - Whether the **Common Name (CN)** or **Subject Alternative Name (SAN)** matches the requested domain.
 - Whether the certificate's **expiration date** is still valid.
- Based on **security policies**, Zscaler **allows, blocks, or applies conditional access** to the transaction.
- If the request is allowed, Zscaler **generates a certificate on the fly**, signed by either:
 - **Zscaler's default CA** (for organizations using Zscaler's built-in SSL inspection).
 - A **private enterprise CA** (for organizations using their own root CA uploaded to Zscaler).

Step 4: Issuing a Man-in-the-Middle Certificate

- **ZIA generates a temporary, spoofed certificate** that mimics the original certificate but is issued by **Zscaler's intermediate CA**.
- The **temporary intermediate CA certificate**:
 - Has a **14-day expiration** and is rotated every **7 days**.
 - Is **only stored in memory** within the **Zscaler Central Authority** and distributed securely to **ZIA Public/Private Service Edges**.
 - Is never exposed externally for security reasons.

Certificate Chain with SSL Inspection



Step 5: SSL Handshake with the Client

- Zscaler **presents the spoofed certificate** back to the **client application** (browser, endpoint, or mobile app).
- The client validates the certificate **against the root CA configured on the endpoint**.
- If the **Zscaler root CA** (or the organization's custom CA) is **trusted**, the handshake is successfully completed.

Step 6: Secure, Dual SSL Connections Established

- At this point, there are **two separate encrypted SSL connections**:
 1. **Client ↔ ZIA Service Edge**: The client thinks it is communicating directly with the website, but the connection is being managed by Zscaler.
 2. **ZIA Service Edge ↔ Destination Web Server**: A secure connection is maintained between Zscaler and the web server.
- Zscaler **inspects the traffic in real-time**, scanning for **malware, data loss, and threats** before securely relaying the traffic.

Step 7: Handling Custom Certificates & Enterprise CA Integration

- If an organization chooses to use its **own CA for SSL inspection**, Zscaler **never stores private keys externally**.
- Instead:
 - The **private CA key remains within the organization**.
 - The organization issues an **intermediate CA certificate** to Zscaler.

- This **intermediate CA certificate** is securely uploaded to **Zscaler's Central Authority** and used to issue **temporary SSL inspection certificates**.

Conclusion: Why ZIA SSL Inspection Matters

With **more than 85% of internet traffic being encrypted**, **cybercriminals exploit HTTPS traffic** to conceal malware, ransomware, and data theft. **ZIA SSL Inspection enables organizations to:**

- Detect **hidden threats within encrypted traffic**
- Enforce **data loss prevention (DLP) policies**
- Apply **granular access controls and tenant restrictions**
- **Ensure compliance** with corporate security policies

By performing **real-time SSL inspection at scale**, Zscaler ensures **secure internet access without introducing latency**, protecting organizations from modern **cyber threats hidden in encrypted communications**.

A Five-Phase Approach to Deploying TLS Inspection

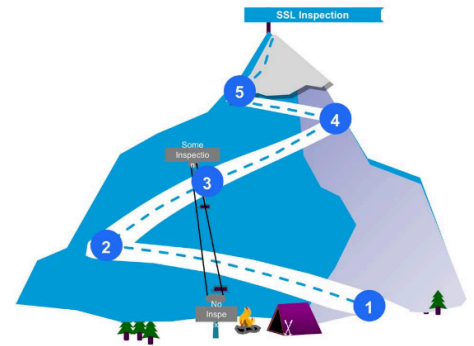
Deploying **TLS (SSL) Inspection** is a structured process that follows **five key phases** to ensure **smooth implementation, minimal disruptions, and maximum security benefits**. Each phase plays a critical role in aligning the deployment with business needs while addressing technical challenges and user concerns.

Phase 1: Preparation & Organizational Alignment

Before deploying **TLS decryption**, it's crucial to **gain internal agreement** within the organization. The goal of **SSL inspection** is not to monitor user activity but to **protect the business** from malware infections, data leaks, and compliance violations. Key preparatory steps include:

- **Defining an Acceptable Use Policy (AUP)** – Clearly communicating what will be inspected and why.
- **User Notifications & Transparency** – Informing employees about the inspection process.
- **Stakeholder Buy-in** – Securing approval from legal, compliance, and IT leadership.

- 1 Pre-work
- 2 Root CA Enrollment
- 3 Initial Roll-out
- 4 Measure & Report
- 5 Extended Roll-out



Phase 2: Certificate Authority (CA) Deployment

To perform **SSL inspection**, organizations must ensure that **all devices trust the intermediate certificate** issued by the **Zscaler Certificate Authority (Zscaler CA)** or a **custom enterprise CA**. Steps in this phase include:

- **Distributing the Root CA** – Rolling out the **trusted CA certificate** to managed devices using **Group Policy (GPO), MDM, or script-based deployment**.
- **Handling Unmanaged & BYOD Devices** – Using **browser-based prompts, enterprise MDM solutions, or Cloud Browser Isolation (CBI)** for untrusted devices.
- **Validating Trust** – Ensuring users don't receive SSL errors when accessing inspected websites.

Phase 3: Initial Deployment & Pilot Testing

A **small-scale rollout** allows IT teams to **identify and resolve potential issues** before a full-scale deployment. This phase involves:

- **Testing with a Limited User Group** – Rolling out SSL inspection to a select set of employees (e.g., IT teams, security analysts).

- **Selective Category-Based Inspection** – Applying TLS decryption only to specific traffic categories (e.g., high-risk sites, personal storage, file-sharing).
- **User Feedback & Issue Resolution** – Collecting input from pilot users to **fine-tune** inspection policies.

Phase 4: Extended Rollout & Issue Mitigation

Once the pilot is successful, the **broader rollout** begins. This phase focuses on addressing **technical challenges** and expanding TLS decryption across the organization. Key considerations include:

- **Handling Certificate Pinning** – Managing applications (e.g., banking apps, secure developer environments) that reject SSL inspection.
- **Addressing Developer & IoT Environments** – Ensuring **mission-critical applications** function without disruption.
- **Optimizing Policies for SaaS & Cloud Services** – Implementing **TLS bypasses for Office 365, Google Workspace, and other trusted services** to maintain performance.
- **Scaling Across Business Units** – Expanding deployment to **remote workers, branch offices, and cloud workloads**.

Phase 5: Monitoring, Measuring, & Optimizing

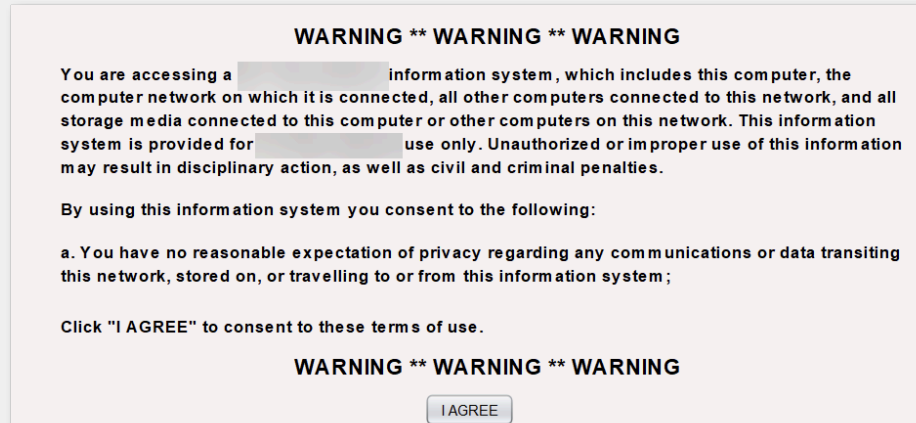
After the **full rollout**, organizations must continuously **monitor, measure, and optimize** SSL inspection to maximize security benefits. This includes:

- **Tracking Decryption Volume** – Measuring **how much traffic is being inspected and which services require SSL decryption**.
- **Quantifying Business Impact** – Reporting on:
 - **Malware prevented through SSL inspection.**
 - **Data Loss Prevention (DLP) incidents blocked.**
 - **Threats neutralized within encrypted traffic.**
- **Analyzing TLS Versions & Cipher Suites** – Understanding **encryption trends** to stay ahead of evolving security risks.
- **Iterative Policy Refinement** – Adjusting policies based on **security analytics and emerging threats**.

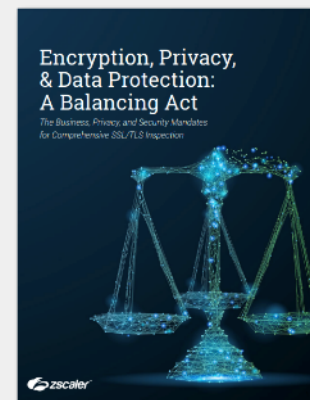
Next we will take a more detailed look at this process:

(1) Pre-Work

Before deploying **SSL inspection**, it is critical to align organizational stakeholders and ensure there is agreement on its purpose. SSL inspection is not about monitoring user activity but rather about safeguarding the business from malware, preventing data leaks, and protecting corporate reputation. Defining an **acceptable use policy (AUP)** and establishing clear user notifications help set expectations and transparency around its implementation.



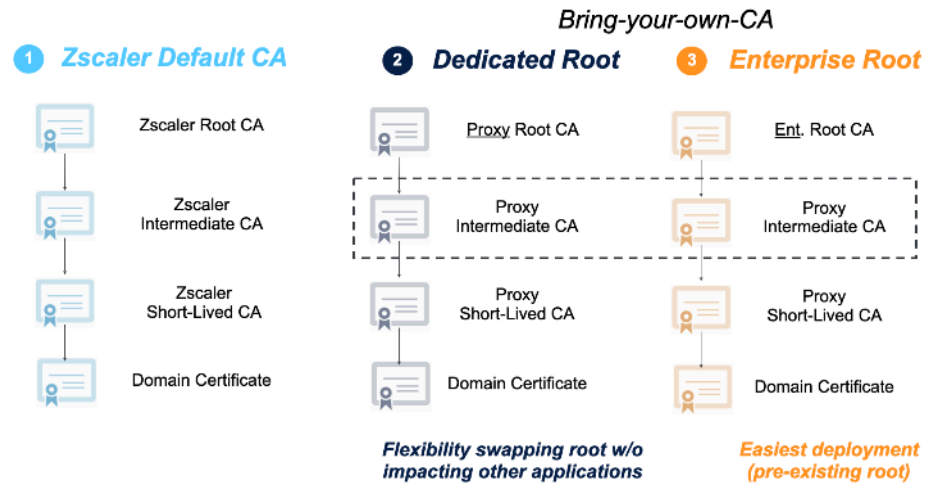
Gaining buy-in from **legal, privacy, and security teams** early in the process is essential to address concerns and regulatory requirements. Misconceptions about SSL inspection, such as fears of user surveillance, can create roadblocks, particularly in regions with **worker councils** or strict privacy regulations. A clear, organization-wide understanding should emphasize that **TLS inspection enhances security** by analyzing encrypted traffic without storing payload content, ensuring **malware prevention, data protection, and blocking of command-and-control communications**.



Lastly, **effective user communication** is key. Updating the **acceptable use policy**, sending user notifications, and providing guidance on how SSL inspection works will help users understand its role. Employees should know whether their traffic is being inspected and how this impacts their browsing choices on corporate devices.

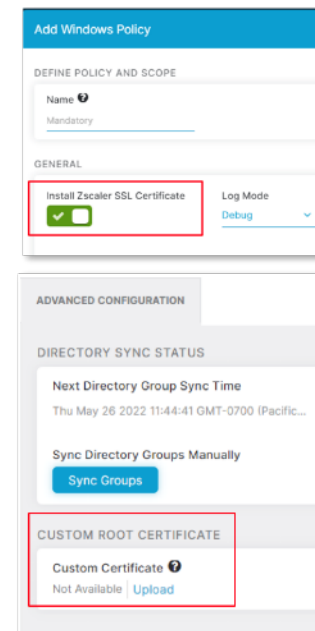
(2) Root CA Enrollment

Once organizational buy-in is secured, the next step is deploying the **root certificate authority (CA)** to ensure all client devices trust the certificates used for SSL inspection. By default, Zscaler provides its own **root CA**, which establishes a **Chain of Trust** from the **intermediate certificate** to a **short-lived temporary certificate**, and finally, the **spoofed web server domain certificate** issued on the fly.



Organizations also have the option to **bring their own CA**, following one of two approaches. The first is a **dedicated root CA**, where a separate offline CA is created specifically for **SSL inspection**. This provides full control over the **Chain of Trust**, allowing organizations to replace or manage certificates as needed. The second approach is leveraging an **existing enterprise root CA**, such as the one included with **Active Directory**. Since all domain-joined devices inherently trust the enterprise CA, this method simplifies certificate deployment by generating an **intermediate CA** and uploading it to Zscaler.

Deploying certificates is straightforward. The **Zscaler Client Connector** can automatically install the **Zscaler SSL certificate** on endpoints. Alternatively, administrators can **upload a custom root certificate** to the **Zscaler Client Connector Portal**, ensuring that both the **Zscaler root CA** and the organization's **custom CA** are installed seamlessly on managed devices.

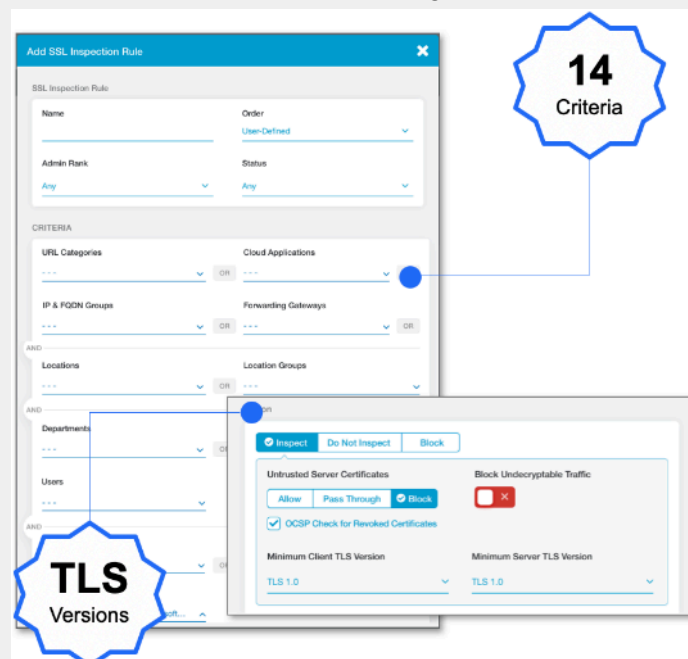


Client Connector Insta

(3) Initial Roll-Out

After establishing a baseline, the next step is rolling out **SSL inspection** for a **select group of users** and categories while collecting feedback on their experience. This pilot phase starts with configuring a **granular policy framework** to ensure inspection rules are applied selectively without disrupting critical applications.

Zscaler's **granular rule-based engine** allows policies to be defined based on **users, groups, departments, destination IPs, FQDN groups, and device attributes** such as OS and trust level. This ensures that applications with **certificate pinning** are not unintentionally broken. Policies can also enforce **secure TLS usage** by setting minimum TLS versions, validating certificates, performing **OCSP revocation checks**, and blocking untrusted or undecryptable traffic.



A **pilot rule set** typically includes inspecting specific categories for a **pilot SSL user group**, blocking untrusted certificates, enforcing **TLS 1.0+**, and ensuring that default rules **do not inspect traffic unless explicitly required**. Higher-level rules prioritize **bypassing inspection for Microsoft 365 services** like **OneDrive and SharePoint**, using **Zscaler's One-Click exemption** to prevent known application issues.

It's also critical to **manage non-standard protocols** like **Google QUIC (UDP 443)** and **Apple Private Relay**, which bypass standard SSL inspection. Blocking these within the firewall forces traffic to **fall back to HTTPS over TCP 443**, ensuring full inspection coverage. As the rollout progresses, the focus remains on fine-tuning rules to accommodate

applications and client environments that may present **inspection challenges**.

Rule Order	Rule Name	Criteria	Action
1	Zscaler Proxy Traffic	DESTINATION IP CATEGORIES Zscaler Proxy IPs NETWORK SERVICES Zscaler Proxy Network Services	Allow
2	Office 365 One Click Rule	DESTINATION IP CATEGORIES Office 365	Allow
3	Recommended Firewall Rule	NETWORK SERVICES DNS; HTTP; HTTPS	Allow
4	Block QUIC	NETWORK SERVICES QUIC	Block/Drop
Default	Default Firewall Filtering Rule	Any	Block/Drop

If sending UDP traffic to Zscaler, drop QUIC in the Cloud Firewall

Chrome | chrome://flags

Experimental QUIC protocol

Enable experimental QUIC protocol support. – Mac, Windows, Linux, Chrome OS, Android, Fuchsia

#enable-quic

Disabled

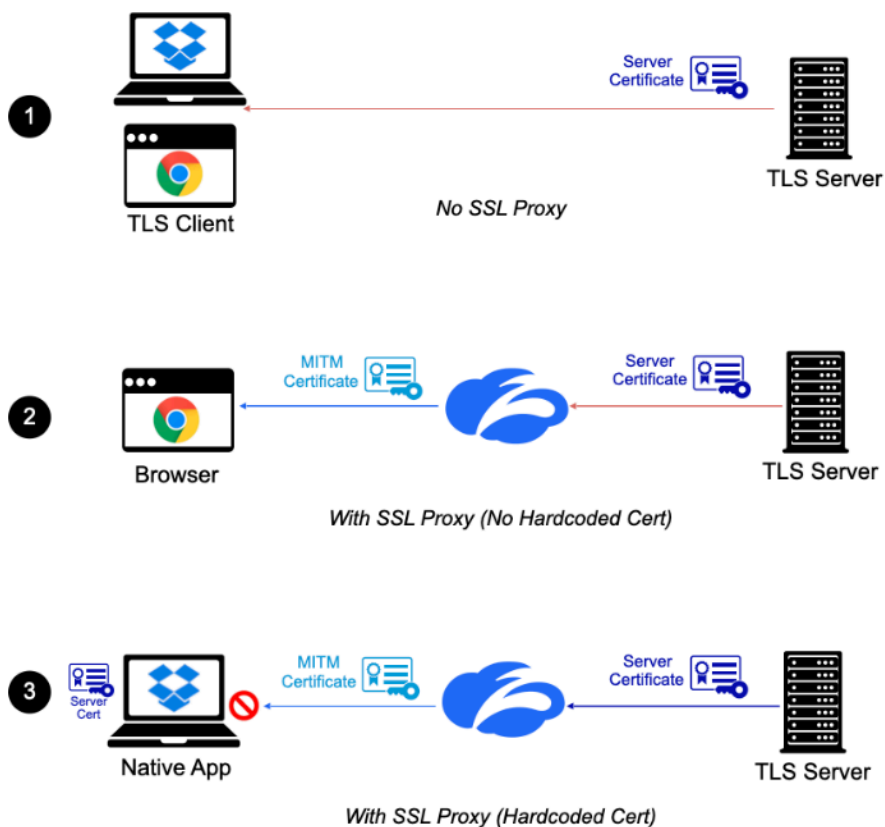
Disable QUIC on the client using Chrome flags (Chrome Enterprise Cloud Management)

(4) Extended Roll-Out

At this stage, we address deeper challenges that may arise, such as **certificate pinning**, handling **developer and IoT environments**, and managing policies for services like **Microsoft 365**.

Certificate pinning occurs when an application expects a specific certificate and rejects any other, including the **man-in-the-middle** certificate provided by Zscaler for SSL inspection. This results in **connection failures**, as seen with apps like **Dropbox**, where the client software expects a predefined certificate, while the web version continues to function. Since **iOS and Android** commonly use certificate pinning, organizations must either **configure clients to trust Zscaler-issued certificates or bypass inspection** for affected applications. DigiCert even recommends avoiding certificate pinning due to its potential impact on security management.

Certificate pinning/Hardcoded certificates:



Troubleshooting certificate pinning issues starts with a **packet capture**, which helps identify if a client closes the connection immediately after receiving a certificate—indicating it **does not trust the certificate**. Additionally, **SSL logs within the Zscaler administration interface (now known as ZIA Admin Portal)** can reveal handshake failures, confirming inspection issues.

To resolve this, organizations can **create policies** that bypass SSL inspection based on **operating system, application type, or user agent behavior**. For example, if an **Android or iOS device connects to a known pinned certificate application with an unrecognized user agent**, a policy can be enforced to exclude that traffic from inspection while maintaining security for other connections.

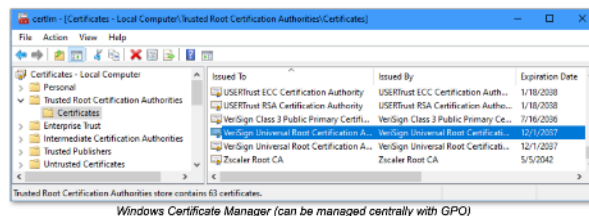
Hardcoded certificates: How to identify?

The diagram illustrates the process of identifying hardcoded certificates. It starts with a screenshot of the Signal Native App for Windows 10 (64 bit) showing an error message: "Something went wrong! Failed to connect to server. Try again". A blue arrow points to a network packet capture (tcpdump) showing a failed connection attempt. The packet capture shows a sequence of events: a successful connection to chat.signal.org:443, followed by a TLS handshake, and then a failure to connect to the server. The failure is indicated by a red box highlighting the packet details: "Signal refuses the MITM certificate and terminates the TCP connection (not TLS alert packet)".

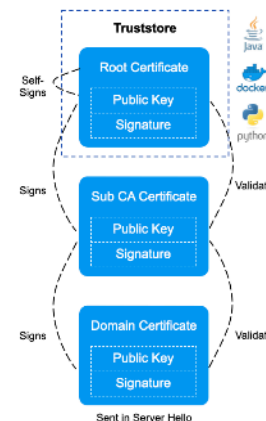
The diagram illustrates the process of identifying hardcoded certificates. It starts with a screenshot of the Signal Native App for Windows 10 (64 bit) showing an error message: "Something went wrong! Failed to connect to server. Try again". A blue arrow points to a network packet capture (tcpdump) showing a failed connection attempt. The packet capture shows a sequence of events: a successful connection to chat.signal.org:443, followed by a TLS handshake, and then a failure to connect to the server. The failure is indicated by a red box highlighting the packet details: "Signal refuses the MITM certificate and terminates the TCP connection (not TLS alert packet)".

Applications with customer truststores: What are they?

- Every OS has a default system root CA certificate store (root-of-trust)
- Some applications have a custom trust store (e.g. Firefox, Python, Developer Environments)
- Zscaler root CA certificate must be pre-deployed in trust store for MITM to work (establish chain-of-trust)



Windows Certificate Manager (can be managed centrally with GPO)

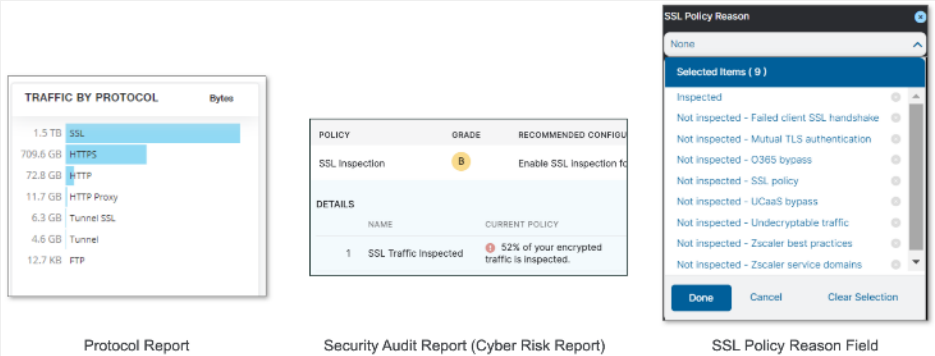


(5) Measure & Report

Throughout the rollout, it is essential to **measure and report on the impact of SSL inspection** to demonstrate its value to the business. Key metrics include the **amount of SSL traffic inspected, the volume of decrypted data, and the number of malware threats or data loss prevention (DLP) incidents identified**. These insights help validate the decision to implement inspection and assess its effectiveness.

Additionally, monitoring **TLS versions and cipher usage** over time provides visibility into security trends and evolving encryption standards. Organizations can track these changes to ensure compliance with best practices and adapt policies as needed.

To evaluate the success of SSL inspection, organizations should leverage key reporting tools, including the **Protocol Report, Security Audit Report (Cyber Risk Report), and the SSL Policy Reason field**, which provide critical insights into inspection outcomes, risk mitigation, and policy enforcement.



Conclusion

A well-structured, phased approach to **TLS inspection deployment** ensures a seamless transition, minimizes disruptions, and strengthens security across the organization. By gradually rolling out **SSL decryption**, businesses can mitigate threats hidden in encrypted traffic while maintaining compliance and transparency with users.

Key Takeaways:

- **TLS/SSL Inspection Overview:** TLS/SSL inspection decrypts and analyzes encrypted network traffic to detect and block malicious activities, strengthening overall security.
- **Zscaler and TLS Decryption:** Zscaler's **Platform Services** enable scalable TLS inspection without compromising performance, applying access control, cyber protection, and data protection policies.
- **Strategic Deployment:** A structured rollout involves deploying **certificate authorities**, conducting **pilot testing**, addressing **challenges like certificate pinning**, and refining policies based on continuous monitoring.
- **Core Functionalities & Impact:** TLS inspection ensures **secure communication** by enabling access control, **compromise prevention**, and **data loss protection**, safeguarding organizations from hidden threats.

By implementing a **comprehensive TLS inspection strategy**, organizations can gain **full visibility into encrypted traffic, enforce security policies, and reduce cyber risks without impacting performance**.

TLS Version and Cipher Visibility

Zscaler supports **hardware-based TLS inspection** for versions **1.3, 1.2, 1.1, and 1.0**, along with **Perfect Forward Secrecy (PFS) Cipher Suites** across all TLS versions. The **Internet & SaaS Public Service Edge** prioritizes the highest **TLS version** and strongest **Cipher Suites** for both **client-to-Service Edge** and **Service Edge-to-server** connections.

Zscaler does **not inspect traffic** for websites that use **unsupported TLS protocols**. Instead, this traffic is classified as **undecryptable** and is either **allowed or blocked** based on the organization's **SSL inspection policy**.

Extended SSL Cipher Visibility

Zscaler provides **deep insights into encrypted SSL traffic**, allowing organizations to monitor and manage SSL/TLS security settings. The following **SSL Cipher Web Insights** filters now apply to encrypted traffic (**Analytics > Web Insights > Logs**):

- **Certificate Expiry**
- **Cipher Certificate Validations**
- **Client Connection Ciphers**
- **Client Connection TLS Version**
- **OCSP Result**
- **Server Connection Ciphers**
- **Server Connection TLS Version**

By implementing **TLS Inspection** through a structured **five-phase deployment**, organizations can enhance security while maintaining **performance and user experience**. Successful implementation requires **careful planning, stakeholder alignment, and continuous monitoring** to detect and mitigate encrypted threats effectively.

Now let's discuss the next Platform Service provided by the Zero Trust Exchange - **Policy Framework**.

Policy Framework

What is the Policy Framework?

The **Policy Framework**, a key component of **Zscaler's Platform Services**, integrates identity and connectivity data to strengthen security controls within **Cyber Protection, Data Protection, and Access Control**. By leveraging **identity providers, SAML assertions, Zscaler Client Connector, and Device Posture**, it enhances **risk scoring, user analytics, and network policy enforcement** across the **Zero Trust Exchange (ZTE)**.

To better understand how **Zero Trust Exchange** operates, we must examine how it identifies users, authenticates them, and enforces access controls. Authentication begins with **SAML assertions**, where the **Identity Provider (IdP)** determines user entitlements. Zscaler evaluates this assertion to decide which services the user can access. Once authenticated, the **Zscaler Client Connector** assesses the **user's network, device posture, and access method**—whether through browser-based access, privileged remote access, or a managed network.

Policy Decisions & Enforcement

Using this information, **network policies** dictate whether the user should connect via **public or private Service Edges** and determine if **Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), or Zscaler Digital Experience (ZDX)** should be enabled. Some users may only require access to **ZIA** without **ZPA** or **ZDX**, while others may need full access based on their role and device posture.

Additionally, **SCIM provisioning, SOAR integrations, and risk posture analysis** refine user access control, allowing the framework to determine if the device is **managed or unmanaged** and apply policies accordingly. **SSL traffic inspection** is another critical component—evaluating **certificate validity, untrusted issuers, expiration errors, and missing SNI (Server Name Indication)**—to decide whether to **allow, inspect, or block** traffic.

Policy Framework

Policy components of the Zero Trust Exchange

- How does the Zero Trust Exchange identify the user/device?
SAML Authentication – Which IDP to use?
- Is this user/device allowed to connect to the exchange?
SAML IDP Policy & Zscaler Policy
- How is this user/device allowed to connect to the exchange?
Trusted Network Policy
Browser Based Access, Privileged Remote Access, Isolated Access, Client Connector
- Which Zero Trust Exchange point should the user connect to?
Trusted Network Policy
Private Service Edge
- Client Connector Policy
Version control & Profile control
- What services can this user/device consume from the exchange? – ZIA/ZPA/ZDX
Group Based – Conditions based on Identity of user & device
- What is this user/device allowed to access through the exchange?
Attribute Based – Browser, SAML Attributes, Risk Score, Posture
Device Based – Managed or Unmanaged
Group Based – SAML or SCIM attributes
Public/Private Applications? Allow/Deny/Other?

By integrating identity, connectivity, and device data, the **Policy Framework** enables **dynamic, context-aware security** within the **Zero Trust Exchange**, ensuring **only authorized users and secure devices** can access critical applications and services.

User Authentication and Policy Configuration in Zero Trust Exchange

User Authentication and Policy Configuration

User authentication and policy configuration play a crucial role in the **Zero Trust Exchange**, ensuring a **strong security posture, compliance**, and a **seamless user experience** while effectively mitigating security risks. By leveraging **context-aware access controls**, Zscaler ensures that users are authenticated and authorized based on specific, predefined criteria.

The **Zero Trust Exchange** determines authentication using the following key factors:

Client Connector Authentication	<ul style="list-style-type: none">• If the user is prompted to enter a Username, the Domain (after the @) is used to identify the corresponding Identity Provider, and the user is redirected to authenticate with that provider.• If the client was installed with a – userDomain option, the Domain directly maps to the Identity Provider for authentication.
Browser-Based Access Authentication	<ul style="list-style-type: none">• Users are prompted to enter a username/email for multiple configured identity providers. The Domain (after the @) helps determine the appropriate Identity Provider for redirection, and users authenticate with that provider.• If only a single Identity Provider is configured, the system automatically directs users to authenticate with that Identity Provider.
Single vs. Multiple Identity Providers	<p>In most organizations, a single Identity Provider (IdP) is typically used for authentication. However, certain scenarios, such as Mergers & Acquisitions or Cloud Migrations, may require managing authentication across multiple IdPs to accommodate different user groups effectively.</p> <p>To configure multiple Identity Providers, follow these steps:</p> <ul style="list-style-type: none">• Add IdPs: Integrate additional Identity Providers within the Administration Configuration.• Configure Domains: Map specific user domains to the appropriate Identity Providers.• User Login: When accessing Zscaler Client Connector or Browser-Based Access, users may be prompted for credentials.

- **Policy Configuration:** Define policies that associate **domains with specific IdPs** to streamline authentication. Users may either encounter authentication prompts or bypass them using **installer options** within Zscaler Client Connector.

This approach ensures a **seamless and secure authentication experience**, especially in environments with diverse user identities.

Service Entitlement

After **authentication into Zscaler Internet Access (ZIA)**, the system utilizes **SAML attributes**, which are then passed to the **Mobile Admin Portal**. The **Mobile Admin policy** determines whether users will be **enrolled in Zscaler Private Access (ZPA) and Zscaler Digital Experience (ZDX)** based on their **group affiliations**.

To configure this process, follow these steps:

- **Add Identity Providers (IdPs):** Integrate IdPs into **Zscaler Internet Access** for authentication.
- **Configure Group Attributes:** Define **user group affiliations** to categorize access levels.
- **Establish Entitlement Policies in Mobile Admin Portal:** Set policies that determine which **groups** have access to **ZPA or ZDX**. You can either assign access based on group membership or configure a **default policy** that grants access automatically.

This configuration ensures seamless integration and automated **user entitlement management** across Zscaler services.

Policy for Zscaler Internet Access

The **policy framework** in **Zscaler Internet Access (ZIA)** enables organizations to **manage and regulate data flow** while maintaining security and efficiency. By enforcing structured policies, ZIA ensures **reliable and safe internet access** for users while preventing unauthorized activity.

As data packets pass through ZIA, they go through multiple layers of **policy enforcement and security inspection**. These include:

- **Policy Framework and Operational Flow in ZIA:** Understanding how policies govern data flow within the system.
- **Web Proxy Configuration:** Applying structured rules to regulate user access, enforce acceptable use, and control traffic.
- **Security and Firewall Configuration:** Defining **security policies** to filter threats, block malicious traffic, and enforce **intrusion prevention rules**.
- **Network Address Translation (NAT) and Intrusion Prevention System (IPS):** Configuring **NAT policies** to manage IP translation and applying **IPS rules** to detect and block potential threats.

Now, let's dive into the **Policy Framework and Operational Flow in ZIA** to understand how these layers work together.

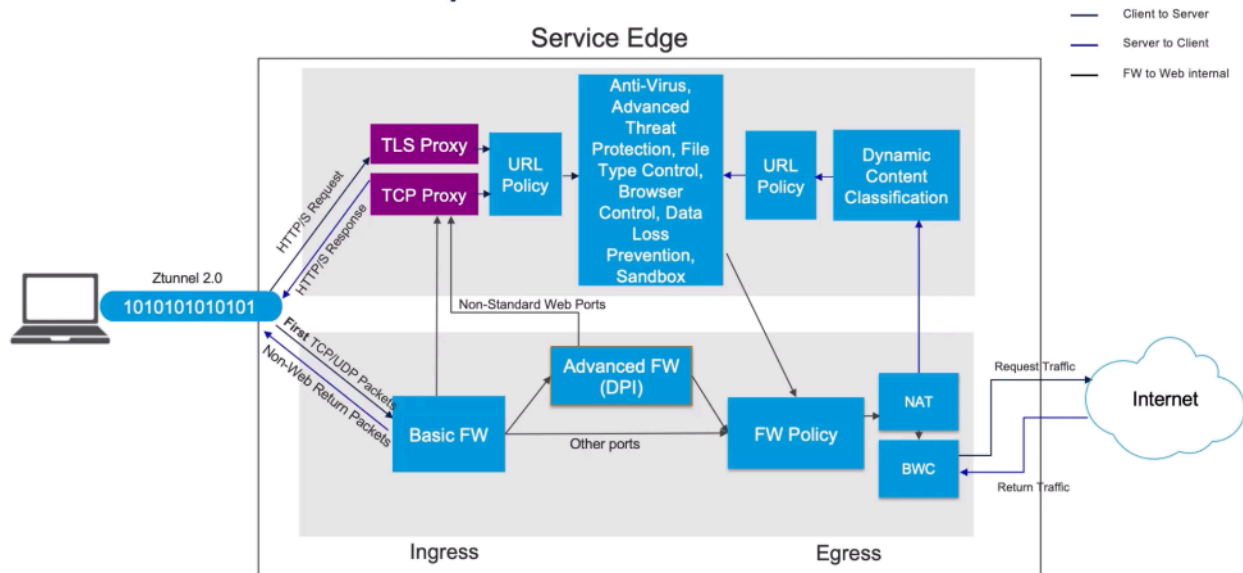
Policy Framework and Operational Flow in ZIA

Zscaler Internet Access (ZIA) enforces a structured **policy framework** to regulate and inspect traffic, ensuring security and compliance. This framework applies multiple layers of security, including **proxy filtering, firewall enforcement, NAT control, data loss prevention (DLP), intrusion prevention system (IPS), and bandwidth management** to inspect and control traffic flow efficiently.

Traffic Flow and Policy Application

As traffic enters ZIA, the **Service Edge terminates the client tunnel** and classifies traffic as **HTTP/HTTPS** or **other protocols**. **Web traffic** is processed through the **proxy engine**, where **TLS inspection, URL filtering, and content security policies** are applied. **Non-web traffic** follows **firewall and NAT policies** before reaching IPS and bandwidth control, ensuring all traffic undergoes security screening before reaching the internet.

Internet Access Order of Operations



Deep Packet Inspection and Security Layers

For **HTTP/HTTPS traffic**, **TLS inspection policies** validate certificate authenticity based on OSCP (Online Certificate Status Protocol) and apply URL filtering. Content is scanned through **file type control, browser control, and DLP policies**, ensuring compliance with organizational security policies. Suspicious files are sent to **sandboxing** for deeper analysis. **Response traffic** undergoes **dynamic content classification**, re-evaluating the request for potential threats. **Antivirus, advanced threat protection, and DLP policies** further analyze the payload before it is securely re-encrypted and sent to the user.

Policy Components and Customization

ZIA policies utilize predefined and custom **URL categories, bandwidth management classes, time-based rules, and firewall filtering definitions**. Organizations can customize **DLP dictionaries and engines** for regulatory compliance, define **Layer 4 (TCP/UDP) and Layer 7 (DPI) filtering rules**, and apply **IP/FQDN-based policies** for granular access control.

Resources – To be used in Policy

Access Control

- **URL Categories** – Predefined and custom categories
- **Bandwidth Classes** – Group Categories to apply Bandwidth Management
- **Time Intervals** – Time windows to apply policy
- **Rule Labels** – Labels to apply to rules

Data Loss Prevention

- **Dictionaries and Engines** – Definitions for matches

Firewall Filtering

- **Network Service** – L4 (TCP/UDP Port) Definitions & Groups
- **Network Applications** – L7 (DPI) Definitions & Groups
- **IP & FQDN groups** – Source IP, Destination IP/FQDN/Wildcards
- **Application Services** – Zscaler Managed Services – E.g. M365

Forwarding

- **Proxies & Gateways** – Upstream proxies to forward to
- **Zscaler Private Access** – Forward to ZPA Applications
- **Location Management** – Static Locations for Policy & Bandwidth Management



Traffic Forwarding and Integration

Traffic forwarding policies allow integration with **upstream proxies**, **Zscaler Private Access (ZPA) segments**, and **Source IP Anchoring** for controlled traffic routing. **Static IP and GRE tunnel configurations** define how policies and bandwidth rules apply across different locations.

By applying this structured **policy enforcement framework**, ZIA ensures **secure, efficient, and policy-compliant** internet access while minimizing security risks and optimizing network performance.

Key Concepts:

What modules process traffic within the ZIA policy framework?	What components form policy rules for ZIA?	What forwarding options exist in ZIA traffic management?
Firewall, NAT Control, IPS, Bandwidth Control, TLS Inspection, File Type Control, Browser Control, Data Loss Prevention, Sandbox, and Dynamic Content Classification.	Policy rules consider URL categories , bandwidth classes , time intervals , rule labels , data loss prevention , firewall filtering , IP and FQDN sources , and application services .	Proxies , Gateways , Zscaler Private Access definitions , and Location Management , covering static IP addresses , names , and GRE tunnels for Policy and Bandwidth Management rules .

Structured Rules and Criteria in Web Proxy Configuration

Zscaler's **web proxy configuration** ensures structured rule management for **traffic control, security enforcement, and data protection**. It follows a **top-down, first-match** processing order, where **rule names, labels, and expiration settings** define enforcement scope and duration. Administrators can prioritize rules based on **organizational needs, security policies, and bandwidth allocation** while allowing flexibility for dynamic changes.

Criteria for Rule Application

Web proxy rules apply based on various **conditions**, including **URL categories, user groups, locations, request methods (POST, DELETE, CONNECT), and device types**. Specific **AND/OR logic** ensures precise policy enforcement. For example, a rule may apply to a **particular user group accessing a sensitive cloud application** only from **trusted locations** using **approved devices**.

For **SSL inspection**, rules determine whether **encrypted traffic is decrypted** based on **certificate validation, URL filtering, and content analysis**. **File type control** uses **MIME types and magic bytes** to classify files, while **DLP policies** examine content for **sensitive data leakage**. Sandbox policies analyze suspicious files before allowing downloads.

Web Proxy Criteria - DLP

Criteria

- Extends criteria to select DLP Engines
- DLP Engines are defined as collections of Dictionaries to trigger on
- Cloud Applications or URL Categories to apply policy on
- Defined Minimum data size to apply DLP rules to
- Applies only to HTTP/HTTPS/FTP traffic

The screenshot displays the 'CRITERIA' configuration page in the Zscaler web proxy interface. It features a grid of dropdown menus for selecting various criteria. The criteria include DLP Engines, URL Categories, Cloud Applications, File Type, Minimum Data Size (KB), Users, Groups, Departments, Locations, Location Groups, Time, and Protocols. Most dropdowns are currently set to 'Any'.

Criteria	Value
DLP Engines	Any
URL Categories	Any
Cloud Applications	Any
File Type	Any
Minimum Data Size (KB)	0
Users	Any
Groups	Any
Departments	Any
Locations	Any
Location Groups	Any
Time	Always
Protocols	HTTP; HTTPS; Native FTP

Rule Actions and Enforcement

Once criteria match, **actions** dictate traffic flow. Administrators can:

- **Allow** access as per policy.
- **Caution** users with acknowledgment pages.
- **Block** traffic with standard or custom block pages.

- **Block with Override**, where privileged users can bypass restrictions (e.g., teachers in an educational setting).
- **Isolate** risky traffic in a secure browser session for additional protection.

Bandwidth Control and Traffic Prioritization

Bandwidth classes ensure **efficient resource allocation** by **guaranteeing minimum bandwidth for critical applications** while capping non-essential traffic. Administrators can define **custom time-based bandwidth rules** for peak and off-peak hours to **optimize network performance**.

By structuring **proxy policies** effectively, Zscaler provides a **granular, flexible, and adaptive** approach to security, ensuring **seamless traffic management while maintaining security, compliance, and performance**.

Key Concepts:

What determines the order of processing for web proxy rules in Zscaler?	What does the Admin Rank define in Zscaler's Web Proxy Rules	What are the criteria considered in Zscaler's DLP rules?
All rules are processed top-down, first-match .	It specifies which administrators can manage the rule , with administrators of equal or lower rank able to manage those rules .	DLP Engines, Cloud Application information, file type, minimum size, Users, Groups, Departments, Locations, Location Groups, Time, and Protocols (HTTP, HTTPS, or native FTP).

Security Policy and Firewall Rules in ZIA

Zscaler Internet Access (ZIA) enforces a **comprehensive security policy** to inspect all incoming and outgoing traffic while allowing exceptions for specific URLs. Advanced Threat Protection assigns a **risk score** to traffic based on multiple factors, helping organizations manage risk effectively. Firewall rules operate in a **top-down, first-match order**, evaluating **users, devices, services, and destinations** to determine whether traffic should be allowed, blocked, or logged.

Security Policy Enforcement

ZIA applies security policies to **all transactions**, inspecting **HTTP, FTP over HTTP, and native FTP** while enforcing **Malware and Advanced Threat Protection**. However, administrators can **exclude specific URLs** from scanning, which removes them from malware and threat detection policies.

Advanced Threat Protection (ATP) analyzes botnet activity, malicious content, and fraud risks. Zscaler assigns a **dynamic risk score** based on page content, external links, website age, and hosting location. The default **risk threshold is 30**, meaning a **30% confidence level that a page is safe**. Organizations can adjust this threshold to determine what level of risk is acceptable.

Firewall Rule Criteria and Actions

Firewall rules function similarly to web proxy rules, following a **top-down priority order**. Administrators define **rule names, statuses, and predefined labels**, and the firewall enforces **standard (port-based) or advanced (deep packet inspection) policies**.

Rules logically **AND together** multiple criteria, including:

- **User & Device Criteria:** Users, groups, departments, locations, devices.
- **Service & Application Rules:** Layer 4 (port-based) services like **HTTP (80)**, **HTTPS (443)**, and **RDP (3389)**, and Layer 7 application definitions.
- **Source & Destination:** Source IP groups, destination IP groups, countries, and URL categories.

Action Types:

- **ALLOW:** Permits the transaction.
- **BLOCK/DROP:** Silently drops traffic, potentially causing retransmissions.
- **BLOCK ICMP:** Sends an ICMP “port unreachable” response.
- **BLOCK/RESET:** Sends a **TCP reset**, forcibly closing the connection.

Traffic Logging & Aggregation

Non-HTTP/S traffic undergoes **full logging**, with transactions grouped and logged periodically. By structuring security and firewall policies effectively, **Zscaler ensures secure, policy-driven internet access, minimizing threats while optimizing traffic control.**

Key Concepts:

What happens when you decide not to scan specific traffic in Zscaler?	How does Zscaler determine whether to allow traffic based on its risk score?	What are some actions that Zscaler's firewall can take when rules trigger?
It excludes traffic from scanning both malware protection and advanced threat protection .	Zscaler creates a dynamic risk score using page content, link destinations, website age, and hosting location . The customer determines their risk tolerance.	Actions can be ALLOWED , BLOCKED (with options like DROP, ICMP, or RESET), and LOGGED for non-HTTP/HTTPS traffic with periodic aggregation.

Policy Configuration and Actions in Network Address Translation (NAT) and Intrusion Prevention System (IPS)

In Zscaler, **Network Address Translation (NAT) Control** and **Intrusion Prevention System (IPS) policies** function similarly to firewall rules, applying criteria based on **user attributes, location, time, and device type**. NAT Control involves **destination and port address translation**, while IPS applies security policies based on **user identity, location, and service attributes**, ensuring proactive threat mitigation.

NAT Control and Actions

NAT policies are defined using a **logical AND** between multiple attributes, including **users, departments, groups (SAML/SCIM), locations, time-based policies, and device types**. NAT rules operate at **Layer 3 and Layer 4**, meaning they must be applied **before** deeper inspection of packet payloads.

NAT Criteria – Logical AND

Who, Where, When

- **Users, Groups or Departments** – Based on SAML/SCIM attributed provided
- **Locations or Location Groups** – Fixed Locations (defined). Road Warrior is default undefined Location
- **Time** – Time-of-day based policy (defined under Administration Resources)
- **Devices or Device Groups** – From Zscaler Client Connector, Isolation, or OS Types

Services (AND)

- **Services or Service Groups** – Defined Services (L4)

Source IP (AND)

- **Source IP Groups (Defined in Resources) OR Specific IPs**

Destination IP (AND)

- **Destination IP Groups (Defined in Resources) OR Specific Ips**
- **Countries OR URL Categories**

The image displays three screenshots of the Zscaler NAT policy configuration interface, illustrating the 'Logical AND' criteria selection process. Each screenshot shows a tabbed interface with 'Who, Where, & When...', 'Services', 'Source IP', and 'Destination IP' tabs. The first screenshot shows the 'Who, Where, & When...' tab with criteria for Users (Any), Departments (Any), Location Groups (Any), Locations (Any), and Time (Always). The second screenshot shows the 'Services' tab with criteria for Network Service Groups (None) and Network Services (Any). The third screenshot shows the 'Source IP' tab with criteria for Source IP Groups (None) and IP Addresses (Add Items). The 'Destination IP' tab is also visible, showing criteria for Destination Groups (None), IP Address or FQDN (Add Items), Countries (Any), and Categories (Any).

NAT Actions Include:

- **Destination NAT (DNAT):** Translates a destination IP to a specific IP or FQDN, triggering a DNS lookup.
- **Port Address Translation (PAT):** Modifies the destination port (e.g., changing client requests from **port 80 to port 8080** before egressing from Zscaler Service Edge).

Intrusion Prevention System (IPS) Criteria and Actions

IPS policies use a **logical AND** between **user, group, department (SAML/SCIM attributes), location groups, time-based rules, and device types**. Policies also integrate **Layer 4 services and Advanced Threat Categories**, applying **IPS signature-based threat detection**.

IPS Actions Include:

- **ALLOW**: Permits the transaction.
- **BLOCK/DROP**: Silently drops packets, potentially triggering client retransmissions.
- **BLOCK/RESET**: Sends a **TCP reset** to terminate the connection or a single drop for UDP traffic.
- **BYPASS**: Ignores IPS inspection for trusted or known-safe traffic.

Logging and Monitoring

Both NAT and IPS policies include **logging mechanisms** similar to firewall policies. Administrators can configure:

- **Full Logging**: Captures all **non-HTTP/HTTPS** transactions.
- **Aggregate Logging**: Groups and periodically logs transactions for efficiency.

By structuring **NAT and IPS policies effectively**, organizations can **enhance network security, enforce access control, and mitigate threats while maintaining seamless connectivity**.

Key Concept:

NAT enables **destination address translation (DNAT)** by mapping traffic to a specific **IP address or Fully Qualified Domain Name (FQDN)**, triggering a **DNS lookup** before forwarding. Additionally, **port address translation (PAT)** modifies port numbers upon egress from the **Zscaler Service Edge**, ensuring seamless traffic routing and policy enforcement.

Policy for Zscaler Private Access (ZPA) Policy Framework

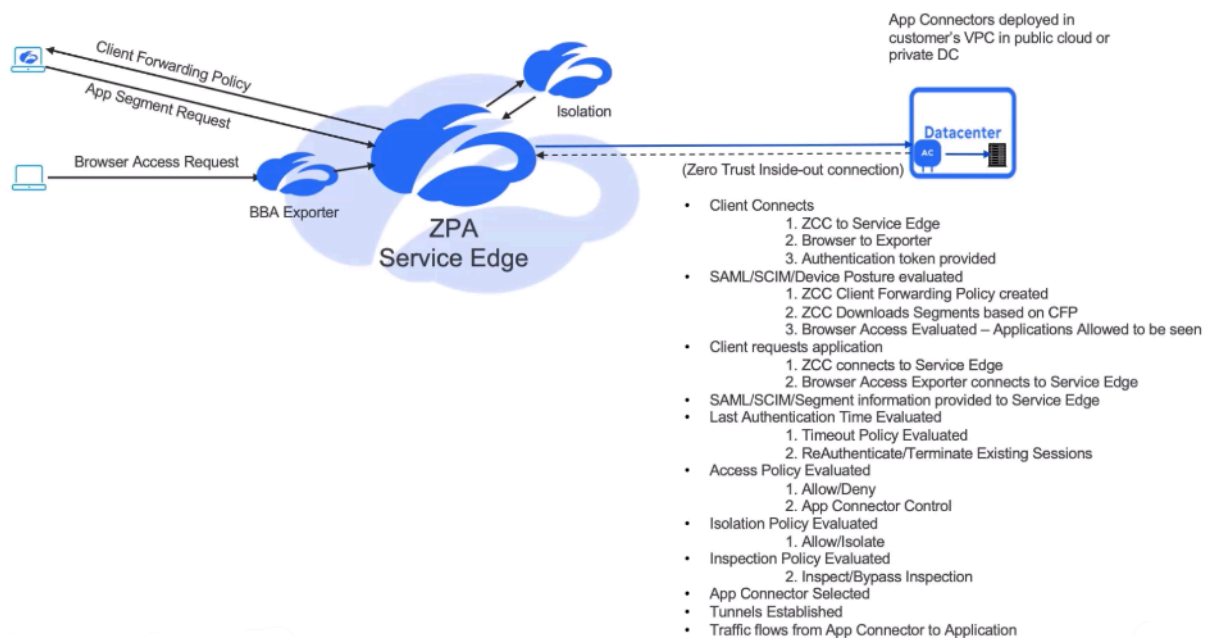
ZPA provides **secure, seamless access** to internal applications without requiring a traditional VPN. Its policy framework defines rules and configurations to **control and secure** access to specific resources within an organization's network.

Operational Flow & Policy Evaluation

The **Zscaler Client Connector** first connects to the **ZPA Public or Private Service Edge**, which evaluates **user authentication** via SAML/SCIM attributes and **device posture** to determine access permissions. The **client forwarding policy** then dictates which application segments the user can access. Based on the request, ZPA applies **access control, isolation, and inspection policies** before establishing secure tunnels between the **Client Connector and App Connectors** to facilitate application access.

Policy Criteria & Order of Operations

Private Access Order of Operations



ZPA policies are evaluated **top-down, first-match**, with an **implicit default deny** rule at the bottom, similar to firewall policies. Policies use a combination of **user attributes (SAML/SCIM)** and **device attributes** (device posture, network location, and compliance status) to determine access. Additional attributes such as **trusted network status** and **client type** (Client Connector, browser-based access, or machine tunnel) further refine policy decisions.

Types of ZPA Policies

- **Access Policy** – Determines whether a user is allowed or denied access to a given application.
- **Timeout Policy** – Defines when users must re-authenticate to maintain access.
- **Client Forwarding Policy** – Specifies which application segments the Zscaler Client Connector can access.
- **Isolation Policy** – Dictates whether a user session should be placed into an **isolated browser environment** for additional security.
- **Inspection Policy** – Controls whether **ZPA inspection** will be applied to user transactions.

By leveraging **user authentication, device posture, and network context**, ZPA ensures a **zero trust approach** to application access while maintaining **strong security controls** without exposing internal networks.

Key Concepts:

What are the initial steps in ZPA policy evaluation?	How does ZPA policy evaluation occur during a transaction?
The Zscaler Client Connector connects to the ZPA Public or Private Service Edge , evaluates SAML/SCIM attributes and device posture , and establishes a Client Forwarding policy .	First, the Timeout policy is evaluated , followed by an access policy based on SAML/SCIM attributes and device information , then an isolation policy , and finally, an Inspection policy before routing traffic through App Connectors .

Analyzing Access Policy Criteria for ZPA

In the **Zscaler Zero Trust Exchange**, access policies determine user permissions based on multiple factors, including **application segments, SAML/SCIM attributes, client types, device posture, and trusted networks**. These policies define access rights, reauthentication intervals, idle timeouts, client forwarding, inspection, and isolation policies.

Policy Criteria

- **Application Segment OR Segment Groups**
- **SAML/SCIM Attributes**
 - Multiple Attributes selected
 - Default – Attributes are A OR B
 - Selective – Attributes are A AND B
- **Client Types – A OR B**
- **Client Connector Posture Profiles**
 - Default – Attributes are A OR B
 - Selective – Attributes are A AND B
- **Client Connector Trusted Networks**
 - Network A OR Network B

Create Multiple rules where single rule construct cannot be built

The screenshot shows the 'Add Access Policy' window. It features a tree view on the left with criteria like 'Application Segments', 'Segment Groups', 'SAML and SCIM Attributes', 'Client Types', 'Client Connector Posture Profiles', and 'Client Connector Trusted Networks'. The main area displays a rule structure where these criteria are combined using 'AND' and 'OR' operators. For example, 'Application Segments' (Apache) is ORed with 'Segment Groups' (Browser). This is then ANDed with a group of SAML and SCIM attributes. Further down, 'Client Types' is ANDed with 'Client Connector Posture Profiles' (Firewall (zscaler.net)), which is then ANDed with 'Client Connector Trusted Networks'. The interface includes 'Add Criteria', 'Add More', and 'Add MP' buttons for each criterion, and 'Save' and 'Cancel' buttons at the bottom.

Each policy rule **combines multiple criteria**. **Application segments, client types, and trusted networks** are ORed together, meaning any match will trigger the rule. **SAML/SCIM attributes and device posture profiles** can be ORed or ANDed, allowing for **granular control** over security requirements. For example, a policy might require a user to meet **multiple device posture checks** before being granted access.

Access policies define whether a **transaction is allowed or denied**. They can also specify which **App Connectors** to use. For instance, users in China might be routed through **China-based App Connectors**, while other users connect to the nearest available connector. **Timeout policies** enforce reauthentication intervals based on application sensitivity, while **Idle Timeout policies** terminate inactive connections after a defined period.

The **Client Forwarding policy** determines which applications the **Zscaler Client Connector** should forward, allowing administrators to define forwarding criteria based on **user attributes, posture profiles, and trusted networks**. Inspection policies, which analyze **HTTP/HTTPS traffic**, can be configured using the same criteria as **access policies** for **simplified rule management**.

Finally, **Isolation policies** apply specifically to **browser-based access**, enabling organizations to route traffic through an isolated browser session for **added security**. By leveraging these access policy criteria, **ZPA ensures** that users can securely connect to authorized applications **while maintaining granular control over security and compliance**.

Key Concepts:

How are criteria combined to trigger a rule in Zscaler’s access policy?	What determines when a user should reauthenticate in Zscaler’s Timeout policy?	Which type of applications are inspected in Zscaler’s Inspection policy?
Application segments, SAML/SCIM attributes, client types, posture profiles, and trusted networks are logically combined to trigger a rule.	The Timeout policy is triggered for business reasons , and criteria include application names, segments, posture profiles, client types, and SAML/SCIM attributes .	The Inspection policy applies to HTTP and HTTPS applications where Inspection is enabled , and access policy rules and criteria can be directly duplicated .

Zscaler Digital Experience Policy

Zscaler Digital Experience (ZDX) policy determines whether **probes** are activated based on **user attributes** such as groups, users, locations, and devices. It also allows for **exclusion criteria**, preventing probes from running in specific scenarios, such as when users are in the office.

By optimizing **probe activation**, ZDX policies ensure **efficient network monitoring**, aligning with user contexts to enhance the **overall digital experience** while minimizing unnecessary performance overhead. Each probe is activated based on pre-defined **criteria**, including user group membership, department, device type, or location. If a scenario meets **exclusion criteria**, such as being within a corporate office, the probe will **not run** to conserve resources and **avoid redundant monitoring**.

Key Chapter Takeaways

Policy Framework Overview: Zscaler's **Policy Framework** integrates **user and device data** to strengthen security across **Cyber Protection, Data Protection, and Access Control** within the **Zero Trust Exchange**.

- **User Authentication & Policy Configuration:** Authentication relies on **Client Connector** or **Browser Access**, mapping **Identity Providers** using **domain information**.
- **ZIA Policy & Security:** **Zscaler Internet Access (ZIA)** enforces structured **traffic management policies**, including **web proxy configurations, firewall rules, and security controls**.
- **NAT & IPS Control:** **NAT policies** function similarly to **firewall rules**, applying **user attributes, location, and device-based controls**. **Intrusion Prevention System (IPS)** policies analyze **user, group, and location data**, enforcing security actions like **allowing, blocking, or resetting transactions**.
- **ZPA Order of Operations:** The **Zscaler Private Access (ZPA)** policy framework evaluates **user identity, device posture, and network attributes** before granting access to **internal applications**.
- **Access Policy & Reauthentication:** **Application segments, SAML/SCIM attributes, posture profiles, and trusted networks** determine **access rights, session timeouts, and reauthentication intervals**.
- **ZDX Probe Activation:** **Probe activation is dynamically controlled** based on **user attributes**, with **exclusions** to optimize performance and user experience.

By **strategically managing policies**, organizations can **enhance security, optimize performance, and improve user experience** across the **Zero Trust Exchange**.

Access Control

This chapter provides an in-depth understanding of **Zscaler's Access Control approach** within a **Zero Trust environment**. By the end of this module, you will gain foundational knowledge of **Zscaler's Access Control Services**, ensuring **secure, scalable, and efficient access** across your organization.

The chapter is structured into two key sections:

- **Access Control Overview:** This section introduces the **core principles** of Zscaler's Access Control, highlights the **suite of services** available, and explores the **limitations of traditional firewalls and legacy access controls**.
- **Access Control Services Suite:** Here, we examine **key security features**, including **Cloud App Control, URL Filtering, Bandwidth Management, M365 Optimization, Segmentation, and Firewall Capabilities**.

By **leveraging Zero Trust principles**, Zscaler ensures **granular, policy-driven access** to applications while eliminating **security gaps** present in traditional network architectures.

By the end of this chapter, you will be able to

1. **Define** what Access Control is within the Zero Trust Exchange and how it enables secure, policy-based connections between users and applications
2. **Describe** how URL/Web Filtering works to regulate and secure web access, ensuring users only reach approved, business-appropriate destinations
3. **Identify** scenarios where Bandwidth Control is beneficial and apply best practices to prioritize critical business traffic, improving user experience and productivity
4. **Discuss** strategies for optimizing Microsoft 365 (M365) traffic flow to maintain secure, high-performing access to essential collaboration and productivity tools
5. **Explain** how Private App Access provides direct, secure connectivity to internal applications without exposing the network, reducing complexity and risk
6. **Summarize** how implementing Segmentation reduces the attack surface by restricting lateral movement, ensuring users only access the resources they need
7. **Illustrate** how Firewall enforcement within Access Control provides a foundational layer of defense, controlling ports, protocols, and IPs to maintain a safe and compliant network environment

Access Control Overview

The challenge of legacy firewalls

In today's dynamic work environment, where employees require **secure access from any location, on any device, at any time**, traditional **on-premises firewalls** fail to meet modern security and performance demands.

Legacy firewall appliances rely on **zone-based architectures**, segmenting networks into **trusted internal** and **untrusted external** zones. This approach introduces **three major business risks**:

1. **Security vulnerabilities** – Broad, network-based access increases the **attack surface** and **lateral threat movement**, leaving organizations exposed to breaches.
2. **Performance issues** – SSL decryption and deep traffic inspection **strain firewall hardware**, leading to **slowdowns and degraded user experiences**.
3. **Operational complexity and cost** – Managing **multiple firewall appliances across branch offices** creates **inconsistencies in security policies**, increases **IT workload**, and requires **constant patching and maintenance**.

Why Legacy Firewalls Fall Short

Traditional **firewall-based access control** is built around **network-to-network** connections. Enterprise branch offices historically relied on **on-premises firewalls** to enforce access policies for **employees, guests, and applications**. These policies grouped endpoints into **trusted zones** (internal users, servers, and applications) and **untrusted zones** (internet traffic and external users).

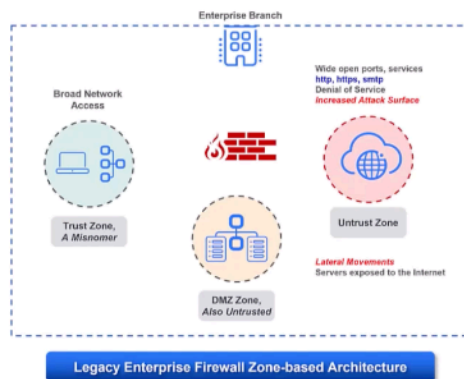
However, **Zero Trust security models** challenge this outdated approach by eliminating **implicit trust** in any zone. Instead, access should be **user, device, and context-aware**, ensuring that **only authorized users and devices** can access specific applications—not entire network segments.

The Risks of Legacy Firewall Architectures

1. **Broad Network Access**: Zone-based access control **grants excessive permissions** based on IP addresses, ports, and protocols—failing to inspect the **user's identity, device posture, or application context**.
2. **Inconsistent Security Posture**: Branch offices often deploy **smaller, less capable firewalls**, leading to **uneven protection** across locations.
3. **Performance Bottlenecks**: **SSL decryption and deep packet inspection** overload firewall appliances, causing **latency and degraded user experiences**.

4. **Increased Attack Surface:** Exposing public-facing IPs increases the risk of **DDoS attacks** and other cyber threats, requiring constant patching and penetration testing.

Problem with Legacy On-Prem Firewalls



Security

- Broad Network Access
- Increased attack surface
- Lateral Threat movement



Performance

- Poor performance with TLS inspection
- Long lived connections to apps
- Can't sustain peak ramp rate



Cost & Complexity

- Increases cost to turn on full stack security
- Inconsistent security posture
- Onus on customer for patches, pen testing etc.

How Zscaler Solves These Challenges

Zscaler's **Zero Trust Exchange** eliminates **network-based access** and replaces it with a **user- and application-centric** approach. Instead of exposing **entire networks**, Zscaler grants **least-privilege access** based on **user identity, device posture, and business policies**.

This cloud-delivered **Zero Trust model** enables organizations to:

- **Eliminate lateral movement risks** by enforcing **direct user-to-application connections** without exposing networks.
- **Enhance performance** with **cloud-based SSL inspection** that scales without hardware limitations.
- **Reduce operational overhead** by shifting security enforcement to the cloud, ensuring **consistent policies across all locations**.

By transitioning from **legacy firewalls** to **Zero Trust Access**, organizations **reduce attack surfaces, improve security, and streamline access control** for today's modern workforce.

Key Concepts:

What limits legacy firewalls in branch offices?	Why inspect network traffic content and context?	What advantages does Zscaler's Zero Trust platform offer?
Legacy firewalls rely on zone-based architectures , which grant broad network access , increasing the attack surface and security risks by failing to enforce user-specific, least-privilege access controls.	Legacy systems often overlook the importance of inspecting traffic content and context , which is crucial for identifying and mitigating security risks effectively.	Zscaler's Zero Trust platform strengthens security by implementing dynamic access control based on user risk and device posture , effectively minimizing potential threats and reducing the attack surface.

Key Takeaways

Here's a summary of the critical insights from this section:

- **Limitations of Zone-Based Firewalls:** Traditional firewalls rely on **broad, static access controls**, making them ineffective against modern cyber threats.
- **Need for Traffic Inspection:** Security depends on **deep content and context inspection**, which legacy firewalls often fail to perform, creating security gaps.
- **Performance Challenges:** Legacy firewalls struggle with **SSL inspection**, leading to degraded network performance and inefficiencies.
- **Inconsistent Security Across Branches:** Variations in **firewall capabilities and maintenance** result in **uneven security postures** across different locations.
- **Zero Trust Advantages:** Zscaler's **Zero Trust Exchange** dynamically adjusts **access controls based on user risk and device posture**, **enhancing security** and minimizing attack surfaces.

Zscaler's Access Control Services Suite

Cloud App Control, URL Filtering, and File Type Control

Zscaler's **Cloud App Control** and **URL Filtering** provide **granular access control** over internet and cloud application usage, ensuring security while aligning with business policies. These features allow organizations to regulate access to applications and URLs based on predefined policies.

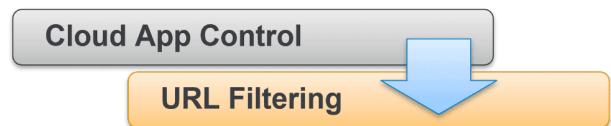
What is Cloud App Control and URL Filtering?

- **Cloud App Control:** Uses predefined or custom application lists as policy criteria to manage access to cloud applications.
- **URL Filtering:** Uses predefined URL categories or custom URL lists to enforce web access control.

Both features enable administrators to create policies that **Allow, Caution, Block, or Isolate** specific cloud apps, URLs, or categories. By default, **Cloud App Control rules take precedence over URL Filtering** in access decisions.

For example:

- If **Webmail is BLOCKED in Cloud App Control** but **ALLOWED in URL Filtering**, access will be **Blocked**.
- If **Webmail is ALLOWED in Cloud App Control** but **BLOCKED in URL Filtering**, access will be **Allowed**.

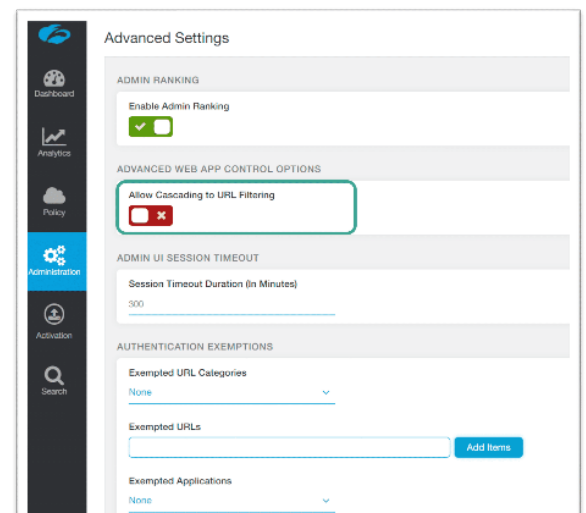


Since Cloud App Control takes priority, **Zscaler recommends using it for access control** whenever possible. Rules are evaluated in sequence, and evaluation stops at the first match, with a default '**Allow All**' rule applied when no other match is found.

How Do They Work Together?

As noted above, **Cloud App Control rules override URL Filtering** when an application is explicitly allowed. However, **Allow Cascading to URL Filtering** is an advanced setting that enables both policies to be enforced simultaneously.

- **Default Behavior:** If Cloud App Control **allows** access, **URL Filtering** is not applied.



- **With Allow Cascading Enabled:** Both **Cloud App Control** and **URL Filtering** are applied, ensuring stricter enforcement of policies.

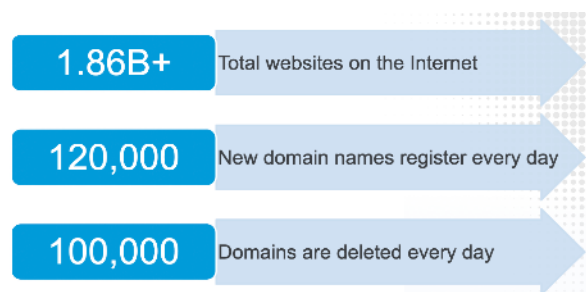
This integration **enhances security** by applying multiple layers of filtering and inspection.

Why is URL Filtering Important?

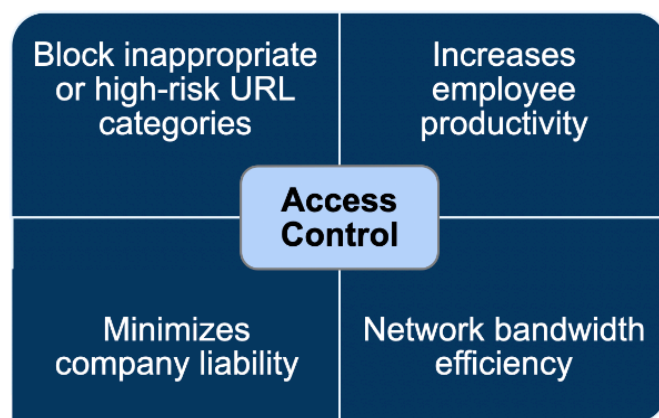
URL Filtering is a **critical component of Zscaler's layered defense strategy**, providing businesses with **enhanced control over web access** while **boosting employee productivity** and **protecting against harmful content**.

With over **1.86 billion websites** on the internet, growing by **120,000 new domains daily**, URL filtering ensures enterprises:

- **Block inappropriate or high-risk content** that could pose security threats.
- **Reduce legal liability** by preventing access to harmful or non-compliant websites.
- **Optimize bandwidth usage** by restricting access to non-essential or bandwidth-heavy content.



By implementing **Cloud App Control**, **URL Filtering**, and **File Type Control**, Zscaler provides a **powerful, multi-layered security approach** that enhances enterprise security while **ensuring compliance and boosting productivity**.



Key Concepts:

Why is URL filtering crucial for enterprises?	How does URL filtering contribute to network efficiency?
URL filtering is crucial for enterprises as it allows them to block inappropriate content and high-risk URL categories, thereby boosting employee productivity and minimizing legal liabilities related to harmful content.	URL filtering helps efficiently use network bandwidth by imposing restrictions on unnecessary or bandwidth-heavy content that is not essential for employee productivity or daily operations.

Cloud App Control and URL Filtering Use-Cases

Zscaler's **Cloud App Control** and **URL Filtering** provide **granular access control, isolation actions, and time-based policies** to manage user behavior, enhance security, and optimize bandwidth. Below are key use cases where enterprises leverage these capabilities.

Granular Access Control

Enterprises can **customize access based on user roles, departments, devices, and locations**. This ensures that only authorized users access specific websites, improving security and compliance.

Granular access control
Isolate webpages
Device OS based policies
Cautioning users
User-agent based policies
Time-based policies
Rule expiration
Bandwidth quota supported
User Risk-Based Policies

Isolate Web Pages

Newly registered websites can be **used for phishing or malicious activity** before being flagged. Isolation prevents direct access to unknown or untrusted sites, protecting users until proper categorization is established.

Device OS-Based Policies

Organizations can enforce **access controls based on supported operating systems**, ensuring that only compliant devices access corporate resources.

Cautioning Users

Before accessing potentially risky websites, users can receive **warnings** advising against entering credentials or sharing sensitive data. This proactive approach helps prevent phishing attacks.

User-Agent Based Policies

Administrators can apply **access rules based on browser type**, ensuring compliance with company policies and security requirements.

Time-Based Policies

Enterprises can **restrict browsing access to specific hours** or allow access to third-party contractors only during authorized periods.

Rule Expiration

Access rules can be **set to expire** automatically after a defined duration, such as **project-based access for external users** or time-limited permissions for certain categories.

Bandwidth Quota Management

To **prevent excessive bandwidth usage**, businesses can set restrictions on specific URL categories, prioritizing network resources for productivity and collaboration tools.

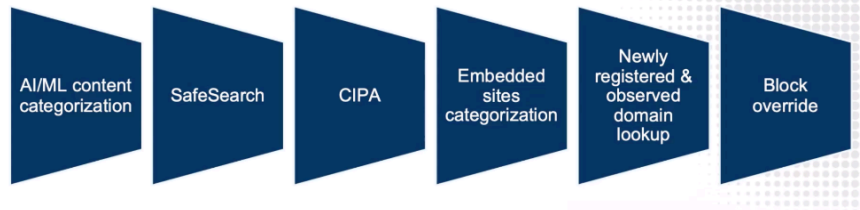
User Risk-Based Policies

Zscaler's **dynamic user risk scoring** adjusts access permissions based on a user's browsing behavior. If a user frequently visits high-risk sites, their access can be **restricted** in real time.

Advanced Use Cases

Advanced Use Cases with URL Filtering

- **AI/ML Categorization:** Uses **AI-driven classification** to analyze new domains dynamically, helping improve **isolation capabilities** for unknown sites.
- **SafeSearch Enforcement:** Ensures search engines like Google **only return safe results**, reducing exposure to harmful content.
- **CIPA Compliance:** Provides **Child Internet Privacy Act** controls for educational institutions, blocking inappropriate content.
- **Embedded Sites Categorization:** Detects **malicious content hidden within trusted websites**, preventing security bypass attempts.
- **Newly Registered & Observed Domains:** Monitors **newly created domains** and applies caution or isolation policies to prevent phishing and malware distribution.
- **Block Override:** Allows certain **users or departments** to override access restrictions under controlled conditions.



By implementing these **Cloud App Control and URL Filtering strategies**, enterprises can **enhance security, optimize resources, and maintain compliance**, ensuring a **safer and more productive** digital environment.

How is Zscaler Cloud App Control and URL Filtering Different?

Zscaler sets itself apart from other **Cloud App Control and URL Filtering** solutions by offering a **comprehensive, AI-driven approach** with **global support, advanced categorization, and granular policy enforcement**.

Key Differentiators:

1. Global URL Database & Multi-Language Customization

- Zscaler supports a **global URL database** covering dozens of countries, ensuring accurate classification worldwide.
- The **block page is fully customizable** and supports **multiple localization languages** to enhance user experience.

2. AI/ML-Based Categorization & Priority Categorization Service

- Zscaler leverages a **combination of in-house AI/ML-based content categorization engines** and **third-party feeds** to classify URLs accurately.
- The **Priority Categorization Service** provides **customized URL classification**, especially beneficial for **financial, insurance, and healthcare** industries.
- Organizations can also **create custom categories** based on their own security intelligence or **SOC (Security Operations Center) insights**.

3. Granular Policy Controls & Enforcement

- Zscaler offers highly **granular enforcement** capabilities, including policies based on **user, location, department, device OS, user agent, protocol, HTTP method, and time of day**.
- Policies follow users **regardless of location**—whether **on-premises, remote, or on untrusted networks**, ensuring **consistent security enforcement**.

4. SafeSearch & Browser Isolation for Enhanced Protection

- Organizations can **automatically enable SafeSearch** to ensure users only receive safe search results.
- Zscaler's **Remote Browser Isolation (RBI)** allows users to **safely access unclassified or potentially risky websites** by **streaming pixels instead of direct website interaction**, effectively **minimizing attack surfaces**.

5. Centralized Management & Actionable Insights

- All **policy configurations, enforcement, and reporting** are managed through a **single, centralized console**, simplifying administration.
- **Advanced dashboards** provide **real-time visibility, drill-down reporting, and transaction-level insights**, helping organizations make **data-driven security decisions**.

6. Full API Support for Automation & Integration

- Zscaler's capabilities are **fully programmable**, allowing **API-based configuration management** and seamless integration into **enterprise security and IT workflows**.

Zscaler's **Cloud App Control and URL Filtering** go beyond traditional web filtering by delivering **AI-powered, highly customizable, and granular security controls**. These capabilities ensure **seamless policy enforcement, advanced threat prevention, and an optimal user experience** across all devices and locations.

Key Concepts:

What makes Zscaler's URL filtering database unique?	How does Zscaler enhance URL categorization?	What advanced search safety feature does Zscaler offer?
Zscaler's global URL database is highly customizable and supports multiple localization languages , allowing organizations to tailor web filtering policies to specific geographic and business requirements while ensuring consistent security enforcement worldwide.	Zscaler improves URL categorization through a multi-layered approach , leveraging AI/ML algorithms , an in-house classification engine , trusted third-party feeds , and a Priority Categorization Service designed for critical industries such as finance and healthcare .	Zscaler offers an automated SafeSearch capability that can be enabled across the entire organization, ensuring secure and filtered search results on popular search engines.

Cloud App Control and URL Filtering Policies & Criteria

Zscaler's **Cloud App Control Policy** provides granular control over web applications, allowing organizations to enforce access policies for users based on predefined or customized rules. With **17 categories**, these policies ensure secure access while optimizing productivity.

- **12 categories** support **Allow or Block** actions, covering collaboration tools, finance, healthcare, IT services, productivity apps, and more.
- **5 categories**—file sharing, instant messaging, social networking, streaming media, and webmail—support additional action-based rules like **Caution or Isolate**.

Granular Policy Criteria

Zscaler's rule-based engine allows organizations to configure access policies with **detailed criteria**, ensuring security while maintaining operational efficiency.

- **Role-Based Access Control (RBAC)** ensures that only authorized administrators manage policies.
- **Location Groups** enable consistent policy application across multiple offices, automatically including new locations.
- **Comprehensive HTTP/HTTPS Support** includes all request methods (CONNECT, GET, HEAD, PUT, DELETE).
- **Protocol and User-Agent Filtering** allows for granular control based on network protocols, device types, and browser details.
- **Device Awareness** supports **BYOD vs. managed device differentiation**, enabling risk-based access policies.

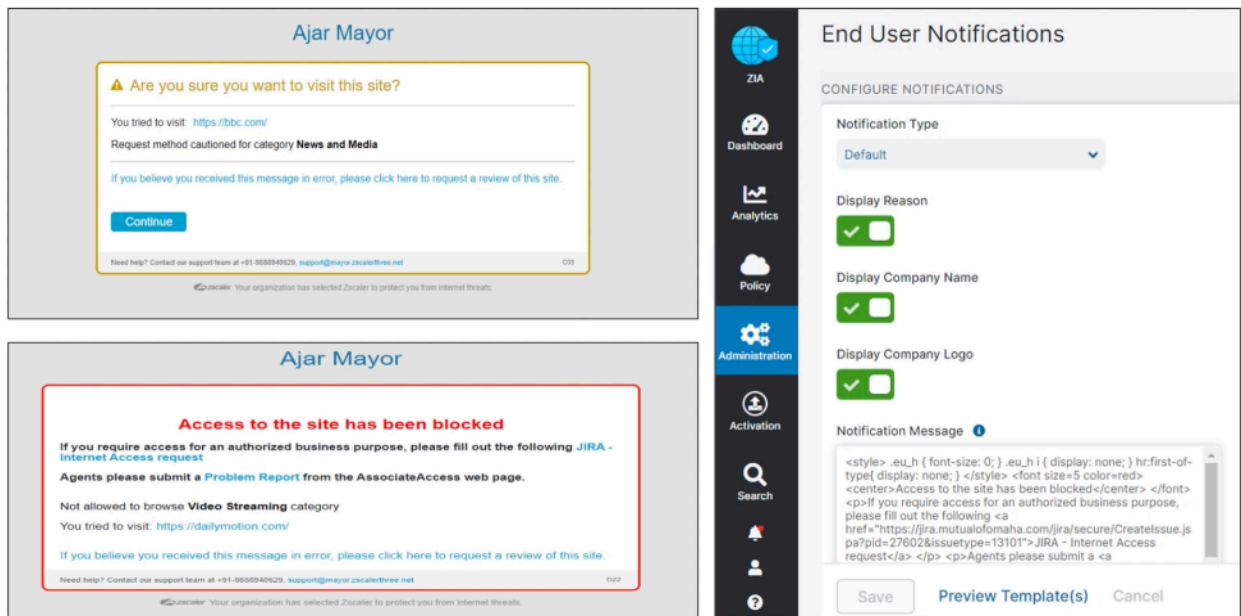
Policy Actions

Zscaler's Cloud App Control and URL Filtering policies support multiple enforcement actions:

- **Allow:** Grants access to a specific URL, application, or category.

- **Block:** Restricts access based on policy settings.

End User Notifications



- **Caution:** Alerts users when accessing potentially risky sites.
- **Isolate:** Uses browser isolation to protect users from unknown or suspicious domains.
- **Bandwidth Control:** Limits network usage for non-business-related activities.
- **ICAP Redirection:** Redirects content for deeper analysis.

Visibility & Dashboards

Zscaler's **real-time dashboards** provide deep insights into browsing activity, helping organizations track:

- **Top users, URLs, and social media usage**
- **Threat intelligence, including spyware and advanced threats**
- **Bandwidth consumption and traffic distribution by category**
- **Granular reporting for optimizing policies and security posture**

Best Practices for Policy Configuration

To ensure optimal security and user experience, organizations should follow these key practices:

1. **Leverage Corporate Acceptable Use Policies** as a foundation for URL filtering rules.
2. **Retain Parent Categories** when creating custom categories to avoid conflicts.
3. **Prioritize Specific Policies** at the top, with broader policies below for efficiency.
4. **Block High-Risk & Liability Categories** (e.g., adult content, gambling, extremism).
5. **Use Isolation for Unclassified Sites**, including newly registered or observed domains.

6. **Regularly Review & Clean Up URL Categories** to prevent duplication and inconsistencies.
7. **Block Anonymizers and Spyware/Adware Categories** for improved threat prevention.
8. **Use Default Allow Strategy** to minimize operational disruptions, while refining policies over time.
9. **Enforce Additional Block Policies for Unauthenticated Traffic** to enhance security.

By implementing these policies effectively, enterprises can balance security, productivity, and network performance while maintaining a Zero Trust security model.**Key Concepts:**

What are key aspects of Zscaler's rule-based URL filtering engine?	How does Zscaler handle diverse HTTP request methods in URL filtering?	What unique action capabilities does Zscaler's URL filtering offer?
<p>Zscaler's URL filtering engine offers granular rule customization, enabling organizations to enforce precise web access policies. Key features include:</p> <ul style="list-style-type: none"> ● Role-Based Access Control (RBAC): Ensures only authorized administrators can create or modify rules. ● Rule Prioritization: Allows ranking among admins to establish policy enforcement hierarchy. ● Enable/Disable Flexibility: Admins can activate or deactivate rules as needed for dynamic policy adjustments. <p>This structured approach ensures secure, efficient, and adaptable web access control within enterprise environments.</p>	<p>Zscaler supports all HTTP request methods, including CONNECT, GET, HEAD, PUT, and DELETE, enabling robust protocol management and precise policy enforcement.</p>	<p>Zscaler's URL filtering provides advanced action capabilities beyond standard allow and block functions, including caution prompts, alert notifications, and isolation features to enhance security when accessing potentially risky websites.</p>

File Type Control

In addition to URL Filtering, Zscaler's **File Type Control** feature allows organizations to enforce policies on specific file types accessed by users. This capability is a key component of the **secure web gateway** functionality within **Zscaler Internet Access (ZIA)**.

Zscaler identifies file types by analyzing **MIME types, magic bytes (first few packets), and other content indicators** to accurately determine the file type involved in a transaction. Policies can be applied at a granular level, considering factors such as **user, group, location, and application**. However, **File Type Control policies must be associated with specific URL categories**, ensuring targeted enforcement based on web content.

File Type Control

Match files based on checking magic byte

Can be applied a user/group/location/app level

Allow, Block and Caution actions

- Archive
- 7-Zip (7z)
- Bzip2 (bz, bz2)
- Cab Archive (Cab)
- GZIP (gzip, gz)
- ISO Archive (iso)
- RAR Files (rar)
- Stuffit Archive (stuffit_sit, stuffit)
- Tar (tar, gtar, tar)
- ZIP (zip)
- ZIP w/Suspicious Script File (js, vbs, svg, ps1, hta, cmd, ink)
- Audio
- MP3 Files (mp3)
- Ogg Vorbis (ogg)
- WAV Files (wav)
- Executable
- Executable Scripts (py, sh, bat)
- Microsoft Installer (msi)
- Windows Executables (exe, exe64, scr)
- Windows Library (dll4, dll, ocl, sys)
- Windows Shortcut (lnk)
- Other Documents
- Autocad Drawing (dwg)
- CATIA Graphical Representation File
- HTML Help (chm)
- HTTP Form data
- Ipt files
- PDF Documents (pdf)
- Postscript (ps, eps)
- SLDPRF File
- Undetectable File
- XPS
- Video
- 3GPP Files (3gpp)
- AVI Files (avi)
- Flash Video (flv)
- MKV Files
- MP4 Files (mp4)
- MPEG Video (mpeg, mpg)
- QuickTime Video (mov, qt)
- webM Files
- Windows Media Video (wmv)

The screenshot shows the 'Add File Type Control Rule' window. It includes fields for Rule Order (set to 2), Admin Rank (set to 7), Rule Name (File_Type_2), Rule Status (Enabled), and Rule Label. Below these are sections for CRITERIA, File Types (set to None), and URL Categories (set to Any). A table displays Unselected Items (Archive, 7-Zip (7z), Bzip2 (bz, bz2), Cab Archive (Cab), DMG (dmg), EGG (egg)) and Selected Items (0). At the bottom are buttons for Save, Cancel, and Clear Selection.

Administrators can define **allow, block, or caution** actions for various file types, enhancing security by restricting access to potentially harmful or unauthorized content. Zscaler provides a **comprehensive and continuously updated list of supported file types**, covering all commonly used formats in internet and cloud-based applications.

When combined with **URL Filtering**, File Type Control serves as a **first line of defense**, strengthening security within the **Zscaler Zero Trust Exchange** and helping organizations **prevent data leaks, mitigate threats, and enforce compliance policies** effectively.

Tenant Restriction

With Zscaler Tenant Restrictions, organizations can enforce policies that block access to unauthorized tenants while allowing access to approved corporate tenants. This capability ensures that users can only log in to Microsoft 365, Salesforce, or other SaaS applications using corporate-approved accounts while preventing personal or external accounts from being accessed.

Zscaler enables tenant restrictions across all users, whether they are on or off the corporate network, providing flexible and consistent policy enforcement. These policies help organizations prevent data exfiltration, ensure compliance, and enhance security by restricting SaaS access based on corporate identity and policies.

Review:

Let's summarize the key takeaways from this section:

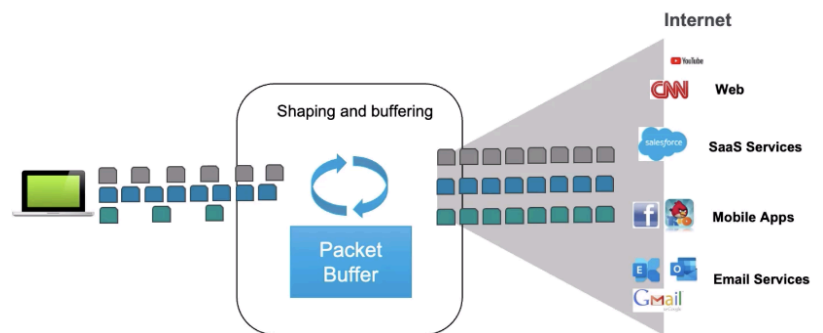
- **Significance of URL Filtering** – URL filtering serves as a **critical first layer of security**, enabling organizations to manage internet access effectively, enhance productivity, and reduce legal risks.
- **Key Use Cases** – It helps categorize and **isolate new or ambiguous websites in real-time**, protecting against malicious activities and unknown threats.
- **Zscaler's Differentiation** – Zscaler's **extensive global URL database**, multilingual customizable block pages, and **AI/ML-driven content categorization** make its URL filtering more advanced and effective.
- **Granular Policy Controls** – Zscaler's **highly customizable URL filtering policies** allow rule enforcement based on **user, device, location, and time-based criteria**, ensuring **secure and efficient internet access** tailored to business needs.
- **File Type Control Integration** – Zscaler's **File Type Control** works alongside URL filtering to enforce **granular policies on downloadable file types**, **strengthening security** and acting as a **first line of defense against cyber threats**.

Bandwidth Control

Bandwidth control is a core capability of **Zscaler's Access Control Services**, ensuring **secure and optimized connectivity** to internet and private applications. Organizations use **bandwidth control** to improve the performance of productivity apps like **Microsoft 365 and Salesforce**, limit non-essential traffic (**YouTube, Netflix, social media, etc.**), and manage bandwidth for software updates or specific locations.

Zscaler employs an **adaptive algorithm** that fully utilizes available bandwidth **unless contention occurs**, at which point **bandwidth policies** manage prioritization. By terminating **TCP sessions at the ZIA Public Service Edge**, Zscaler controls **window sizing, buffering, and traffic shaping** to optimize bandwidth usage. Unlike traditional **packet-dropping methods**, Zscaler **smooths out traffic flow** using shaping and buffering techniques, preventing disruptions in performance.

Zscaler Bandwidth Control

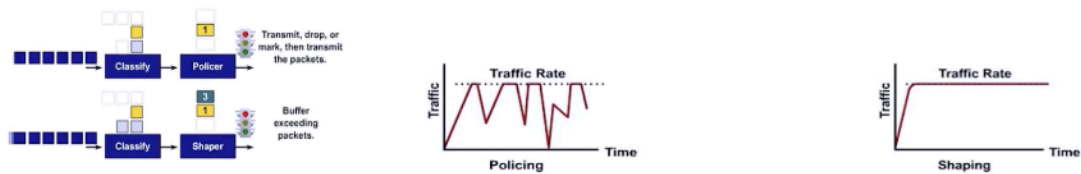


- Algorithm allows full utilization of BW unless there is contention
- Once beyond quota, packets are buffered (shaping and buffering vs. packet drop/policing)
- Slow down applications using TCP window size and other techniques

Policing vs. Shaping: Key Differences

- **Policing** – Drops excess packets when traffic exceeds a set limit, often leading to **TCP retransmissions, video buffering, and degraded performance**. This method is useful for applications where small packet loss is tolerable, such as **UDP streaming and voice traffic**.
- **Shaping** – Uses **buffering** to **smooth traffic flow**, preventing packet loss and ensuring consistent application performance. For instance, shaping **reduces video resolution dynamically** rather than causing buffering or playback issues. This approach is ideal for **web traffic, SSL-based applications, and latency-sensitive services**.

Policing vs. Shaping



	Policing	Shaping
Goal	Drop excess traffic beyond set limit. (typical UTM boxes). Also called "rate limit."	Delay (buffer) above committed rate traffic in a queue for later transmit
Direction	Inbound and outbound	Outbound
Bursts	Transmitted as is with sawtooth. Drop excess	Smooths out traffic rate, buffer excess
TCP traffic behavior	Drops causes TCP retransmits (YouTube resets) — choppy video	Minimizes TCP retransmits by buffering — smoothens YouTube at 480p vs 720p.
Queuing	Not performed	Queuing is performed with high memory buffers
Commonly used	Delay sensitive traffic (UDP, voice)	Delay insensitive traffic that can bear latency

By leveraging **shaping over policing**, Zscaler ensures **seamless user experiences** while maintaining **optimized bandwidth distribution**, prioritizing critical business applications, and preventing congestion.

What is the default behavior of Zscaler's Bandwidth Control?	How does Zscaler manage TP connections for bandwidth control?	What distinguishes Zscaler's bandwidth shaping from bandwidth policing?
--	---	---

By default, **Zscaler maximizes available bandwidth** unless a policy is configured to manage contention, ensuring optimal utilization while dynamically prioritizing traffic as needed.

Zscaler acts as a **TCP proxy**, optimizing bandwidth by **adjusting TCP window size and buffering traffic** instead of dropping packets. This approach ensures **smoother application performance** and prevents disruptions caused by congestion.

Unlike bandwidth policing, which **drops packets** once a threshold is exceeded, Zscaler's **bandwidth shaping** uses **buffering techniques** to **smooth traffic flow**, prevent packet loss, and **maintain a seamless user experience**.

Configuring Bandwidth Control

Bandwidth control is configured at the **location level** to manage available bandwidth per site. When setting up a location, you can enable **bandwidth control**, which will also apply to its sub-locations. Once enabled, you need to specify the **upload and download Mbps** that Zscaler's **Public Service Edge** will manage for that location's internet circuit.

After configuring bandwidth control, you can monitor traffic patterns in the **historical bandwidth visibility dashboard** to analyze **inbound and outbound traffic fluctuations** and adjust settings accordingly.

Defining Bandwidth Classes

Zscaler provides **eight predefined bandwidth classes** and allows up to **17 custom bandwidth classes**. Predefined classes cover **common URL categories**, making them easy to configure, while custom classes let you tailor policies based on actual network usage.

Before defining bandwidth classes, it's recommended to **observe bandwidth usage** by enabling bandwidth control without creating classes on the first day. Use **web overview dashboards or QBR reports** to identify the most commonly used applications and traffic patterns, then **categorize traffic into appropriate bandwidth classes** based on utilization reports.

Bandwidth Classes

- Customer issues — What Bandwidth classes should I define and how? What applications are running in my network that I should prioritize?
 - [QBR reports](#) — app usage (top streaming apps, social networking apps, top productivity apps)
 - Web insights
- There are 8 pre-defined BW Classes and up to 17 custom BW Classes can be created

Creating Bandwidth Control Rules

Bandwidth control rules define how bandwidth is allocated across applications and services. When creating a rule, you can specify:

- **Location** where the policy applies, including sub-locations
- **Time of enforcement** (e.g., during work hours)

BW Control Rule Order is critical

- BW Class in highest rule order gets BW first; followed by second and so on
- First BW rule should ideally be for critical apps with 0-100% BW

Min BW %

- Use Min BW % to reserve BW for productivity apps during contention
- Sum of Min BW % should not exceed 100% per location (system enforced)

Max BW %

Use Max BW % to cap *bad* traffic at specified time in BW Control rules

- **Rule order, name, and admin ranking**
- **Protocols** (HTTP, HTTPS, FTP, DNS, etc.)

The **most critical setting** in bandwidth control is the **action**—defining how bandwidth is allocated between **business-critical** and **non-business** applications.

- **Minimum Bandwidth:** Reserves bandwidth for **essential productivity apps** (e.g., Office 365, Salesforce). This ensures that a certain percentage of bandwidth is always allocated to critical services.
- **Maximum Bandwidth:** Limits bandwidth for **non-essential applications** (e.g., YouTube, social media, gaming), restricting them to a set percentage of available bandwidth.

The **minimum bandwidth allocation cannot exceed 100%**, as it is system-enforced. The **maximum bandwidth ensures non-critical apps do not consume excessive network resources**, preserving performance for business applications.

Like other Zscaler policies, **rule order matters**, so prioritizing bandwidth rules ensures the right allocation for each application category.

Key Concepts:

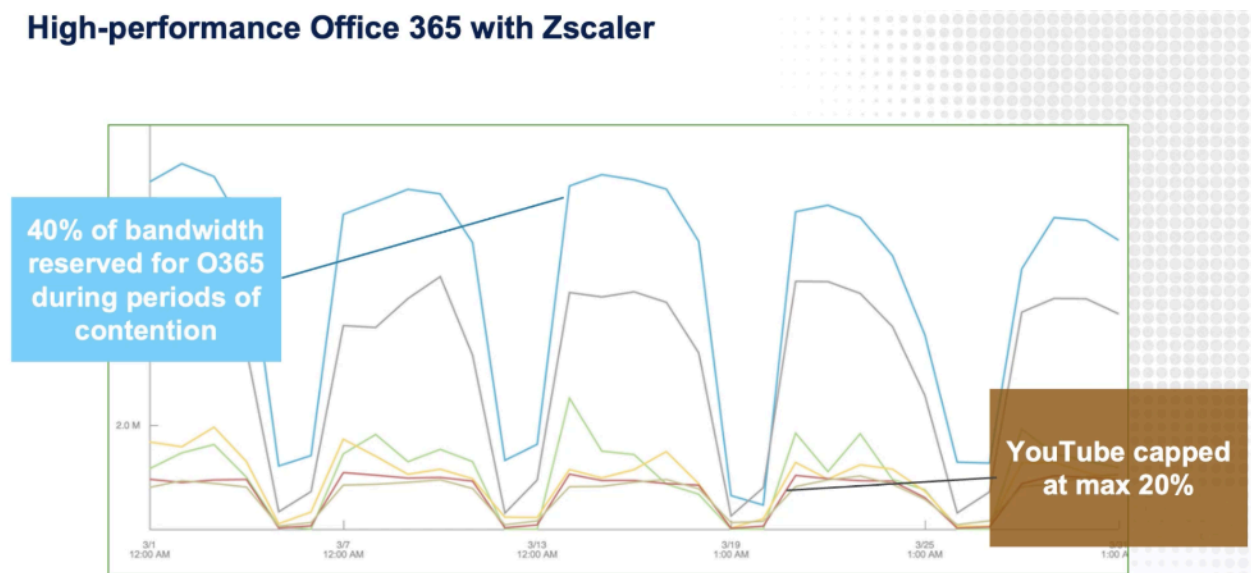
How is Bandwidth Control initially set up in Zscaler?	What are bandwidth classes in Zscaler's Bandwidth Control?	How does Zscaler ensure optimal bandwidth usage for different applications?
Bandwidth Control is configured at the location level by defining the upload and download speeds (Mbps) that Zscaler's Public Service Edge will manage. This setting ensures traffic is efficiently allocated based on the available bandwidth for that location. Once enabled, the configuration applies to all sub-locations , allowing for consistent bandwidth management across the organization.	Zscaler utilizes predefined and custom bandwidth classes to regulate traffic based on application types, such as file sharing, streaming, or social media . These classes help prioritize business-critical applications while managing non-essential traffic to optimize overall bandwidth usage.	Zscaler optimizes bandwidth usage by enforcing minimum and maximum bandwidth limits through configurable rules. This ensures that business-critical applications receive guaranteed bandwidth , while non-essential traffic, such as streaming or social media, is restricted to prevent network congestion.

Bandwidth Control Use-Cases

Now that we've explored how Zscaler's Bandwidth Control works, let's revisit key **real-world use cases** where it optimizes network performance:

- **Prioritizing Productivity Apps:** Ensuring business-critical applications like Office 365, Salesforce, and collaboration tools receive **higher priority** over non-essential traffic.
- **Limiting Bandwidth for Non-Productivity Apps:** Managing consumption for entertainment or social media applications like YouTube, Facebook, and TikTok to **prevent network congestion**.
- **Optimizing O365 Performance While Restricting Other Apps:** Allocating maximum bandwidth to collaboration apps while controlling media streaming and other bandwidth-intensive applications.

High-performance Office 365 with Zscaler



Prioritizing Productivity Apps

To guarantee bandwidth for critical business applications, Zscaler allows **creating bandwidth classes** that dynamically allocate available bandwidth:

Use Case 1 — Improve performance of productivity apps by prioritizing these apps over others

Bandwidth Control

Configure Bandwidth Control Policy
Rules are evaluated in the order specified. Rule evaluation stops at first match. Unless otherwise defined, URLs fall into General Browsing by default.

+ Add Bandwidth Control Rule

Rule Or...	Admin ...	Rule Name	Criteria	Action	Description
1	7	Bandwidth_Gold	BANDWIDTH CLASSES BW_Class1 PROTOCOLS DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP ov...	Bandwidth Limits: 0 - 100%	
2	7	Bandwidth_Silver	BANDWIDTH CLASSES BW_Class2 PROTOCOLS DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP ov...	Bandwidth Limits: 25 - 100%	
Default	7	Default Bandwidth Co...	PROTOCOLS Any	Bandwidth Limits: 0 - 100%	Default Bandwidth Rule

In this case O365 gets required BW at all times. During contention, Outlook and OneDrive will get at least 25% of BW.
Note: Use this config when not sure about *bad* traffic.

- **Gold Class:** Reserves up to **100% of available bandwidth** for key productivity applications, ensuring priority access when network contention arises.
- **Silver Class:** Provides up to **25-100% bandwidth** for applications like OneDrive and Outlook, ensuring flexibility if the Gold Class does not fully utilize available bandwidth.
- **Default Class:** Ensures that remaining bandwidth is distributed efficiently across all other applications.

This setup **prioritizes mission-critical apps** while ensuring available bandwidth is not wasted.

Limiting Bandwidth for Non-Productivity Apps

In contrast, bandwidth restrictions can be applied to non-essential applications:

Use Case 2 — Limit BW for non-productivity apps at all times

Bandwidth Control

Configure Bandwidth Control Policy

Rules are evaluated in the order specified. Rule evaluation stops at first match. Unless otherwise defined, URLs fall into General Browsing by default.

In this case non-productivity apps will have max BW of 50% at all times.

Note: This does not guarantee more BW for productivity apps.

Add Bandwidth Control Rule

Recommended Policy

Search...

Rule Or...	Admin ...	Rule Name	Criteria	Action	Description
1	7	Bandwidth_1	BANDWIDTH CLASSES BW_Class1 PROTOCOLS DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP ov...	Bandwidth Limits: 0 - 50%	
Default	7	Default Bandwidth Co...	PROTOCOLS Any	Bandwidth Limits: 0 - 100%	Default Bandwidth Rule

- **Social Media & Streaming Apps (Facebook, Netflix, YouTube, TikTok, etc.)** are grouped into a **limited bandwidth class**.
- Example: **Capping these applications at 50%** of available bandwidth at all times, ensuring that even if excess bandwidth exists, it remains reserved for productivity apps.
- This guarantees that **no more than 50%** of the available bandwidth is used for non-essential applications, maintaining network efficiency.

This method **ensures balance**—allowing some access to non-essential applications without compromising productivity.

Enhancing Office 365 & Collaboration App Performance

For organizations reliant on O365 and collaboration tools, Zscaler allows:

Use Case 3 — Improve performance of O365 and limit BW for non-productivity apps

Bandwidth Control

Configure Bandwidth Control Policy
Rules are evaluated in the order specified. Rule evaluation stops at first match. Unless otherwise defined, URLs fall into General Browsing by default.

+ Add Bandwidth Control Rule

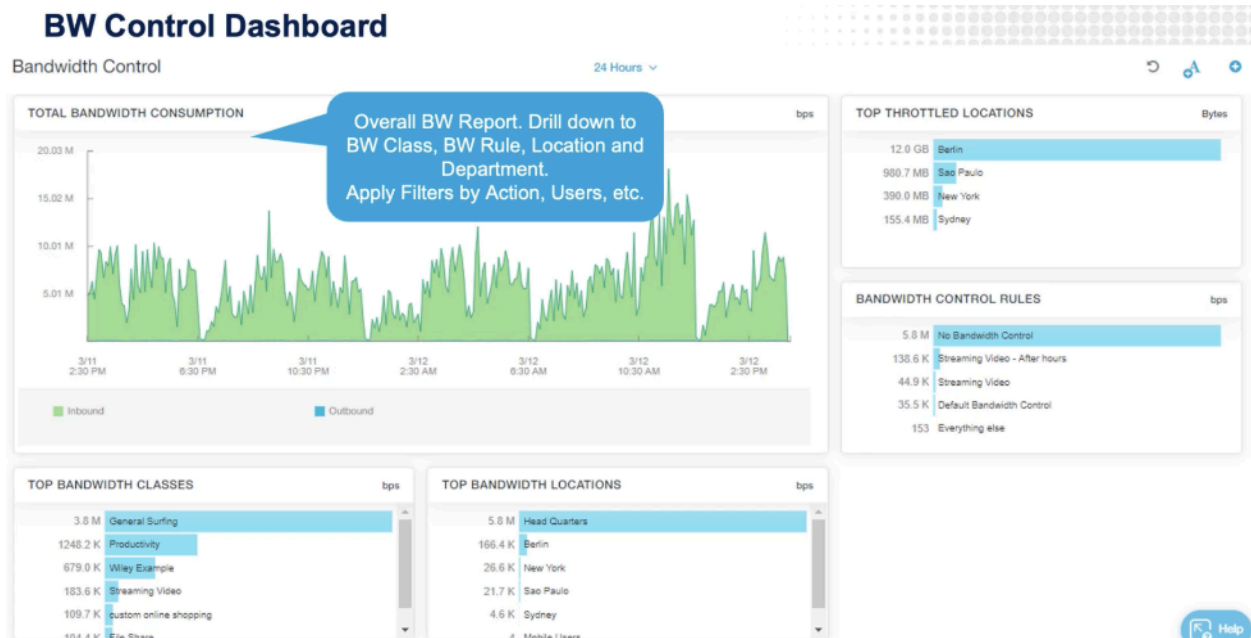
Rule Or...	Admin ...	Rule Name	Criteria	Action
1	7	Bandwidth_1	BANDWIDTH CLASSES BW_Class1 PROTOCOLS DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP ov...	Bandwidth Limits: 0 - 100%
2	7	Bandwidth_2	BANDWIDTH CLASSES BW_Class2 PROTOCOLS DNS Over HTTPS; Tunnel SSL; HTTP Proxy; FTP ov...	Bandwidth Limits: 0 - 50%
Default	7	Default Bandwidth Co...	PROTOCOLS Any	Bandwidth Limits: 0 - 100% Default Bandwidth Rule

In this case O365 gets required BW at all times and non-productivity apps get max 50%.
Note: Use this config when sure about *bad* traffic.

- **Creating separate bandwidth classes** for O365 and media applications.
- **Applying a priority rule** that ensures O365 **always gets bandwidth preference** over streaming and other non-essential services.
- **Dynamic allocation based on need**, ensuring that O365 remains **uninterrupted** during peak business hours.

Visibility & Reporting

The **Bandwidth Control Dashboard** provides **historical insights** into inbound/outbound traffic usage, highlighting:



- **Top bandwidth-consuming applications**
- **Locations experiencing throttling**
- **Bandwidth control rules being triggered**

A real-world example demonstrates how **Office 365 consistently receives higher priority** over YouTube during working hours. This ensures **optimal bandwidth allocation**, preventing slowdowns for critical business applications while maintaining a smooth user experience.

By leveraging **Zscaler's Bandwidth Control**, organizations can **boost collaboration, enhance productivity, and ensure optimal bandwidth distribution** across their network infrastructure.

Review

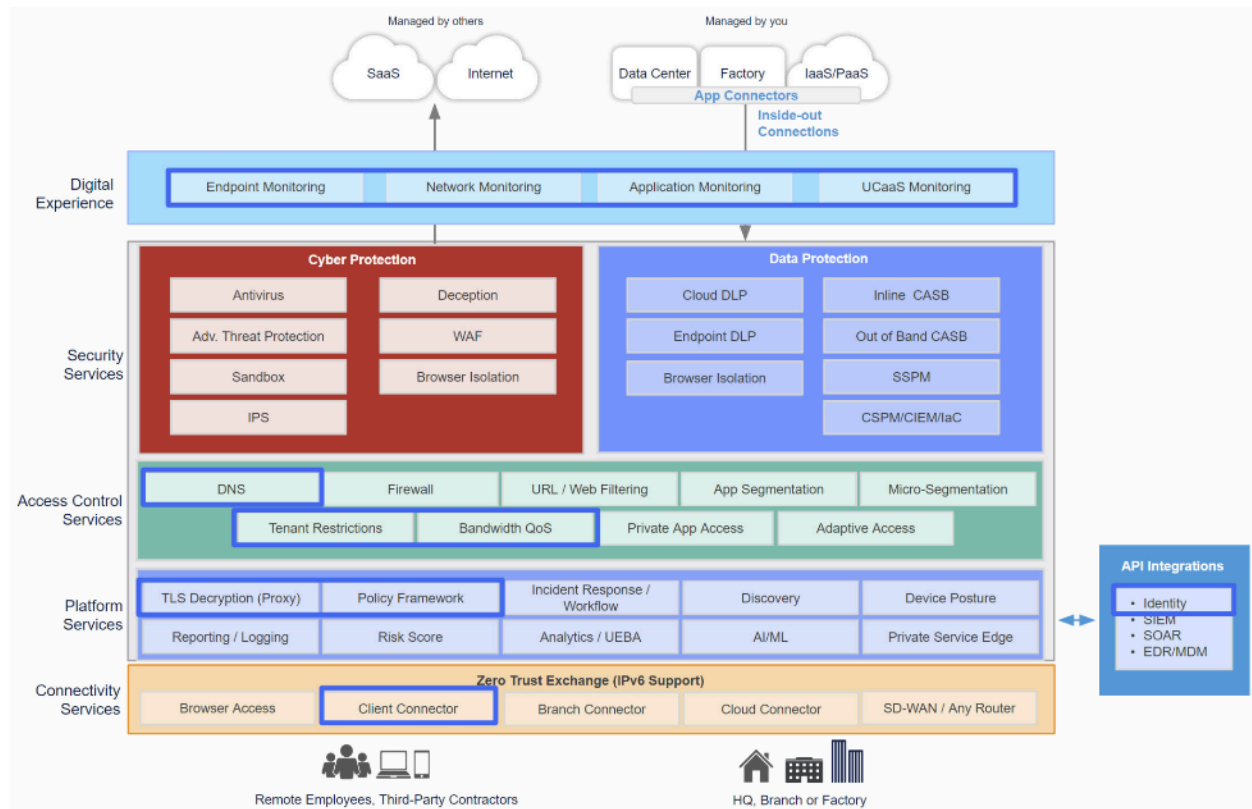
Let's summarize the key insights from this section:

- **Zscaler Bandwidth Control:** Unlike traditional packet-dropping methods, Zscaler utilizes **shaping and buffering technologies** to dynamically adjust TCP window sizes, ensuring **smooth application performance** without unnecessary traffic loss.
- **Optimized Bandwidth for Critical Applications:** Business-critical apps like **Office 365 and Salesforce** receive **priority bandwidth allocation**, ensuring productivity is not impacted by non-essential traffic.
- **Shaping vs. Policing:** Unlike **policing**, which simply **drops packets** exceeding bandwidth thresholds, Zscaler's **shaping approach buffers excess traffic**, maintaining seamless performance, particularly for TCP and SSL-based applications.
- **Granular Bandwidth Control Configuration:** Bandwidth settings are **configured per location**, allowing organizations to **fine-tune traffic distribution** and prioritize essential applications while limiting non-productive usage.

With these capabilities, Zscaler ensures **efficient bandwidth utilization**, improving network performance and user experience across all locations.

Microsoft 365 (M365) Deployment with Zscaler





After discussing Zscaler's capabilities in **bandwidth and network configurations**, it's crucial to explore how Microsoft 365 (M365) deployments face challenges using **traditional network models** and how Zscaler overcomes them.



A key element of **Zscaler's Access Control Services** is its **secure local internet breakout for M365 traffic**, designed to improve efficiency and reduce latency. By enabling **direct and secure connections**, Zscaler enhances M365 performance across applications like **Exchange Online, Teams, SharePoint, and OneDrive** while maintaining robust security.

Beyond **URL Filtering** and **Bandwidth Control**, Zscaler integrates **TLS Inspection, Policy Framework, and the Zscaler Client Connector** into the **Zero Trust Exchange**, ensuring organizations can optimize Microsoft 365 traffic **without compromising security**.

Issues with the traditional model for Office 365 traffic

Exchange Online 	Microsoft Teams 	SharePoint Online & OneDrive for Business 	Office and Windows updates 
Latency due to distance and operations	Traditional proxies don't handle User Datagram Protocol (UDP) traffic	Additional persistent connections by client	High update frequency
Outlook requires multiple TCP connections per user (5–10)	Additional persistent connections by client	Large amount of data movement	Risk of bandwidth saturation due to repeated downloads for each machine
Designed for transient rather than persistent connections	Teams media traffic prefers UDP for transport	Same destination IP used for all connections	Microsoft 365 app updates range from about 100–500 MB and can be numerous each year depending on channel
	Media traffic can add high load		

Legacy deployment models struggle with M365 applications due to inefficient traffic routing and network constraints:

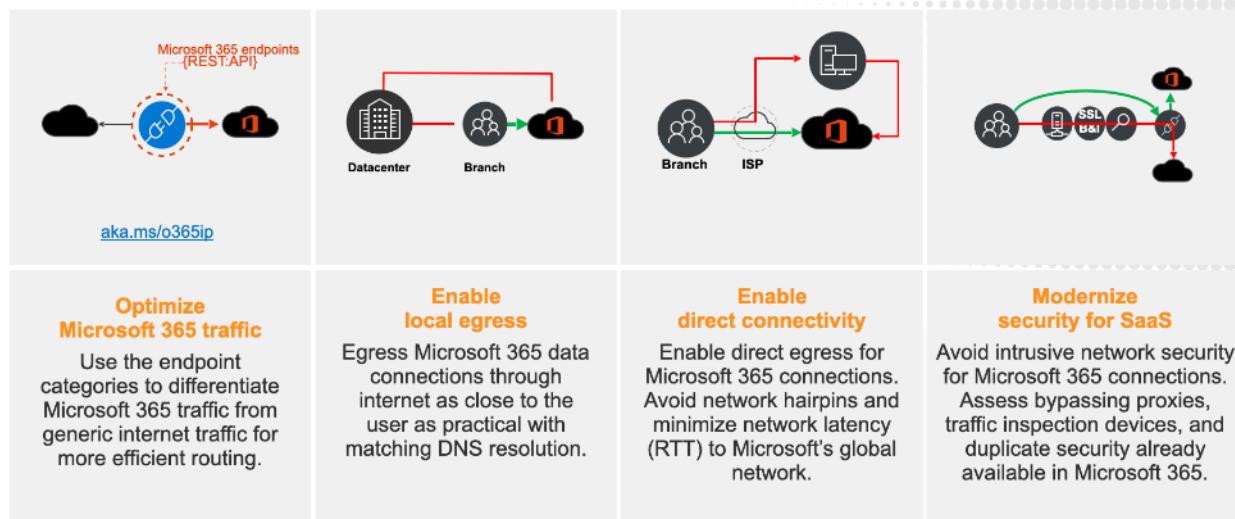
- **Exchange Online:** Requires multiple long-lived **TCP connections** per user, increasing strain on firewalls and on-premises infrastructure. A small branch with 50 users can generate over **1,000 persistent connections**, overwhelming traditional firewalls.
- **Teams:** Relies on a **control channel** and **UDP-based audio/video traffic**, requiring **low-latency routing and efficient DNS resolution**. A hub-and-spoke network **increases path latency**, degrading call quality.
- **SharePoint & OneDrive:** Involve **persistent data transfers**, demanding **direct, high-speed access** to Microsoft endpoints. Poor network design can severely impact performance.
- **Office & Windows Updates:** Frequent updates consume significant bandwidth (100-500MB per user), and if unmanaged, can **slow down business-critical applications** during peak hours.

Microsoft 365 Network Connectivity Principles

To address **network challenges in M365 deployments**, Microsoft has established key **network connectivity principles** to optimize **traffic flow**, **reduce latency**, and **enhance security**. Zscaler, as the **first certified security partner in Microsoft's networking program**, fully aligns with these principles to enable **secure and efficient local internet breakouts**.

Key Microsoft 365 Network Connectivity Principles:

Microsoft 365 network connectivity principles



1. Optimize Microsoft 365 Traffic

Microsoft categorizes its **IP addresses, domains, and ports** via an API, providing a constantly updated list through the [aka.MS/o365 IP portal](https://aka.ms/o365ip). Organizations must continuously **identify and prioritize M365 traffic** to ensure optimal performance. Zscaler automates this process, eliminating the need for **manual updates** across multiple locations.

2. Enable Local Egress

Microsoft recommends **direct local egress** rather than routing M365 traffic through **centralized data centers**. This ensures **DNS resolution** occurs near the user, **not the data center**, reducing latency and improving performance. Zscaler enables **intelligent local egress**, optimizing connectivity for M365 services.

3. Enable Direct Connectivity

Traditional hub-and-spoke architectures add unnecessary delays when connecting to M365. Microsoft advises enabling **direct internet access** from branch offices to **Microsoft front doors**, avoiding **network bottlenecks**. Zscaler facilitates **direct, secure M365 access** without compromising security.

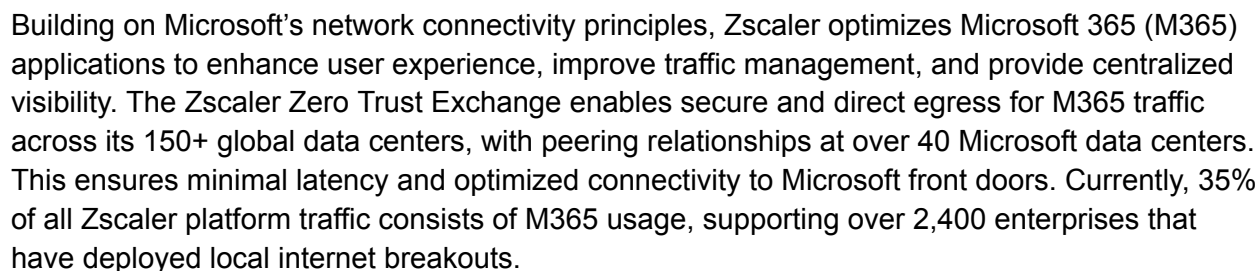
4. Modernize Security for SaaS

Microsoft **discourages SSL inspection** on M365 traffic, as it can **disrupt protocols** like MAPI and degrade user experience. Instead, Microsoft recommends **bypassing security appliances like proxies and firewalls** to prevent performance issues. Zscaler ensures that **trusted M365 traffic is intelligently bypassed** while maintaining **strong security and compliance controls**.

By fully integrating **Microsoft's connectivity best practices**, Zscaler ensures **optimal M365 performance**, providing **seamless access, reduced latency, and enhanced security** across all enterprise locations.

Key Concepts:

What is the first principle of Microsoft's network connectivity?	How does Microsoft recommend handling DNS for M365 traffic?	What is Microsoft's stance on SSL traffic inspection for its applications?
Microsoft provides endpoint details , including URLs, IP addresses, ports, and protocols , through the aka.MS/o365 IP portal . Network operators must use this information to identify, prioritize, and optimize Microsoft 365 traffic at each branch office , ensuring seamless connectivity and performance.	Microsoft recommends configuring DNS to resolve near the user's location, ensuring intelligent local egress for improved connectivity and performance.	Microsoft advises against SSL traffic inspection for its applications to prevent user experience issues and IT disruptions, recommending minimal proxy or firewall interference.



172

Increased load on firewalls and proxies

- Office 365 creates a high number of long-lived sessions that quickly exhaust firewall ports (we've seen 12-20 connections per user)
- Around 2,000 clients can be supported by a single public IP safely (may require architectural changes)
- Office 365 use will require more than Web browsing (ports 80/443) — uses ephemeral ports



IMPACT ON THE USER EXPERIENCE

Random hangs and connection issues
(Outlook in a disconnected state)

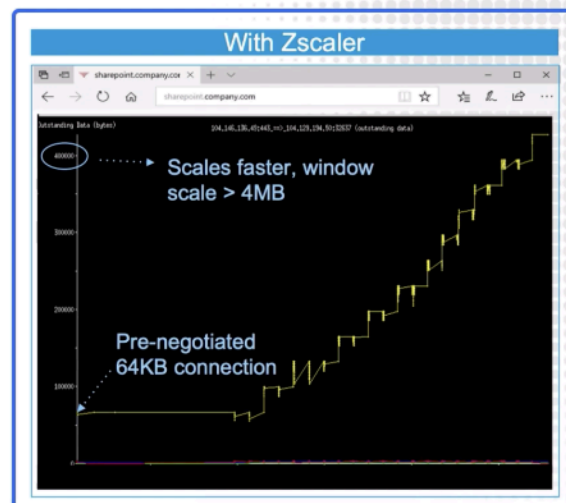
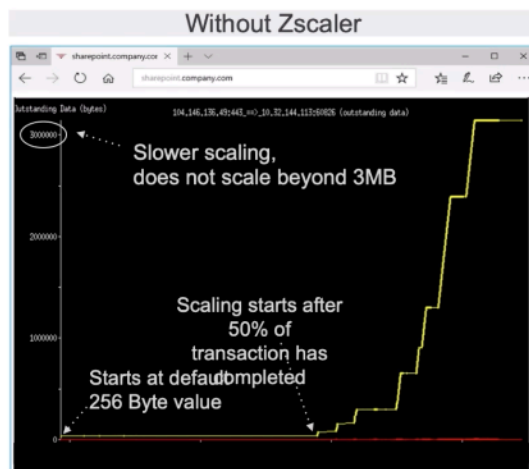
TCP	10.32.147.199:49362	173.194.33.21:443	TIME WAIT
TCP	10.32.147.199:49618	23.72.104.134:443	ESTABLISHED
TCP	10.32.147.199:49623	74.125.239.32:443	ESTABLISHED
TCP	10.32.147.199:49629	132.245.4.137:443	ESTABLISHED
TCP	10.32.147.199:49633	138.91.137.28:10106	ESTABLISHED
TCP	10.32.147.199:49637	138.91.137.28:10106	ESTABLISHED
TCP	10.32.147.199:49645	19.32.146.250:137	TIME WAIT
TCP	10.32.147.199:49647	70.37.98.82:443	ESTABLISHED
TCP	10.32.147.199:49645	70.37.97.234:443	ESTABLISHED
TCP	10.32.147.199:49667	70.37.97.234:443	ESTABLISHED
TCP	10.32.147.199:49668	70.37.97.234:443	ESTABLISHED
TCP	10.32.147.199:49669	70.37.97.234:443	ESTABLISHED
TCP	10.32.147.199:49671	70.37.97.234:443	ESTABLISHED
TCP	10.32.147.199:49672	70.37.97.234:443	ESTABLISHED
TCP	10.32.147.199:49672	161.69.92.10:443	ESTABLISHED
TCP	10.32.147.199:49672	23.72.95.56:80	ESTABLISHED
TCP	10.32.147.199:49718	157.56.38.46:443	ESTABLISHED
TCP	10.32.147.199:49722	132.245.113.24:443	ESTABLISHED
TCP	10.32.147.199:49722	132.245.113.24:443	ESTABLISHED
TCP	10.32.147.199:49716	65.55.127.47:443	ESTABLISHED
TCP	10.32.147.199:49717	65.55.127.47:443	ESTABLISHED
TCP	10.32.147.199:49728	65.55.127.47:443	ESTABLISHED
TCP	10.32.147.199:49722	65.55.127.47:443	ESTABLISHED
TCP	10.32.147.199:50012	157.56.245.118:443	ESTABLISHED
TCP	10.32.147.199:50017	132.245.0.44:53113	SYN_SENT
TCP	127.0.0.1:55679	132.245.113.23:443	ESTABLISHED
TCP	127.0.0.1:7438	0.0.0.0:0	LISTENING
TCP	127.0.0.1:8888	0.0.0.0:0	LISTENING
TCP	127.0.0.1:8888	127.0.0.1:49592	TIME_WAIT
TCP	127.0.0.1:8888	127.0.0.1:49602	TIME_WAIT
TCP	127.0.0.1:8888	127.0.0.1:49603	TIME_WAIT
TCP	127.0.0.1:8888	127.0.0.1:49604	TIME_WAIT

For SharePoint and OneDrive, large file transfers typically start with small TCP window sizes that gradually increase. Zscaler optimizes this by acting as a proxy, starting with a pre-negotiated 64KB TCP window and scaling up to 4MB, significantly improving upload and download speeds. Additionally, Zscaler enhances DNS resolution by automatically resolving M365 traffic locally using its distributed DNS resolvers, **ensuring the shortest path from your end user to the Microsoft front door**, which significantly improves the user experience and provides faster connectivity regardless of the location.

Optimized Zscaler TCP Scaling for faster file downloads



Differentiate O365 traffic



3MB file download from a SharePoint public site hosted at Iowa instance

Minimize Office 365 latency with Local DNS

Guarantee a fast, local connection regardless of location

Microsoft | TechNet

Local Egress & DNS



Zscaler Local DNS Architecture

San Jose User > San Jose DNS > San Jose O365
Shortest path, fewer hops = faster user experience

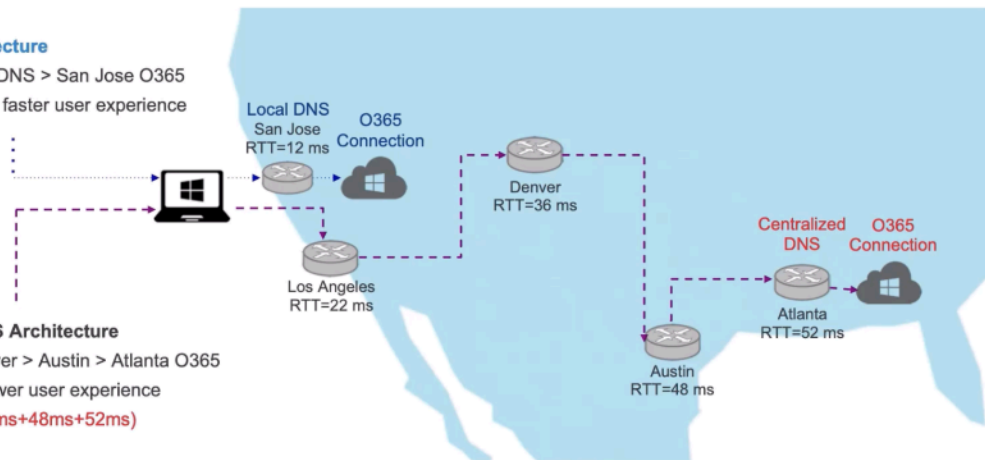
Latency: 12ms



Common Centralized DNS Architecture

San Jose user > LA > Denver > Austin > Atlanta O365
Lots of hops increases: slower user experience

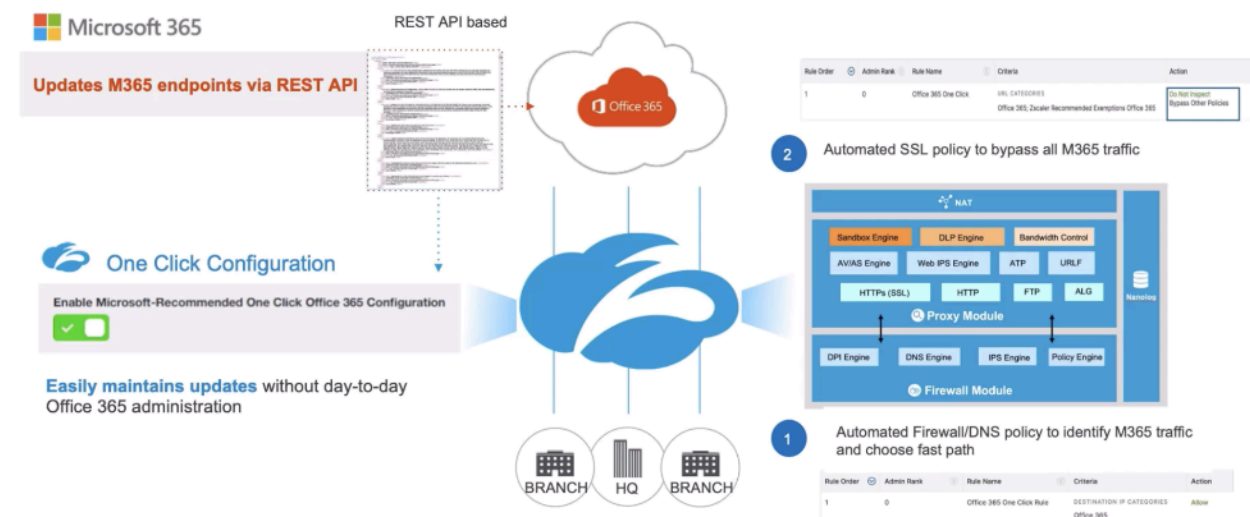
Latency: 158ms (22ms+36ms+48ms+52ms)



Zscaler's deep integration with Microsoft includes a REST-based API that continuously updates Microsoft's evolving IP addresses, endpoint URLs, and port lists. This enables enterprises to implement Microsoft's recommended **One Click** configuration, which automates access control policies, bypasses SSL inspection for M365 traffic, and ensures seamless, direct connectivity via Zscaler's Microsoft peering locations.

Zscaler One Click Configuration

Simplify day to day Office 365 administration



Visibility is another crucial advantage. Even without inspecting M365 traffic, Zscaler provides real-time insights into traffic volume, usage trends, top users, and bandwidth consumption across different locations. This helps IT teams optimize network planning while ensuring a seamless, high-performance M365 experience.

Key Concepts:

What is the first principle of Microsoft's network connectivity?	How does Microsoft recommend handling DNS for M365 traffic?	What is Microsoft's stance on SSL traffic inspection for its applications?
Zscaler optimizes Microsoft 365 traffic by routing it through its 150+ global data centers, leveraging direct peering with Microsoft to minimize latency and ensure the most efficient network paths.	Zscaler offers a one-click configuration for secure Microsoft 365 breakouts, optimizing TCP window scaling and DNS resolution to improve performance and user experience.	Zscaler integrates with Microsoft through a REST API for real-time updates, enabling efficient management of persistent connections and delivering comprehensive usage insights without traffic inspection.

M365 Deployment Best Practices

When deploying Microsoft 365, following best practices ensures optimal performance, security, and a seamless user experience. Zscaler offers a robust framework for managing M365 traffic through secure local internet breakouts, advanced traffic forwarding, and intelligent bypass configurations.

Traffic Forwarding and Secure Access

For optimal connectivity at branch offices, Zscaler recommends using **GRE or IPSec tunnels** for traffic forwarding. Authentication, SSL, and firewall settings should be enabled, though **SSL inspection does not apply to M365 traffic when using Microsoft's One Click configuration**. To prevent accidental drops in web traffic, ensure HTTP and HTTPS network service rules are allowed by default.

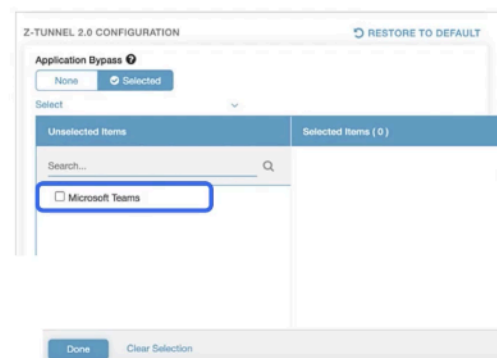
Optimizing Remote Work and Microsoft Teams

With the rise of remote work, **Microsoft Teams has become a critical business tool**. For the best user experience, Zscaler offers an **Application Bypass** feature. When deploying **Zscaler Client Connector with Z-Tunnel 2.0**, organizations should enable **Application Bypass for Teams**, which automatically detects and bypasses Teams traffic, including TCP and UDP. While TCP can still be routed through Zscaler selectively, **bypassing all Teams-related TCP and UDP traffic** is recommended to optimize performance. Additionally, **split tunneling** ensures that only M365 traffic is optimized while allowing other applications to follow a custom routing policy.

MS Teams deployment for remote users (WFA)

For optimal WFA user experience

- Deploy Zscaler Client Connector (with Z-Tunnel 2.0) for all WFA users.
- Login to the Zscaler admin portal and go to : Policy → Zscaler Client Connector portal.
- Add **Microsoft Teams** under Application bypass as shown below: App Profile → Windows → Add Windows Policy (modify existing profile as needed) Under Z-Tunnel 2.0 configuration → Application bypass → selected.



Enterprise Connectivity Principles

For **corporate locations** such as branch offices, headquarters, and data centers, Microsoft 365 traffic should be **forwarded via GRE/IPSec tunnels** with Microsoft's **One Click configuration enabled**. Avoid **split tunneling or bypassing specific locations**, as this can lead to **inconsistent routing, performance issues, and a poor user experience**.

For **work-from-anywhere users**, install **Zscaler Client Connector with Z-Tunnel 2.0** and configure **Microsoft Teams bypass** to ensure seamless connectivity.

Addressing Regulatory and Compliance Needs

Organizations subject to **strict compliance or data protection regulations** may require **full SSL inspection, even for M365 traffic**. In these cases, **Zscaler offers an alternative M365 One Click configuration**, which enables inspection while ensuring key Microsoft services remain functional. Some M365 URLs, particularly those with **pinned certificates, must be bypassed** to avoid service disruptions.

For **data security and access control**, Zscaler enables:

- **Granular policies for OneDrive and Outlook** (e.g., preventing file uploads to personal accounts).
- **Phishing detection in emails and attachments**.
- **CASB/SaaS Security API integration for advanced security controls**.

Teams Traffic Optimization for Inspected Deployments

Even when **SSL inspection is enabled**, for the best **user experience**, **bypassing UDP traffic for Microsoft Teams** is recommended. This allows organizations to monitor **TCP-based document sharing** while ensuring smooth voice and video performance.

Standard vs. Inspected Deployment Options

For enterprises focused on **connectivity and user experience**, Zscaler recommends following **Microsoft's standard One Click configuration**, which does **not inspect M365 traffic**.

For organizations needing **content inspection**, Zscaler supports:

- **Selective SSL Inspection** for login services to enforce **tenancy restrictions**.
- **Granular SSL policies** that inspect or bypass **specific categories of M365 traffic** based on Microsoft's recommended endpoint classifications (**Optimize, Default, and Allow**).

Recommended Connectivity to Zscaler

Location	Traffic Forwarding Options	Comments
Corporate Site (HQ or Branch Office)	<ul style="list-style-type: none">GRE or IPSEC is requiredConfigure Microsoft recommended one-click configuration setting	Send all ports and protocols traffic (including UDP) to Zscaler
Remote user (WFA)	Zscaler Client Connector (Tunnel2.0) with Application bypass (MS Teams) enabled	We've implemented the ability for customers to send Teams traffic direct to Microsoft 365. This should be configured in every Tunnel 2.0 ZCC implementation.

By following these best practices, organizations can **maximize Microsoft 365 performance, maintain security and compliance, and ensure a seamless experience** for both remote and on-site users.

Key Concepts:

Provide Direct Access to M365	Stop Backhauling and Hair Pinning	The Optimal Path to M365
Enable local internet breakouts and remove VPNs	Eliminate costly and slow MPLS connections	150+ global edge locations includes direct geographic peering

Review: Key Takeaways on Microsoft 365 Deployment with Zscaler

Challenges in Microsoft 365 Deployment

Deploying **Microsoft 365** can **strain on-premises infrastructure**, as each user requires multiple **persistent connections** for services like **Exchange Online, Teams, and SharePoint**. This leads to increased **bandwidth demand, firewall port exhaustion, and performance bottlenecks**. Efficient network planning is essential to support **high-traffic workloads and frequent updates** without compromising **performance or security**.

Microsoft 365 Connectivity Principles

To ensure **optimal M365 performance**, Microsoft recommends:

- **Traffic optimization** using **Microsoft's endpoint data** (URLs, IPs, and domains).
- **Local egress DNS resolution** to minimize latency by directing traffic to the nearest Microsoft front door.
- **Direct internet access from branch locations**, avoiding hub-and-spoke architectures that increase delay.
- **Avoiding SSL traffic inspection**, as breaking and inspecting M365 traffic can disrupt applications and degrade user experience.

Optimizing Microsoft 365 with Zscaler

Zscaler's **Zero Trust Exchange platform** is designed to enhance **M365 connectivity** by:

- **Providing direct egress** for M365 traffic through its **150+ global data centers**.
- **Establishing direct peering** with Microsoft at **40+ locations** to **minimize latency** and optimize connectivity.
- **Leveraging real-time REST API integration** with Microsoft to dynamically update endpoint configurations.

Best Practices for M365 Deployment

For **seamless deployment** and **optimized performance**, Zscaler recommends:

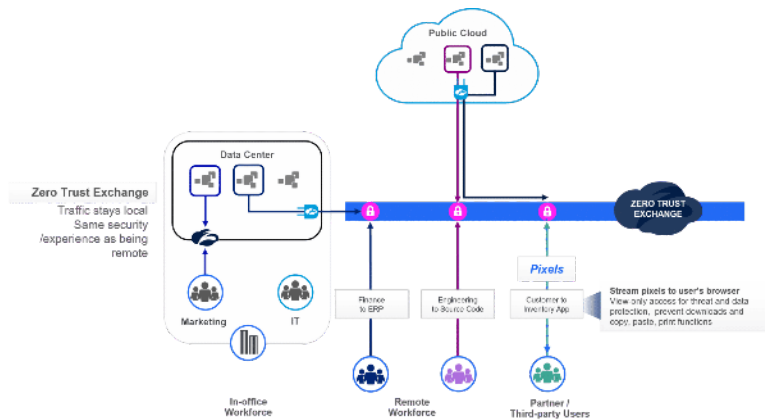
- **Using GRE or IPSec tunnels** for secure traffic forwarding.
- **Maintaining SSL and firewall settings**, ensuring Microsoft 365 traffic is managed efficiently.
- **Enabling Microsoft's One Click configuration**, which automates policy updates, prioritizes bandwidth, and simplifies connectivity management.

By **adopting these best practices**, organizations can achieve **high-performance Microsoft 365 deployments**, ensuring **seamless user experience, reduced latency, and enhanced security** while **minimizing operational complexity**.

Segmentation & Conditional Access through Policies

Private Application Access

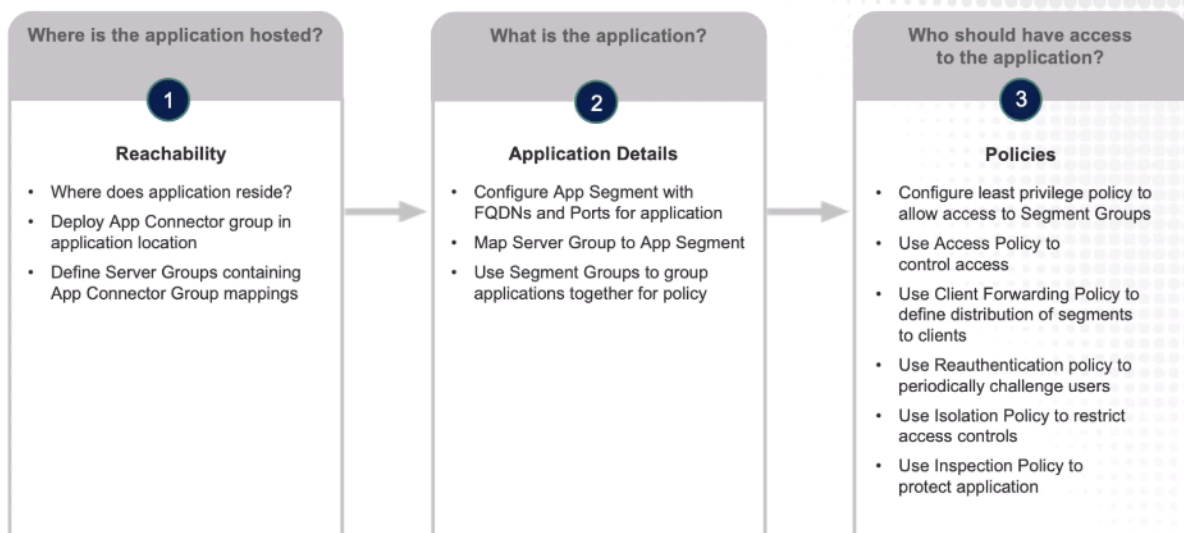
Zscaler's **Private Application Access** enables **secure, seamless connections** to an organization's **private applications**, ensuring users can **access only what they are authorized for**—without being placed on the corporate network. This **Zero Trust** approach eliminates the risks of **lateral movement**, enforcing strict **application-level access controls** based on user identity, device posture, and contextual security policies.



Three Pillars of Secure Private Application Access

To configure and implement **Zscaler Private Access (ZPA)** effectively, we focus on three key pillars:

Overview of configuration steps for secure private application access



1. Reachability & Application Connectors

- Deploying **App Connectors** to establish a secure outbound connection to private applications.
- **Best practices** for deploying connectors efficiently while ensuring minimal latency and optimal performance.

- **Application discovery methods** to identify and catalog accessible private applications.

2. Application Configuration

- **Defining application segments** based on security policies.
- Configuring **browser-based access** for agentless access scenarios.
- Implementing **isolation** for high-risk applications.
- **User and privileged portals** for secure and organized access control.

3. Access Policies & Security Controls

- **Creating and enforcing access policies** to govern private application access.
- Applying **context-aware security policies** for **user authentication, device posture, and risk-based access**.
- Enabling **inspection and additional security controls** for sensitive applications.

By implementing these **three pillars**, organizations can **enable Zero Trust private application access**, ensuring **secure, seamless, and policy-driven connectivity** while **eliminating the risks associated with traditional VPNs and network-based access models**.

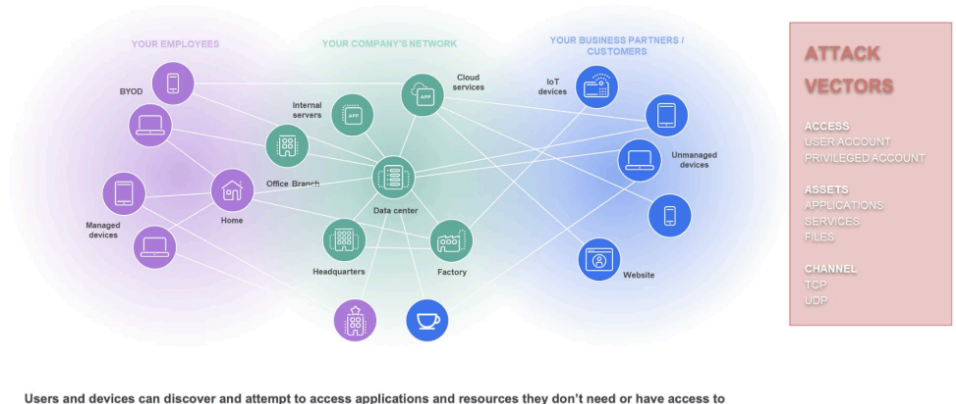
Modern Segmentation with Zero Trust

The Flaws of Legacy Segmentation

Traditional network segmentation approaches require placing users **inside the corporate network**, exposing organizations to increased **attack surfaces** and enabling **lateral threat movement**. Legacy solutions, such as VPNs, inherently grant access to an entire network, allowing attackers to exploit exposed applications, steal credentials, and move laterally across systems.

Moreover, as corporate networks **blend** with employee home networks, partner environments, and customer interactions, **attack surfaces expand**, making it easier for bad actors to gain unauthorized access. In reality, **most users and devices should not even be aware of, let alone have access to, private applications unless explicitly required**.

Traditional VPNs provide open access to all devices on the network



Zero Trust Segmentation with Zscaler

Rather than granting broad network access, **Zscaler applies Zero Trust segmentation**, allowing users to connect only to the **specific applications they need—without ever being placed on the network**. By eliminating network access, organizations remove the ability to **discover, probe, or move laterally** to unauthorized applications and resources.

Why segmentation?

Segmentation limits the network access only to the application or resource required

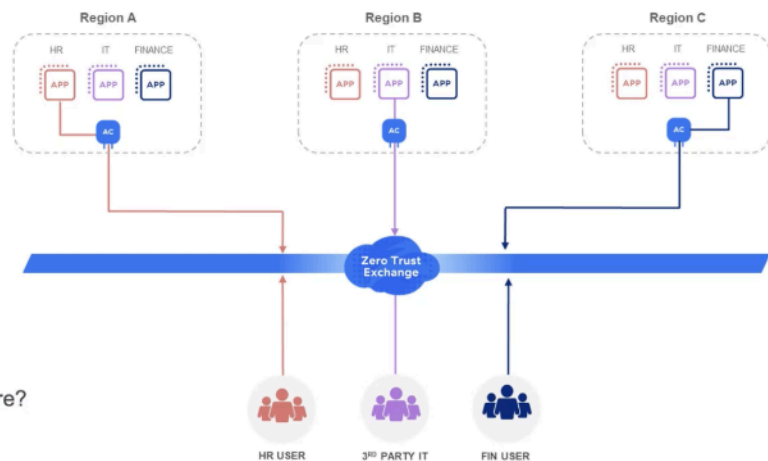
Contrast to traditional VPNs that provide access to all resources on the network when the user or device connects

Eliminates discovery of applications not granted access to

Segmentation uses policies to provide conditional access when the application is requested

Policies are based on:

1. Identity — is the user who they say they are?
2. Device posture — Is the device secure?
3. Access — Should the user have access to the application?



For example, an **HR user should only see and access HR applications**—even if other applications, such as finance or engineering tools, exist within the same region or cloud environment. **Unauthorized applications remain invisible** to those who don't have explicit access.

5 steps for segmenting applications

List your critical Applications.



App Risk Tiering

Ask your Application Owners.



App Owner Guidance

Let ZPA discover your Applications.



Wildcard Discovery

Who's accessing which Applications?



User App Access Discovery

Which users should have priority access?



User-focused granularity

Three Core Segmentation Approaches

1. User-to-Application Segmentation

- Limits access **based on user identity, device posture, and business policies**.
- Ensures **employees, third-party contractors, B2B suppliers, and other users** only access the applications relevant to their roles.
- **Prevents lateral movement by connecting users to applications, not networks.**

2. Workload Segmentation in Hybrid & Multi-Cloud Environments

- Enforces **least-privilege principles** across **VPCs (Virtual Private Clouds), cloud services, and data centers**.
- Secures **cloud-to-cloud and cloud-to-data center communications**, preventing unauthorized access.

3. Identity-Based Micro-Segmentation

- **Uniquely identifies** applications and processes to **automate least-privileged access** for workload communications.

Bonus: Use **decoy workloads and applications** (Zscaler Deception) as a proactive security measure to deceive and deter attackers.

By **removing implicit trust and enforcing granular segmentation policies**, organizations can **eliminate lateral movement, enhance security, and successfully implement Zero Trust segmentation** with Zscaler.

Key Concepts:

How does traditional network access contribute to security risks?	How does Zscaler's Zero Trust approach to segmentation differ from traditional methods?	What are the three ways Zscaler handles segmentation?
Traditional VPNs expose the internal network, increasing security risks by allowing users broad access and enabling lateral movement, which compromises security and drives up infrastructure costs.	Zscaler restricts access to only necessary applications or resources, keeping users off the network to minimize attack surfaces and eliminate lateral movement risks.	Zscaler enforces user-to-application segmentation, workload segmentation across hybrid and multi-cloud environments, and identity-based microsegmentation to ensure secure, isolated access.

Application, Application Segment, and Segment Group

An application is defined by its fully qualified domain name (FQDN), local domain name, or IP address on specific standard ports. These applications must be organized within an application segment.


Application Segments and Segment Groups

An application segment is a collection of related applications grouped based on access type or user privileges. For better organization, similar application segments should be assigned to a Segment Group. For example, if multiple application segments serve the “Sales” department, creating a Segment Group named “Sales Applications” ensures all related applications are managed together under a common policy.

Deploying App Connectors for Application Segments

When configuring application segmentation, the first step is deploying App Connectors and grouping them appropriately. In this setup, an App Connector named “London” is associated with the Welshgeek.net domain controller and located in London. Ensuring proper geo-IP configuration allows users to connect to the closest App Connector based on their location. Additionally, in this case, IPv4 DNS Resolution Only is disabled to support both IPv4 and IPv6 hosts within the network.

Connector Group




Name	Status	Version Profile	Next Periodic Software Update	Actions
▼ London ✕	✓	New Release	May 23 between 1:00 - 5:00 (BST)	🔍 ✎ ✕
<div><div>Description: London</div><div>IPv4 DNS Resolution Only: Disabled</div><div>App Connectors: <div>WG - DC-1643816167146</div></div><div>App Connector Provisioning Keys: WG - DC  (2 of 100 used)</div><div>Location: London, UK</div><div>Location Coordinates: 51.5072178, -0.1275862</div><div>Persist Local Version Profile: ✓ Enabled</div></div>				

Mapping App Connectors to Server Groups

A server group named “DC Discovery” is configured with a single App Connector group. With **Dynamic Server Discovery** enabled, the App Connector dynamically resolves DNS entries,

automatically creating virtual servers for each resolved hostname. This functionality operates similarly to a load balancer, and enabling **Dynamic Server Discovery** is considered best practice in most deployments.







Server Group

Name	Status	Dynamic Server Discovery	App Connector Groups	Actions
1. DC Discovery	✓	✓	London	  
<div>Description</div> <div>DC Discovery</div> <div>Servers</div>				

Defining Application & Server Group Mapping

Wildcard application segments are often used to simplify access control. For instance, a wildcard representing the internal domain *.Welshgeek.net ensures that all Active Directory servers fall under the same segment. The policy includes all TCP and UDP ports from **1-52** and **54-65535**, deliberately omitting **Port 53** to preserve DNS resolution. The application segment is assigned to the **Segment Group “DC Apps”**, allowing a unified policy to be applied across multiple applications. The **Server Group “DC Discovery”** dictates which App Connector groups the access policy should query.




Access Policy

▼ Wildcard	 *.welshgeek.net	✓	On Access	    
<div>Description</div> <div><div>Segment Group</div><div>DC Apps</div></div> <div><div>Server Groups</div><div>1. DC Discovery</div></div> <div><div>Double Encryption</div><div>✗ Disabled</div></div> <div><div>Bypass</div><div>Use Client Forwarding Policy</div></div> <div><div>Client Connector can receive CNAME</div><div>✓ Enabled</div></div> <div><div>Source IP Anchor</div><div>✗ Disabled</div></div> <div><div>ICMP Access</div><div>✗ Disabled</div></div>				

Access Policy for Application Segments

Access policies define user permissions for application segments. Initially, broad access is granted to ensure all necessary applications are available before gradually refining security controls. For example, a wildcard policy *.Welshgeek.net ensures all users can access internal applications before implementing more granular restrictions.

Access Policy

Rule Order	Name	Rule Action	Actions
> 1	Allow Wildcard	✓ Allow Access	  

Application Discovery

This approach supports **real-time application discovery** by monitoring access patterns and dynamically identifying applications. Best practices recommend first enabling broad access to internal applications, then refining policies over time using discovered applications. Admins can select discovered applications directly from the console, define new segments, and apply policies accordingly.

Zscaler also incorporates **machine learning-driven recommendations**, leveraging usage data to suggest refined policies. This structured approach enables organizations to progressively implement **granular user-to-application segmentation**, prioritizing **critical applications**, **high-risk users**, and **insights from application owners**. With application discovery and wildcard segmentation in place, organizations can continually refine access policies to enhance security without disrupting operations.

Review: Key Takeaways on Private Application Access and Segmentation

Private Application Access with Zero Trust

- Zscaler's **Private Application Access (ZPA)** secures connections to private applications for users, regardless of location or device.
- The **Zero Trust** model ensures that users only access authorized applications without being placed on the corporate network.

Streamlined and Secure Remote Access

- **ZPA eliminates the need for traditional VPNs**, significantly reducing the risk of lateral movement and attack exposure.
- Users connect to specific applications **through the Zero Trust Exchange**, rather than gaining broad network access.

Configuring Private Application Access

Private Application Access is configured using three key pillars:

1. **Reachability** – Deploying App Connectors and ensuring proper discovery.
2. **Application Details** – Defining application segments and segment groups.
3. **Access Policies** – Enforcing security controls to regulate access.

Eliminating Network-Based Risks with Segmentation

- **Application Segmentation prevents lateral threat movement** by restricting access only to necessary applications.
- Users are never brought onto the network, **reducing exposure and preventing unauthorized discovery of internal resources**.
- Access is enforced based on **identity, device posture, and business policies**.

Application Segmentation Implementation

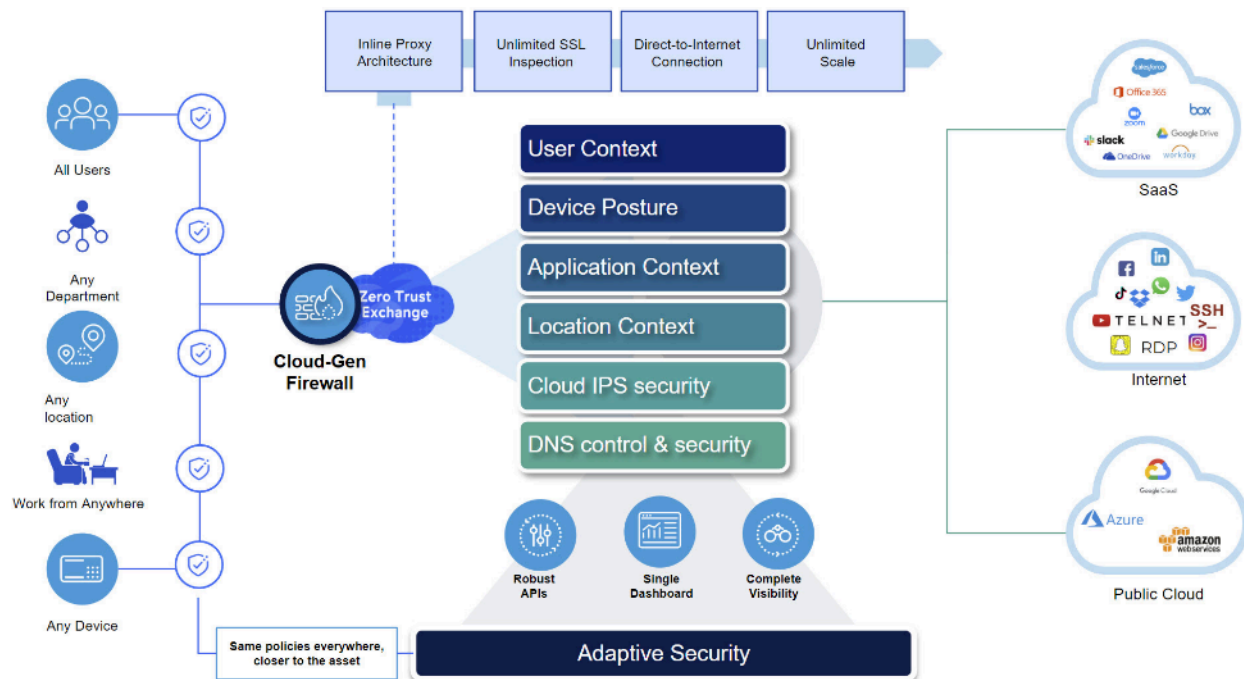
- **User-to-application segmentation** limits access to only essential applications based on roles, risk levels, and business needs.
- **Machine learning-driven application discovery** enhances segmentation by identifying access patterns and suggesting new policies.
- Organizations can **progressively refine security policies**, starting with broad access and narrowing permissions as applications and user needs are better understood.

By leveraging **Zscaler's Zero Trust Exchange**, organizations can **enhance security, simplify remote access, and implement dynamic segmentation strategies** that prevent network-based threats while maintaining seamless user access to critical resources.

Firewall

Zscaler Cloud Firewall

The **Zscaler Cloud Firewall** is a **Next-Generation Firewall (NGFW)** that provides comprehensive security and granular control over all ports, protocols, applications, and services—regardless of user location or device type. Unlike traditional hardware-based firewalls, Zscaler's cloud-delivered model offers **unlimited scalability** without the constraints of legacy infrastructure.



Key Features of Zscaler Cloud Firewall

Zscaler Cloud Firewall includes advanced security capabilities that ensure **defense in depth**, such as:

- **Full Protection for Work-From-Anywhere Users** – Security policies follow users no matter where they connect.
- **Cloud-Delivered Local Internet Breakouts** – Optimized direct-to-cloud connectivity for faster, more efficient traffic routing.
- **Always-On Intrusion Prevention System (IPS)** – Continuous protection against threats through deep packet inspection (DPI).
- **DNS Control & Security** – Prevents DNS-based threats and allows granular control over domain resolution.
- **Complete Visibility Through a Single Pane of Glass** – Centralized monitoring and policy enforcement across all locations.

Granular Firewall Policy Controls

Once a **location** is enabled with **Next-Gen Firewall** capabilities, administrators can configure detailed policies through the **Firewall Filtering Control** section. This includes:

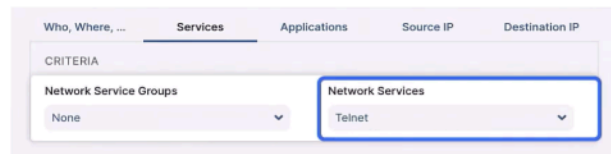
- **Network Services Policies:** Control traffic based on **port and protocol combinations**.
- **Predefined & Custom Network Services:** Hundreds of **predefined network services** (e.g., TCP 443 for HTTPS, UDP 53 for DNS) are available, with the option to create **custom services**.
- **Network Application Policies:** Supports **over 1,300 network applications** and **8,000+ cloud and SaaS applications** identified via **deep packet inspection (DPI)**.

Granular Policy Control

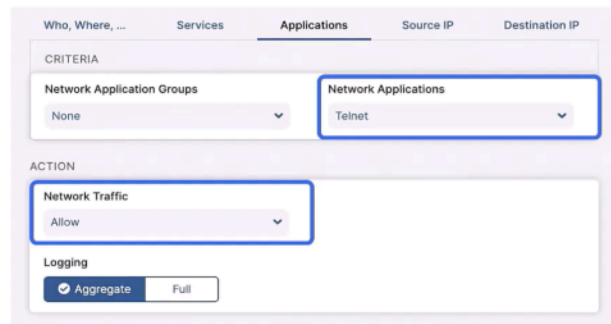
	Rule Order ▾	Admin Rank	Rule Name	Criteria	Action
HTTP/HTTPS traffic only on guest Wi-Fi	1	7	DNS-rule	NETWORK SERVICES DNS	Allow
	2	7	Guest Wi-Fi	NETWORK SERVICES HTTP; HTTPS TIME Work-time	Allow
Allow FTP for IT users only	3	7	File Transfers	NETWORK APPLICATIONS FTP; FTP-Data; FTPS; TFTP USERS IT	Allow
Block all P2P apps except Skype for Bus.	4	7	Office 365	DEPARTMENTS Engineering; Engineering QA; Executive; Finance; Human Resou... NETWORK APPLICATION GROUPS MSOffice365	Allow
	5	7	P2P Except Skype	NETWORK APPLICATION GROUPS Peer-to-Peer Apps	Block/Reset
Allow access to dynamic IPs based upon FQDN	6	7	Finance AWS Test Server	DEPARTMENTS Finance	Allow

Firewall Control Policy

- Network Service: {Port+Protocol}
 - Predefined – HTTP : TCP+80, HTTPS: TCP+443, DNS: UDP/TCP+53
- Network Application : { Layer 7 metadata+Port+Protocol+IP}
 - DPI signature: Irrespective of port and IP
- Network service & network application criteria in the same rule results in a logical “AND” condition
 - Telnet network service on Port 23
 - Telnet network application on any port
 - “AND” results in telnet protocol as detected by DPI must be on port 23
- Criteria within the same network service or network app is logical “OR”



This screenshot shows the 'Services' tab in a firewall configuration interface. The 'CRITERIA' section has two dropdown menus. The first, 'Network Service Groups', is set to 'None'. The second, 'Network Services', is set to 'Telnet' and is highlighted with a blue box.



This screenshot shows the 'Applications' tab in a firewall configuration interface. The 'CRITERIA' section has two dropdown menus. The first, 'Network Application Groups', is set to 'None'. The second, 'Network Applications', is set to 'Telnet' and is highlighted with a blue box. Below the criteria, the 'ACTION' section has a dropdown menu set to 'Network Traffic' with 'Allow' selected, also highlighted with a blue box. At the bottom, the 'Logging' section has two buttons: 'Aggregate' (selected) and 'Full'.

FQDN-Based Firewall Rules & DNS Resolution

Unlike legacy firewalls that rely heavily on **IP-based filtering**, Zscaler fully supports **Fully Qualified Domain Names (FQDNs)** for better policy enforcement. Zscaler operates **DNS servers across 150+ global data centers**, allowing administrators to define policies for specific FQDNs **without relying on on-premises DNS resolution**. This ensures seamless enforcement of **internet-bound traffic policies** at scale.

Network Services vs. Network Applications

- **Network Services:** Defined by **port and protocol** (e.g., TCP 443 for HTTPS, UDP 53 for DNS).
- **Network Applications:** Identified at **Layer 7** using **DPI metadata**, independent of the port/protocol.

When configuring policies, it's important to remember that **Network Services and Network Applications** are evaluated using a **logical AND** condition. This ensures accurate policy enforcement, preventing conflicts where **standard port-based rules** could contradict **deep packet inspection findings**.

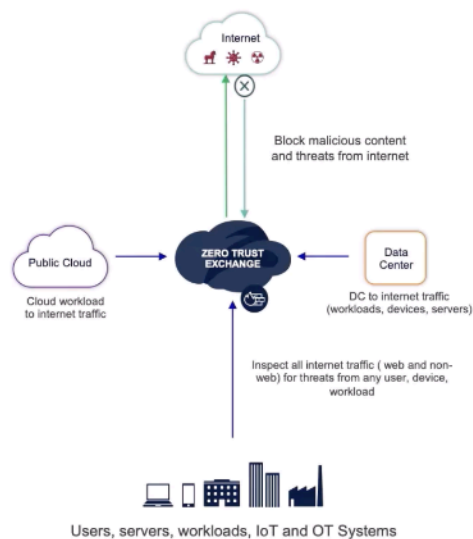
Key Concepts:

What options do customers have for configuring network services in Zscaler's firewall?	How does Zscaler handle domain name resolutions in firewall policy?	How do network service and application relate in Zscaler's policies?
Customers can select from hundreds of predefined network services or define custom services by specifying port and protocol combinations , ensuring precise traffic control and security enforcement.	Zscaler leverages DNS servers across its 150+ global data centers to resolve fully qualified domain names (FQDNs) , enabling direct policy enforcement without requiring local DNS redirection.	In Zscaler's policies, network service and application are linked by a logical AND , meaning both must match the defined criteria for the policy action to be enforced, ensuring granular and precise access control .

Cloud Firewall Use-Cases

Zscaler's **Cloud Firewall** enables enterprises to achieve **consistent, adaptive, and scalable security** regardless of user location, supporting the evolving needs of hybrid work environments.

Cloud Firewall Use-Cases



Adaptive Work-from-Anywhere policies for all traffic

- Dynamically inspects traffic for all users, apps, devices, and locations – both remote and on site/branch
- Anomaly detection and dynamic risk computation for user, device and location



Secure Local breakout of M365 and SaaS Applications

- Direct shortest path to M365 / Teams, optimized DNS resolution minimizing backhaul latency with easy 'one-click configuration'
- Bandwidth Control to Prioritize Teams, M365



Optimized DNS Resolution, Security & Control

- Protects users from reaching malicious domains as the first line of defense
- Optimizes DNS resolution to deliver better user experience and cloud app performance
- Provides granular controls to detect and prevent DNS tunneling



Context-aware Cloud IPS

- Delivers always-on IPS threat protection and coverage, regardless of connection type or location
- Inspects all user , IOT/OT traffic on and off the network, even SSL



Protect ALL traffic

- Dynamically identify web and non-web traffic, evasive apps on non-standard ports

Here are some of the **most critical use cases**:

1. Seamless Security for Hybrid Workforces

With remote and hybrid work now standard, ensuring **consistent next-generation firewall (NGFW) capabilities** across all locations is essential. Unlike traditional on-premises firewalls, which enforce different policies for remote and on-site users, Zscaler delivers **uniform security postures**, ensuring seamless protection and policy enforcement everywhere.

2. Modernizing Network Architecture: Moving from Hub-and-Spoke to Direct-to-Internet

Many enterprises are shifting from **legacy hub-and-spoke architectures** to **direct-to-internet models** to enhance **performance and security** for critical SaaS applications such as **Microsoft 365, Salesforce, and other cloud services**. Zscaler's **cloud-delivered firewall** provides **complete visibility, access control, and threat prevention**, ensuring safer and more efficient connectivity for SaaS applications.

3. Securing DNS as the First Line of Defense

Since **DNS is a common attack vector**, securing it is crucial for **blocking threats at the initial stage**. Zscaler's **Cloud Firewall integrates DNS security**, preventing threats such as phishing, malware, and command-and-control (C2) attacks at the DNS resolution level—acting as a **first layer of defense** for enterprises.

4. **Scalable Intrusion Prevention & Detection (IPS)**

Zscaler's **always-on cloud IPS** provides **real-time threat protection** across all locations and connection types without degrading performance. Unlike traditional firewall appliances that struggle under heavy IPS signature loads, Zscaler's **Zero Trust Exchange scales elastically**, ensuring **consistent and effective IPS coverage** regardless of traffic volume, port, or protocol.

5. **Advanced Application Identification & Evasive App Control**

Zscaler dynamically identifies **both web and non-web traffic** to apply precise access controls, including **detecting and blocking evasive applications** like **BitTorrent**, which often disguise themselves by using standard ports. This **deep traffic analysis** ensures **stronger security posture** while allowing legitimate applications to function seamlessly.

By addressing these **key use cases**, Zscaler's **Cloud Firewall delivers enterprise-grade security with unmatched scalability, visibility, and flexibility**, replacing legacy firewalls and securing organizations in today's cloud-first world.

When implementing **Zscaler's Cloud-Gen Firewall**, organizations should follow best practices to ensure **strong security, seamless application access, and efficient policy management**.

1. Default Block vs. Default Allow

There are two approaches to handling default rules: **Default Block** or **Default Allow**. **Zscaler's recommended best practice is to start with a Default Block Drop rule**, which aligns with cybersecurity best practices. This ensures that **all traffic is blocked by default**, and organizations can then **explicitly allow only the necessary applications and services**.

- By default, new Zscaler tenants are set to **block all traffic** as a security measure.
- It is strongly recommended to maintain this **default block-first approach** and gradually allow only the required traffic.
- For organizations needing a **Default Allow** rule for specific use cases, Zscaler provides an option to modify the default rule.

2. Preserving Essential Predefined Rules

Certain **predefined firewall rules** are dynamically applied when specific capabilities, such as **Microsoft 365 One Click**, are enabled. These rules ensure that **critical business applications function properly**.

- **Best practice:** Keep these predefined rules **unchanged**, as they automatically allow essential traffic while maintaining security controls.

3. Allowing Zscaler Proxy Traffic

Zscaler uses **proxy-based security** for deep inspection and threat prevention. To ensure proper **traffic forwarding and filtering**, organizations must **allow Zscaler proxy traffic**:

- This predefined rule includes the **IP addresses of Zscaler data centers** and necessary **proxy services**.
- **Best practice:** Keep this rule **enabled** to ensure seamless traffic processing and policy enforcement.

4. Enabling Auto Proxy Forwarding

For **web-based protocols like HTTP, HTTPS, and FTP**, Zscaler automatically forwards traffic to the proxy module for **header content analysis and security inspection**.

- **Best practice:** Enable **Auto Proxy Forwarding** to dynamically detect and inspect non-standard port traffic.

- Example: If FTP traffic is detected on an **unexpected port**, **Zscaler automatically identifies it** through **Deep Packet Inspection (DPI)** and forwards it to the proxy, **enhancing security visibility and enforcement**.

5. Granular Access Control for Critical Services

Organizations should apply **granular firewall rules** for protocols like **SSH, Telnet, FTPS**, and others based on **business needs**.

- **Best practice:** Configure access based on:
- **User identity and roles**
- **Wildcard or fully qualified domain names (FQDNs)**
- **Specific destinations, locations, or sublocations**
- **Least-privilege principles**, ensuring that only required users and devices can access certain applications.

By following these **top firewall best practices**, organizations can **enhance security, optimize network performance, and prevent unauthorized access** while maintaining flexibility for business needs.

Key Benefits of Zscaler Cloud Firewall

- **Comprehensive Threat Protection:** Utilizes **Intrusion Prevention System (IPS) signatures** for real-time threat mitigation.
- **Optimized DNS Security:** Enhances **DNS resolution** and security to **prevent DNS-based threats**.
- **Secure Internet & SaaS Breakouts:** Facilitates **secure local breakouts** for **internet and cloud applications**.
- **Reduced Operational Costs:** Eliminates the need for **on-premises firewalls**, reducing **hardware and maintenance costs**.
- **Unified Security for Work-from-Anywhere Users:** **Centralized policy management** ensures that users are **protected across all locations**.

By **leveraging these best practices**, organizations can maximize the **effectiveness, scalability, and security** of **Zscaler's Cloud-Gen Firewall**, ensuring **consistent protection across all environments**.

Key Concepts:

What is the recommended default rule for a new tenant in a cloud-gen firewall configuration?	How should rules for applications like Microsoft 365 be handled?	What is auto proxy forwarding and its benefit in firewall settings?
The recommended best practice is to start with a Default Block rule , ensuring that all traffic is initially denied . Organizations should then gradually define Allow rules for only the necessary applications and services. This approach aligns with cybersecurity best practices , minimizing risk by restricting unauthorized access from the start .	Leverage predefined rules that dynamically identify and allow application traffic, such as Microsoft 365 One Click . These rules automatically adapt to Microsoft's changing endpoints, ensuring seamless connectivity while eliminating the need for manual configuration and preventing productivity disruptions.	Auto proxy forwarding automatically redirects web and FTP traffic to a proxy module for enhanced evaluation . This feature strengthens security by leveraging deep packet inspection (DPI) to detect and properly handle applications operating on non-standard ports , ensuring comprehensive traffic analysis and policy enforcement.

Review:

Zscaler Cloud Firewall

Zscaler Cloud Firewall is a **Next-Generation Firewall (NGFW)** that provides **full control** over **ports, protocols, and applications** across all users, regardless of location or device. It offers **unlimited scalability** without the constraints of legacy hardware.

Granular Firewall Policies & Deep Packet Inspection

With **deep packet inspection (DPI)** capabilities, Zscaler's Cloud Firewall enables **granular policy configuration**, identifying and managing **over 1,300 network applications** and **8,000–12,000 cloud and SaaS applications** while enforcing precise control over network services and protocols.

Key Use Cases

- **Consistent security for hybrid and remote workforces**
- **Direct-to-internet architecture support** for SaaS applications like M365 and Salesforce
- **Scalable Intrusion Prevention System (IPS)** that provides **always-on** threat protection, **reducing risk at the DNS level** and mitigating threats regardless of traffic volume

Best Practices

- **Default Block-Drop Approach** – Start with a **default block rule**, then create Allow rules based on business needs
- **Predefined Rules for SaaS Apps** – Utilize **Microsoft 365 One Click** and other preconfigured rules to **dynamically identify and allow** application traffic
- **Auto Proxy Forwarding** – Automatically redirects **FTP/HTTP traffic** to proxy modules for **enhanced evaluation and security**
- **Granular Access Control** – Configure specific policies for **SSH, TELNET, and other critical protocols**, leveraging **DPI** for advanced threat detection

Zscaler Cloud Firewall Benefits

- **Unified policy management** for hybrid and remote workforces
- **Reduced operational costs** through **Firewall-as-a-Service (FWaaS)**
- **Secured local breakouts** for **SaaS applications**
- **Optimized DNS resolution & security** with integrated **DNS protection**
- **Robust IPS threat protection** to safeguard against evolving cyber threats

Cyberthreat Protection Services

What is Cybersecurity?

Cybersecurity Overview

Cybersecurity is the practice of **safeguarding systems, networks, and programs** from digital threats that seek to **access, alter, or steal sensitive data**.

It is designed to **prevent unauthorized access, exploitation, and destruction** of devices, applications, and critical information.

A robust cybersecurity strategy incorporates **multiple layers of defense** to protect against cybercrime, including cyberattacks aimed at **compromising, modifying, or erasing data**.



By the end of this chapter, you will get a clear overview of:

1. Describe cybersecurity and its challenges
2. Explain the cybersecurity, types of attack surfaces and cybersecurity and the different stages involved in a cyber attack framework
3. Discuss the types of cyberattacks and malware, and how Zscaler holistically stops them to
4. List the malicious file protection capabilities that Zscaler offers through the malware protection configuration
5. Identify Zscaler's Advanced Threat Protection capabilities and the options to utilize to configure the capability
6. Describe and explain Cloud Sandbox, IPS, Deception, ITDR, Private AppProtection, and Browser Isolation

The Need for Cybersecurity

In today's digital era, **cybersecurity is essential** as businesses, individuals, and governments increasingly rely on digital technologies. Protecting sensitive data, critical systems, and online activities from cyber threats has become a **top priority** due to the following reasons:



- **Protection Against Cyber Threats:** Cybersecurity safeguards individuals and organizations from threats such as hacking, malware, phishing, and other cyberattacks that can result in financial losses, data breaches, and reputational damage.
- **Preventing Unauthorized Access:** Strong security measures help prevent attackers from gaining access to confidential systems and sensitive data.
- **Reducing the Risk of Exploitation:** Cybersecurity helps mitigate risks associated with digital exploitation, ensuring data integrity and business continuity.

Understanding the Attack Surface

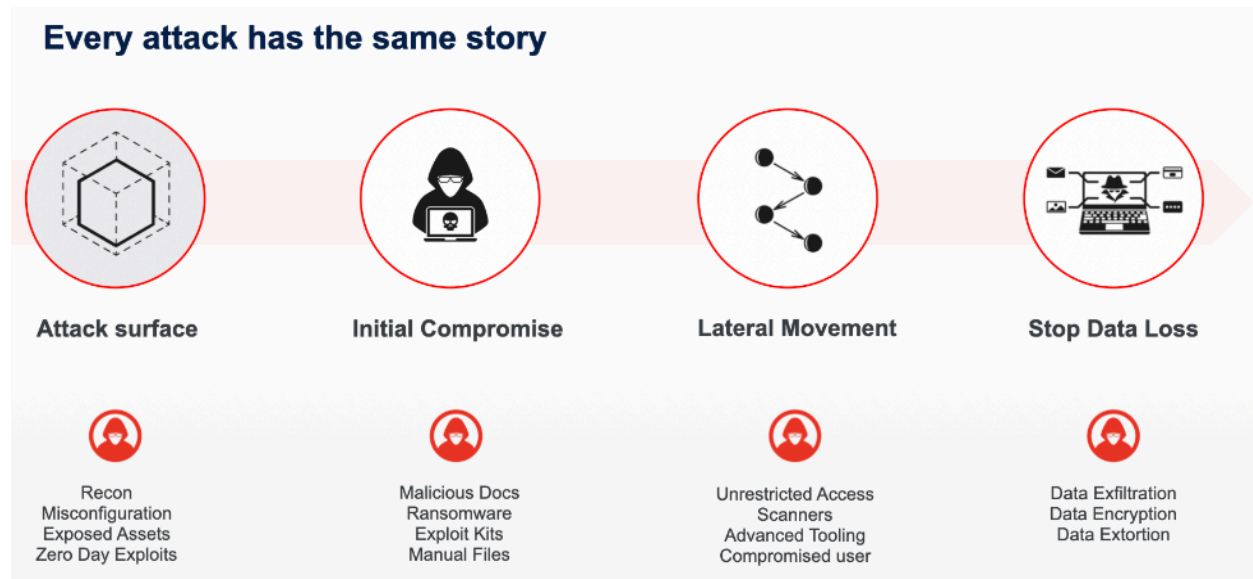
The **attack surface** refers to **all entry points that attackers can exploit** to gain unauthorized access to an organization's network and computer systems.

- **Minimizing the Attack Surface:** A fundamental security measure is to keep the attack surface **as small as possible** to reduce vulnerabilities.
- **Complexity in Modern Businesses:** With the rise of **devices, web applications, and network nodes**, managing the attack surface has become increasingly complex, creating multiple cybersecurity risks.



Stages of a Cyberattack Framework

A cyberattack typically follows four **high-level stages**:



1. **Attack Surface Identification** - Attackers look for exposed endpoints such as public-facing servers, VPN users, or vulnerable applications.
2. **Initial Compromise** - Attackers use tactics like **phishing emails, malicious downloads, or compromised websites** to gain initial access to a system.
3. **Lateral Movement** - Once inside, attackers attempt to **navigate through the network**, escalating privileges and searching for **critical data and assets**. If **network segmentation** is weak, attackers can easily move across applications and environments.
4. **Data Theft & Exfiltration** - Attackers steal **sensitive data** for **financial gain, extortion, or blackmail**. **Ransomware attacks** may use **double extortion**, where data is **encrypted before being exfiltrated**, pressuring victims into paying ransoms.

This framework applies to **all types of cyberattacks**, from **ransomware to advanced supply chain attacks**, making it crucial for organizations to implement **robust cybersecurity defenses**.

Types of Cyberattacks

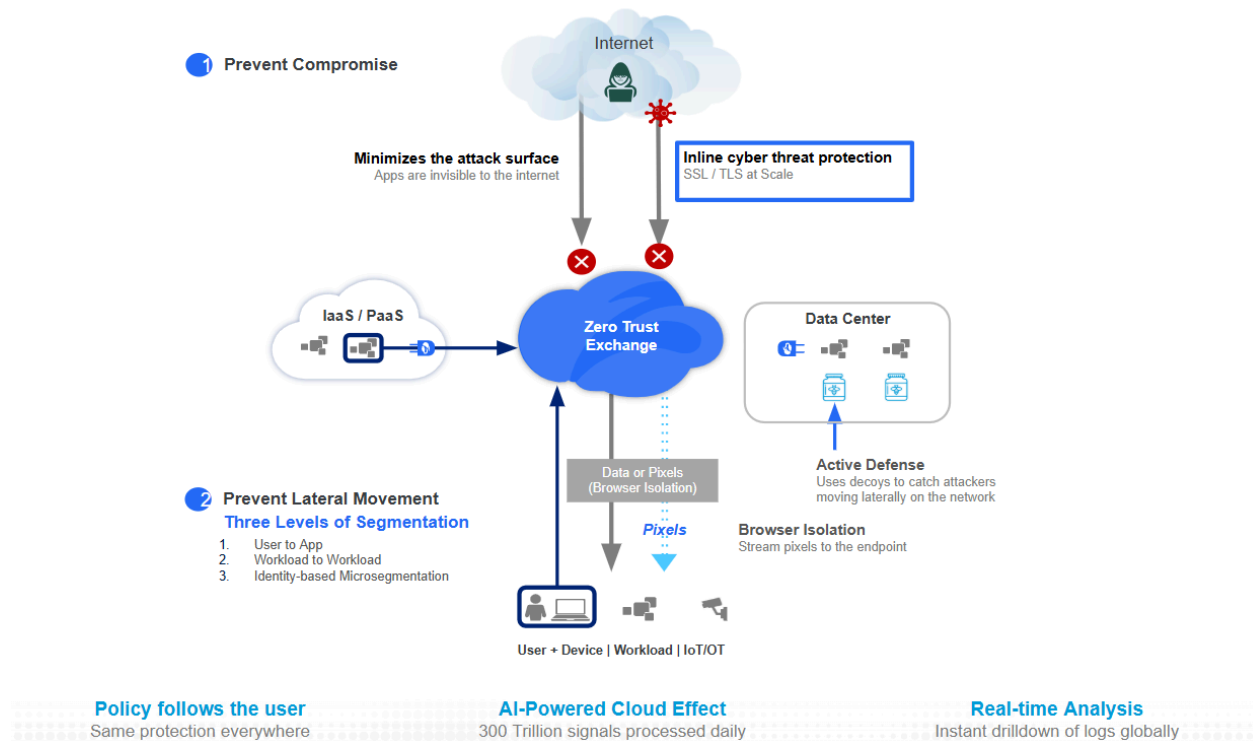
Cyberattacks come in various forms, each designed to exploit vulnerabilities and compromise systems. Below are some of the most prevalent cyber threats:

- **Malware** – Malicious software designed to damage, disable, or gain unauthorized access to computers and connected network devices. Common types include viruses, worms, Trojans, ransomware, and spyware.
- **Phishing** – An attack where cybercriminals impersonate legitimate entities (such as banks, government agencies, or trusted companies) to deceive users into revealing sensitive information, such as login credentials or financial details.
- **Distributed Denial-of-Service (DDoS)** – A malicious attempt to overwhelm a system, network, or website with excessive traffic, rendering it unable to respond to legitimate users and causing service disruptions.
- **Man-in-the-Middle (MITM) Attack** – A tactic where an attacker intercepts and potentially alters communication between two parties who believe they are directly interacting with each other. This can compromise sensitive data, such as login credentials or financial transactions.
- **SQL Injection** – A cyberattack targeting data-driven applications, where an attacker inserts malicious SQL code into a database query, allowing unauthorized access, modification, or deletion of sensitive data.
- **Insider Threat** – A security risk originating from within an organization. This can be intentional (e.g., employees stealing sensitive information for financial gain or revenge) or unintentional (e.g., employees unknowingly exposing systems to vulnerabilities).
- **Cryptojacking** – A cyberattack where hackers hijack a victim's computer resources to mine cryptocurrency without their consent. This unauthorized activity can significantly slow down system performance and consume computing power.

Understanding these cyber threats is crucial in implementing strong security measures to protect networks, data, and users from potential breaches.

Holistic Approach to Stopping a Cyberattack

The **Zero Trust Exchange** offers a fundamentally different approach to cyberthreat protection by significantly reducing the attack surface. Instead of granting broad network access, users, devices, and workloads connect directly to the specific resources they need, with **inline security controls** operating at the speed of the cloud. This architecture **eliminates the attack surface, prevents lateral movement, and enhances user experience** by enforcing Zero Trust principles.



Zscaler employs a **holistic and layered** approach to cybersecurity, focusing on:

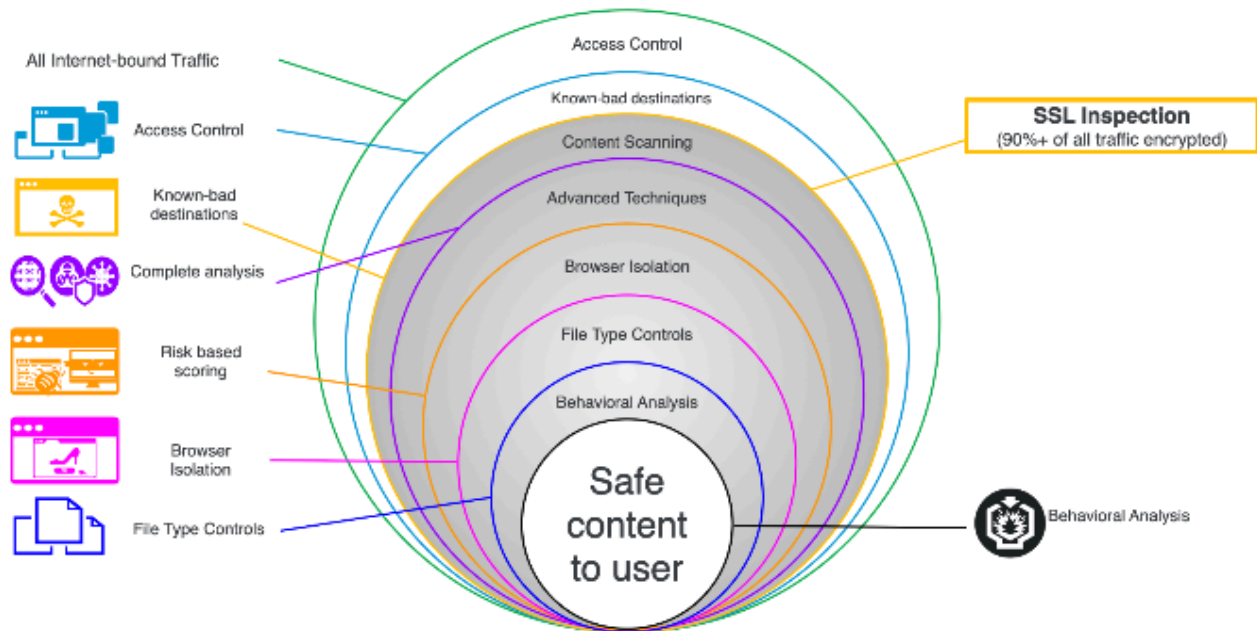
- Preventing compromise
- Reducing the attack surface
- Stopping lateral movement

Each of these elements plays a crucial role in delivering **comprehensive threat and malware prevention**.

A Layered Approach to Threat Protection

The Zero Trust Exchange works by enforcing multiple security layers, ensuring cyber threats are neutralized before they can cause harm.

Layered approach to threat and malware protection



1. Controlling Internet-Bound Traffic

- The first step is applying **access control policies** for all outbound traffic.
- **URL Filtering** is implemented to block known malicious destinations based on threat intelligence.
- Filtering is applied to **domains, IP addresses, URLs, and file hashes** identified as threats.

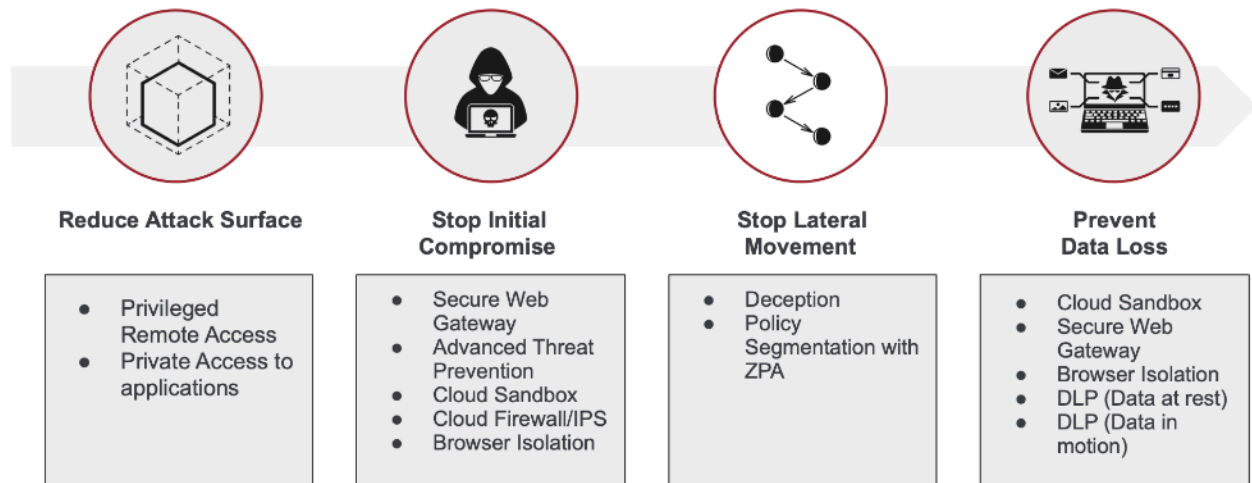
2. Deep Content and Traffic Inspection

- Full **SSL inspection** ensures encrypted traffic is scanned for hidden threats.
- **PageRisk** dynamically evaluates website risk in real time based on various risk factors.
- **Browser Isolation** protects users from visiting suspicious websites that may host **watering hole attacks** (compromised legitimate sites injecting malicious JavaScript).
- **File Type Control** prevents unauthorized file downloads and execution.
- **Cloud Sandbox with AI/ML-based behavioral analysis** detects and blocks zero-day malware before it reaches users.
- Ultimately, only **safe, verified content** is delivered to the user.

Mapping to the Cyberattack Framework

Zscaler's Zero Trust Exchange aligns with the **four-stage cyberattack model**, ensuring end-to-end protection:

Zero Trust Exchange prevents cyber attacks



1. Reducing the Attack Surface

- **ZPA (Zscaler Private Access)** ensures applications remain invisible to the internet, eliminating exposed attack surfaces.
- Users receive **privileged access** only to necessary applications, preventing unauthorized discovery.

2. Stopping Initial Compromise

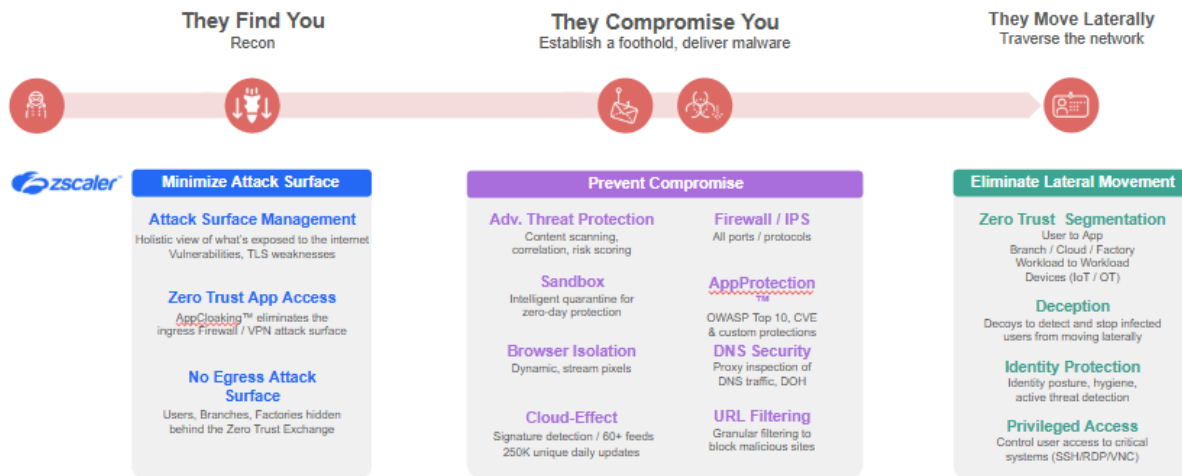
- **ZIA (Zscaler Internet Access)** provides **Secure Web Gateway (SWG)** protection, **Advanced Threat Protection (ATP)**, **Cloud Sandbox**, **Cloud Firewall, IPS**, and **Browser Isolation** to detect and neutralize threats.

3. Preventing Lateral Movement

- **Deception technology** lures attackers into false environments, reducing the risk of network infiltration.
- **Policy-based segmentation** ensures compromised devices cannot spread malware or access critical assets.

4. Preventing Data Loss

- **DLP (Data Loss Prevention)** policies protect sensitive data from leaks and exfiltration.
- **Browser Isolation and Cloud Sandbox** further safeguard against data theft and unauthorized file transfers.



By integrating these **preventive, detection, and response** strategies into a **unified Zero Trust security framework**, Zscaler provides **proactive, scalable, and intelligent** cybersecurity, ensuring enterprises can operate securely in an increasingly complex threat landscape.

Zscaler Delivers Comprehensive Cyber Threat Protection

Zscaler's cybersecurity capabilities are categorized into three key areas:

- **Minimizing the Attack Surface** – Reducing exposure by ensuring users and applications are never directly exposed to the internet.
- **Preventing Compromise** – Blocking threats before they reach users or devices through advanced security layers.
- **Stopping Threat Movement** – Preventing lateral movement and containing breaches with segmentation and deception techniques.

What Sets Zscaler Apart in Cyber Threat Protection?

Zscaler stands out by securing **all four stages of a cyberattack** with industry-leading capabilities:

- **Comprehensive Cloud Platform** – A fully integrated **Zero Trust Exchange** that provides security at scale.
- **Unmatched Inline Threat Protection** – Advanced AI/ML-driven defense mechanisms that operate in real-time.
- **Enterprise-Wide Risk Quantification** – The only vendor offering complete **risk assessment and prediction** using enterprise data.

- **Actionable Insights & Remediation** – Real-time analytics, managed threat hunting, and proactive breach prevention.

With over **40% of Fortune 500 companies** relying on Zscaler, our platform ensures **end-to-end cyber threat protection**, enabling businesses to operate securely in an evolving digital landscape.

Review: Key Takeaways from This Section

Understanding Cybersecurity

Cybersecurity is the practice of safeguarding systems, networks, and applications from digital threats aimed at unauthorized access, modification, or theft of sensitive data.

Stages of a Cyberattack Framework

Cyberattacks typically follow four high-level stages:

1. **Attack Surface** – Identifying vulnerable entry points.
2. **Initial Compromise** – Gaining unauthorized access through tactics like phishing or malware.
3. **Lateral Movement** – Expanding control within the network.
4. **Data Theft & Exfiltration** – Stealing and extracting sensitive information.

Common Types of Cyberattacks

Some of the most prevalent cyber threats include:

- **Malware** – Malicious software designed to harm or exploit systems.
- **Phishing** – Deceptive attempts to steal user credentials or sensitive data.
- **DDoS Attacks** – Overwhelming a system with excessive traffic.
- **Man-in-the-Middle Attacks (MITM)** – Intercepting and altering communications.
- **SQL Injection** – Exploiting database vulnerabilities.
- **Insider Threats** – Risks posed by employees or internal users.
- **Cryptojacking** – Unauthorized use of computing resources for cryptocurrency mining.

Effective Approach to Stopping Cyberattacks

A successful cybersecurity strategy includes:

- **An Adaptive Platform** – Continuously evolving defenses against emerging threats.
- **Automated & Integrated Protection** – Real-time threat detection and response.

- **Layered Defense** – Multiple security layers to prevent, detect, and contain threats.

How Zscaler Zero Trust Exchange Stops Cyberattacks

Zscaler's **Zero Trust Exchange** platform ensures end-to-end protection by:

- **Reducing the Attack Surface** – Eliminating direct exposure to the internet.
- **Preventing Compromise** – Blocking threats before they reach users or systems.
- **Stopping Lateral Movement** – Restricting unauthorized access and segmentation to contain breaches.

By leveraging a **zero trust architecture** and **AI-driven security**, Zscaler provides a **comprehensive, scalable, and proactive defense** against modern cyber threats.

Zscaler's Cyber Security Services Suite

Malware Protection

What is Malware Protection?

Malware Protection is a critical security feature within Zscaler that safeguards organizations and users from malicious files and cyber threats. As part of Zscaler's **Cyber Protection** capabilities within the **Security Services** suite, it works alongside **Advanced Threat Protection** and **Antivirus** to provide comprehensive defense against malware-based attacks.

Types of Malware

To fully understand **Zscaler's Cyber Protection** capabilities, it's essential to identify the most common types of malware targeting enterprises.

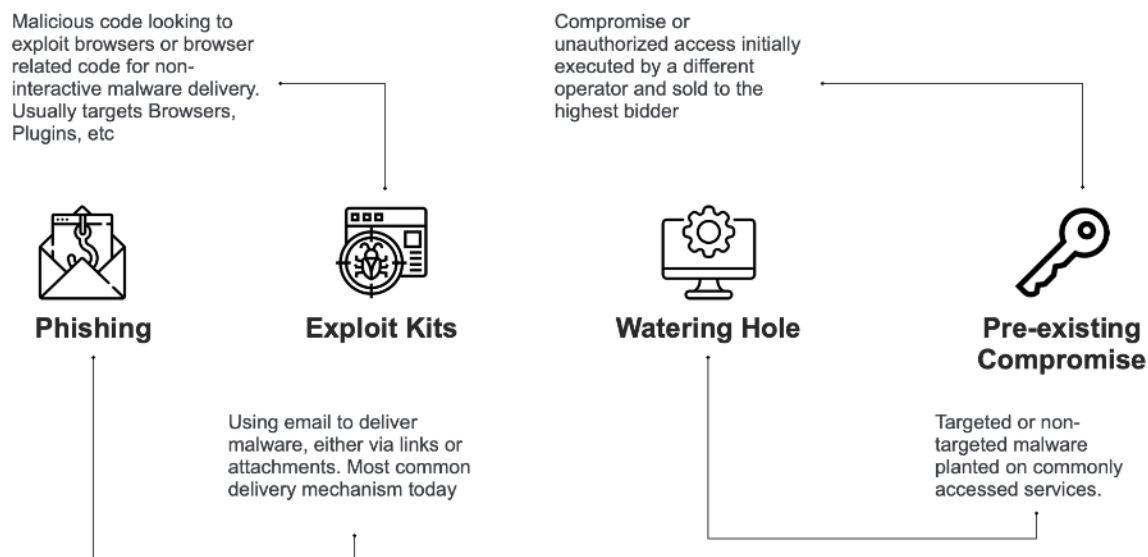


- **Malicious Document (Maldoc):** Used to deliver harmful code or software through documents such as **Microsoft Office files** or **PDFs**, aiming to compromise systems or networks.
- **Downloader Malware:** Specifically designed to **deliver additional malware** onto infected systems. Notable families include **Emotet, SmokeLoader, and Pony**.
- **Ransomware:** Encrypts files and steals data, often demanding ransom payments. Common ransomware families include **Ryuk, REvil, Maze, and EKANS**.
- **Information Stealer:** Focused on extracting sensitive data from target systems. Notable examples include **Trickbot, Qakbot, Agent Tesla, and Ursnif**.
- **Post-Exploitation Tools:** Deployed **after an attacker gains access**, used for further exploitation and persistence. Examples include **Mimikatz, Meterpreter, and Empire**.
- **Remote Access Trojan (RAT):** Provides attackers with **full remote access** to compromised systems. Common RAT families include **Nanocore, njRAT, and Remcos**.

Malware Delivery Mechanisms

Understanding how malware is delivered is crucial in preventing cyber threats. Below are some of the most common delivery mechanisms used by attackers:

Common Delivery Mechanisms



1. Phishing

Phishing remains the most widely used method for delivering malware. A targeted form of phishing, called **spear phishing**, specifically involves sending malicious attachments or links via email. When a user clicks the link or opens the attachment, malware is downloaded unknowingly, leading to system compromise.

2. Exploit Kits

Exploit kits contain **malicious code designed to exploit vulnerabilities in web browsers**. These were highly effective when **Internet Explorer** was commonly used, but with the rise of **Google Chrome** and other modern browsers, exploit kits have declined. However, advanced exploit kits targeting modern browsers and plugins are still active.

3. Watering Hole Attacks

In a watering hole attack, hackers **inject malicious content into a popular and frequently visited website**. This can include malicious JavaScript, drive-by downloads, or infected advertisements. Users visiting the compromised site unknowingly download

malware. A well-known example was **Forbes.com**, which fell victim to a watering hole attack through **malicious ad injections**.

4. Pre-Existing Compromise

In this method, **attackers gain initial unauthorized access to a system but do not exploit it themselves**. Instead, they sell access to the highest bidder on dark web marketplaces. This approach allows different cybercriminal groups to use the compromised system for various attacks, such as ransomware deployment or espionage.

Zscaler Malware Protection & Configuration

To combat these threats, **Zscaler's malware protection** provides multiple layers of defense, including the ability to **block spyware, adware, viruses, trojans, worms, and unwanted applications**. It also detects and blocks **password-protected files, malicious active content, and unscannable files** that may contain malicious payloads.

Most of these protections rely on **antivirus signatures, file-based detection, and AI/ML-powered analysis**. Traditional **MD5 hash-based identification** helps detect known malware, while **AI-driven behavioral analysis** identifies **zero-day and unknown threats** before they can execute.

Advanced Threat Protection

What is Advanced Threat Protection (ATP)?

Zscaler **Advanced Threat Protection (ATP)** is a comprehensive security solution designed to protect sensitive data from **sophisticated cyber threats**, including **malware, phishing campaigns, and unauthorized access**. It integrates multiple security layers such as **cloud security, email security, and endpoint security** to enhance an organization's defense against evolving cyber threats.

How ATP Enhances Security

The **Advanced Threat Protection policy** safeguards network traffic by detecting and blocking fraud, malicious scripts, and unauthorized communication attempts. This ensures that enterprises remain protected against **zero-day threats, advanced persistent threats (APTs), and other high-risk attacks**.

Handling ATP Security Exceptions

In some cases, legitimate **partner or vendor websites** may be unintentionally blocked by **antivirus, anti-spyware, or anti-malware policies**. To address this, Zscaler **ATP allows users to create security exceptions**, exempting trusted websites from inspection. This ensures seamless access to **essential downloads, webmail services, or partner portals** while maintaining overall security.

Understanding Command and Control (C2) Channels

Command and Control (C2) channels are a critical component of **cyberattacks**, enabling adversaries to maintain control over compromised systems. These channels facilitate **communication between a compromised device and an attacker's infrastructure**, allowing them to execute commands, exfiltrate data, and deploy additional payloads.

How Command and Control Works in a Phishing Attack

To illustrate how C2 channels operate, let's consider a **phishing attack** scenario:

1. A user is **tricked into clicking a malicious link** or downloading an infected file.
2. The attacker **delivers one or more payloads** onto the user's machine.
3. A **secondary-stage payload** may be downloaded to strengthen the compromise.
4. Once the endpoint is compromised, **an outbound C2 connection** is established to the attacker's infrastructure.
5. The adversary gains **remote control over the victim's machine**, enabling further actions.
6. Attackers may assess the system and **deploy additional malware or commands** to escalate their attack.

Why Attackers Use Command and Control Channels

C2 channels allow attackers to:

- **Maintain persistence** on compromised devices.
- **Execute remote commands** to control the victim's system.
- **Deploy secondary malware payloads** for further exploitation.
- **Exfiltrate sensitive data** without immediate detection.

Common Tools Used for C2 Attacks

One widely used **open-source tool** for command and control operations is **Cobalt Strike**. Originally designed for **penetration testing**, Cobalt Strike has been widely abused by cybercriminals to create **customized C2 traffic**, making it a preferred tool for adversaries.

Understanding **how C2 channels function** is essential for **detecting and preventing cyber threats**, ensuring organizations can defend against **sophisticated, multi-stage attacks**.

Zscaler Advanced Threat Protection (ATP)

Zscaler Advanced Threat Protection (ATP) is a critical component of **Zscaler Internet Access (ZIA)** within the **Secure Web Gateway portfolio**, providing **comprehensive defense against cyber threats** such as **phishing, malware, and advanced persistent threats**.

Core Capabilities of Zscaler ATP

Zscaler ATP leverages multiple security layers to **reduce the attack surface** and prevent **compromise**:

1. **URL Categorization** – Classifies websites to block access to high-risk domains, including newly registered and observed domains.
2. **File Type Controls** – Restricts high-risk file types, preventing the download of **malicious executables** from **untrusted sources**.
3. **Reputation-Based Blocking** – Uses threat intelligence from **ISACs, industry peers, and security exchanges** to block **known malicious domains and IP addresses**.
4. **Signature-Based Protection** – Uses **Zscaler ThreatLabz** research to apply **client-side and server-side signatures** for threat detection.
5. **AI/ML-Based Detection** – Identifies **patient-zero attacks** using **advanced behavioral analysis** and **machine learning models**.

Threat Mitigation Techniques

Zscaler ATP provides **granular security controls** to protect organizations from sophisticated threats:

- **Blocking High-Risk URL Categories** – Prevents access to **malicious domains**.
- **Country-Based Blocking** – Restricts access from **regions where the organization does not operate**, reducing risk.
- **Blocking Password-Protected & Unscannable Files** – Prevents **stealthy malware payloads** from bypassing security inspections.
- **Filtering Non-RFC Compliant Traffic** – Blocks **suspicious web traffic** that does not adhere to **standard web protocols**.

Newly Registered & Observed Domains

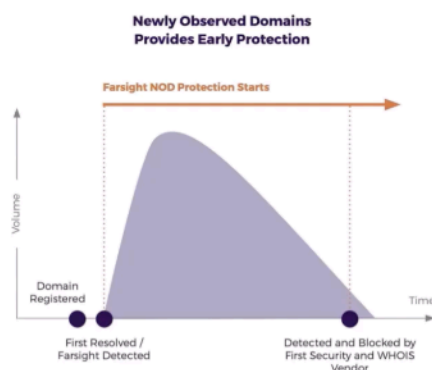
Cybercriminals frequently register domains **shortly before launching attacks**. Zscaler ATP provides two key categories for identifying these threats:

- **Newly Registered Domains (NRD)** – Domains registered within **the last 24 hours**, often used for **phishing and malware distribution**.
- **Newly Observed Domains (NOD)** – Captures domains that appear **suddenly in DNS traffic**, even if they were **not recently registered**.

Zscaler leverages **Farsight**, the world's most advanced **DNS sensor network**, to identify domains as soon as they show DNS activity. Within **three minutes** of a domain coming online, a Farsight sensor detects the DNS request and adds it to the **newly registered and observed domains** category. Organizations can then choose to **block these domains entirely** or apply **Cloud Browser Isolation** to mitigate potential threats. Initially, these domains are categorized as **miscellaneous**, as they lack an assigned category. However, after **30 days**, they are reassessed and categorized appropriately based on their activity and characteristics.

Newly Registered & Observed Domains

- Sources
 - WhoisXMLApi for Newly registered domains
 - Farsight Feed for Newly Observed Domains
- Domains are categorized after 30 days
- Customers can block or isolate these categories



CRITERIA

URL Categories

--- ^

Unselected Items	Selected Items (1)
Search...	Newly Registered and Observed Domains
<input type="checkbox"/> Militancy/Hate and Extremism	
<input type="checkbox"/> Miscellaneous	
<input type="checkbox"/> Miscellaneous or Unknown	
<input checked="" type="checkbox"/> Newly Registered and Observed Domains	
<input type="checkbox"/> Non Categorizable	
<input type="checkbox"/> Other Miscellaneous	
<input type="checkbox"/> News and Media	

AND

AND

AND

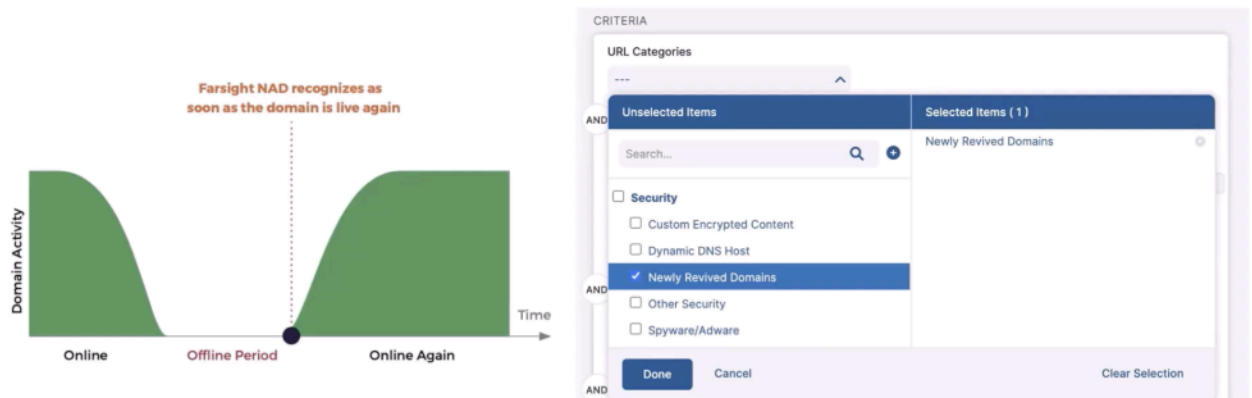
Done Cancel Clear Selection

Newly Revived Domains

Attackers sometimes **recycle** previously legitimate domains, repurposing them for malicious activity.

Newly Revived Domains

- Sources
 - Farsight Feed for Newly Revived Domains
- These are domains that went offline and came back online
- Prevents attacks that repurpose old domains with good reputation



- **Zscaler ATP detects domains that were inactive for more than 10 days and suddenly become active again.**
- **Instead of outright blocking them, security teams can apply Cloud Sandbox and Browser Isolation for additional scrutiny.**

Botnet Protection and AI-Powered Command & Control (C2) Detection

Botnet protection is a critical component of cybersecurity, as botnets serve as the backbone for **command and control (C2) operations**, enabling attackers to **deploy malware, steal sensitive data, and launch cyberattacks** by remotely controlling compromised devices. Disrupting these C2 channels is essential to preventing cyber threats from escalating.

With **Zscaler's Advanced Threat Protection**, organizations can effectively **block both C2 servers and C2 traffic**, cutting off adversaries' ability to communicate with infected systems. By enabling **command and control server blocking**, Zscaler automatically **denies connections to known malicious servers**, halting active threats before they cause damage. Zscaler continuously **updates its database of known C2 infrastructures** through **real-time intelligence sharing** across the cybersecurity ecosystem. Additionally, **ThreatLabz**, Zscaler's in-house research team, actively

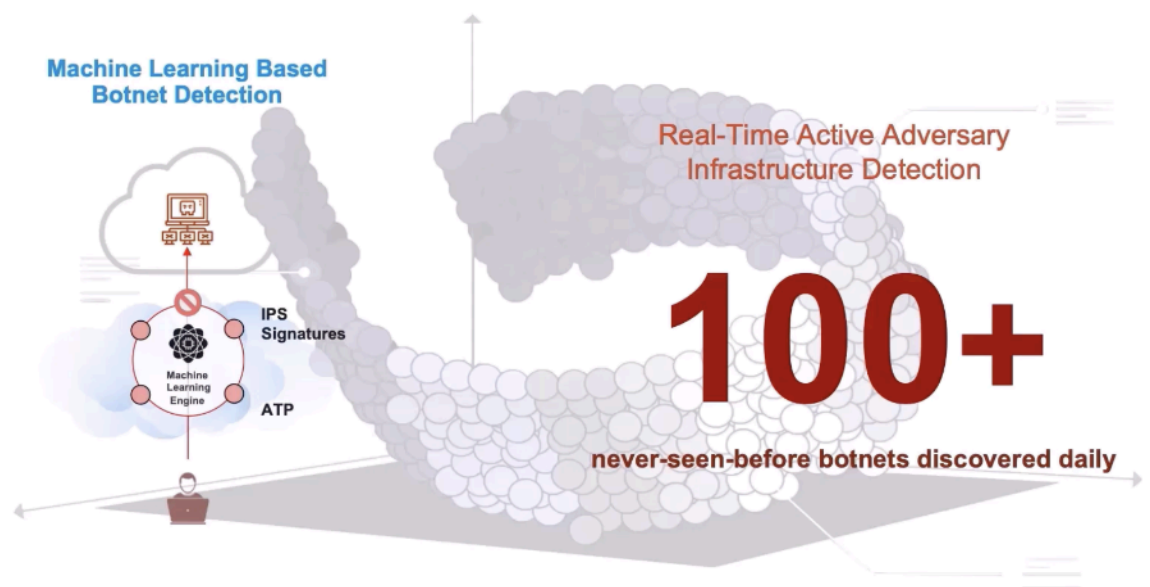
analyzes malware behavior using **Cloud Sandbox technology**, monitoring how malicious files attempt to establish C2 communication.

Leveraging **AI-powered C2 detection**, Zscaler's **machine learning (ML) models** inspect **network traffic in real-time**, detecting suspicious patterns that indicate **active C2 activity**. This capability enables Zscaler to **map adversary infrastructure, uncover hidden botnets, and block both known and unknown C2 channels**. Since **every modern cyberattack relies on command and control**, this proactive approach is essential in preventing cyber threats.

On average, Zscaler **detects and neutralizes over 100 new botnets daily**. More importantly, **AI-driven threat intelligence** enables Zscaler to **identify and stop emerging C2 infrastructures**, making it one of the most **effective defenses against evolving cyber threats**. Through **Zscaler's cloud effect**, threat intelligence gathered from one customer benefits the entire Zscaler ecosystem—even customers without **Advanced Cloud Sandbox** receive **instant updates**, ensuring newly identified **C2 servers** are blocked immediately.

By **disrupting command and control channels**, Zscaler effectively **stops cyberattacks before they escalate**, preventing **data breaches, ransomware deployment, and lateral movement within networks**. This **AI-powered, cloud-native approach** ensures that organizations stay ahead of cyber threats with a **scalable, intelligent, and proactive defense system**.

Extending Defense In Depth: AI-Powered C2 Detection



A key feature within **Zscaler's Advanced Threat Protection (ATP)** is **dynamic page risk analysis**, which assesses the security risk of web content in real time. This capability is accessible through a **configurable slider** on the ATP settings page, allowing organizations to set their acceptable risk tolerance.

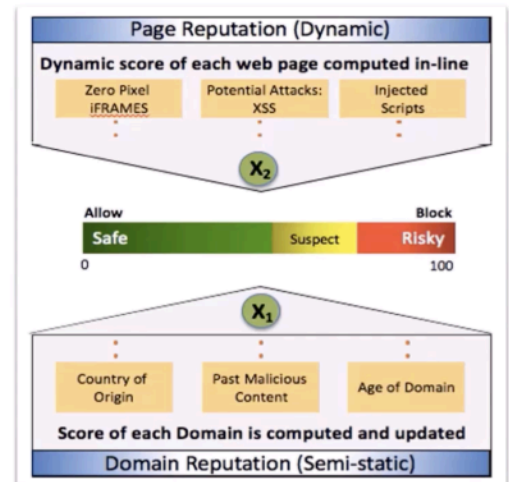
Zscaler inspects all webpage content **in-line** using a **multi-data algorithm** that evaluates several risk factors, including:

- **Top-Level Domain (TLD):** Does the domain belong to a known high-risk category?
- **User Agent Analysis:** Is the user agent unknown or suspicious?
- **Missing HTTP Headers:** Are critical security headers absent?
- **Domain Entropy:** Is the domain name randomly generated, indicating potential malicious intent?
- **iFrame Behavior:** Does the page contain **zero-pixel iFrames**, commonly used for hidden tracking or malicious scripts?
- **JavaScript Obfuscation:** Is the page running encoded or obfuscated JavaScript, a common technique for concealing malware?
- **Suspicious URL Structure:** Does the URL path, JavaScript, or CSS code display anomalies suggesting malicious activity?

By applying these criteria, **Zscaler assigns a risk score** to web content, classifying it as **safe, suspicious, or risky**. The **slider-based control** enables organizations to adjust their security posture, determining how aggressively they want to filter potentially harmful websites. This **scalable and automated approach** enhances protection against phishing sites, drive-by downloads, and other web-based threats, ensuring **real-time threat mitigation** without compromising user experience.

PageRisk engine Detection via web page and domain features

- Suspicious Content Protection (aka PageRisk)
 - Multi data algorithm applied to web page (not file)
 - The algorithm determines the riskiness
 - Blocked based on customer set threshold
- Risk (0-100) is based on several factors
 - Risk TLD (.tk, .ru, etc.)
 - Unknown user agent
 - Missing HTTP headers (User-Agent, Accept, etc.)
 - High entropy domain name
 - zero-pixel IFRAME
 - Script or IFRAME before the tag or after the tag (code injection)
 - Obfuscated Javascript
 - Signatures for suspicious URL path, HTML/Javascript/CSS code



AI-Powered Phishing Detection

Zscaler's **AI-powered phishing detection** is designed to **stop even the most advanced phishing attacks** by analyzing webpage content in real-time. Using **machine learning (ML) models**, Zscaler examines multiple attributes of a webpage, including:

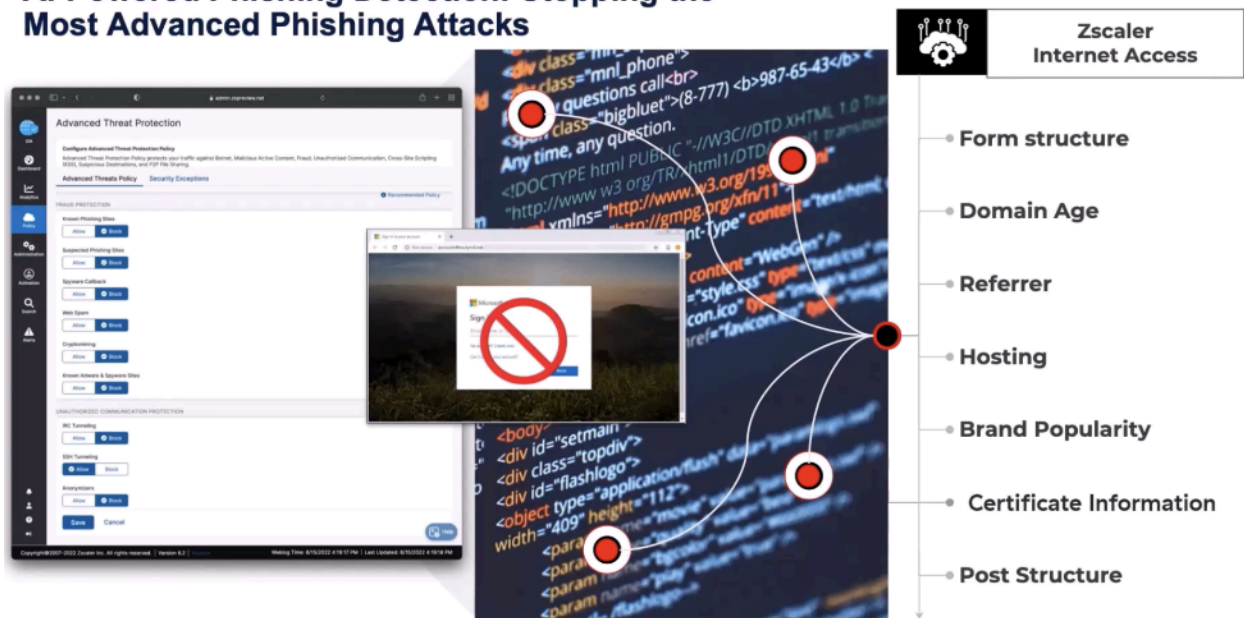
- **Form and Structure:** Detects deceptive login forms and data input fields.
- **Domain Age and Reputation:** Identifies newly registered or suspicious domains.
- **Referrer and Hosting Details:** Assesses if a site is linked from an untrusted source.
- **Brand Popularity:** Checks for spoofing of well-known brands.
- **SSL Certificate Information:** Verifies if the certificate is legitimate or self-signed.
- **Post Structure:** Examines how data is submitted from the page.

By feeding this data into an **ML model**, Zscaler determines **whether a webpage is a phishing site** and blocks it accordingly.

This AI-driven technique is highly effective against **man-in-the-middle (MITM) phishing attacks**, where adversaries create **fake front-end websites** that look identical to legitimate sites but secretly **relay user credentials to the actual website**. Since the user experiences a seamless login, they remain unaware that their credentials have been compromised. These sophisticated attacks have become increasingly common, making **real-time AI-powered detection critical for preventing credential theft**.

Activation is simple—by enabling **Advanced Threat Protection (ATP)** settings, all **AI and ML-based phishing detection capabilities** automatically operate in the background, delivering continuous, proactive protection without manual intervention.

AI-Powered Phishing Detection: Stopping the Most Advanced Phishing Attacks



Blocking Malicious Content, Exploits, and Evasive Threats

Zscaler provides robust protection against **malicious active content**, **server-side vulnerabilities**, and **evasive applications** to safeguard users and networks from cyber threats.

Malicious Active Content & Exploits:

Zscaler blocks **malicious active content** and compromised websites, including **malicious ActiveX controls**, **browser exploits**, and **file format vulnerabilities**. For example, if a user visits a website running an **exploit kit** or **malicious adware**, Zscaler's **content inspection technology** can **detect and block these threats in real-time**, preventing users from being exposed to harmful code.

Cross-Site Scripting Protection:

Cross-site scripting (XSS) vulnerabilities allow attackers to inject malicious code into legitimate websites. With Zscaler's XSS protection, organizations can **block these exploit attempts** and prevent attackers from executing unauthorized scripts that can compromise users' sensitive information or hijack sessions.

Blocking Anonymizers and Peer-to-Peer Applications:

Zscaler also provides **controls to block anonymizer and peer-to-peer (P2P) applications**, which are often used to bypass security measures. **Anonymizers** allow users to **mask their activity by routing traffic through VPNs or proxy services**, commonly seen in K-12 environments where students use services like **XVPN** to access

restricted websites. Additionally, **P2P anonymizers like Tor** enable users to hide their identity and evade security controls, increasing the attack surface for potential threats. Zscaler's **policy enforcement ensures these evasive applications are blocked**, maintaining security and compliance across the organization.

By implementing these layered security controls, Zscaler **proactively prevents cyber threats, secures web traffic, and ensures organizations can maintain visibility and control over internet usage** while protecting users from sophisticated attacks.

An Early Warning System for Enterprises

Zscaler ATP is **continuously trained on trillions of security signals**, allowing **daily updates** to block new and emerging threats:

- **250,000+ protection updates per day**
- **7 billion threats blocked daily**
- **AI/ML-powered detection of zero-day and patient-zero threats**

Key differentiator: The world's largest security cloud



By integrating **real-time threat intelligence, cloud-based security, and AI-driven detection**, **Zscaler ATP delivers a proactive, layered defense against the evolving cyber threat landscape**.

Review:

Let's summarize the key takeaways from this section.

Advanced Threat Protection (ATP): A core capability of Zscaler's **Secure Web Gateway** within **Zscaler Internet Access (ZIA)**, ATP safeguards traffic from fraud, unauthorized communications, and various malicious threats, including scripts and objects that could compromise security.

Command and Control (C2) Channels: Attackers utilize **command and control techniques** to communicate with compromised devices within a network, enabling data theft, malware deployment, and further exploitation. **Cobalt Strike**, a widely used open-source tool, is commonly leveraged by adversaries to generate and manage C2 traffic.

Zscaler Advanced Threat Protection: One of the most effective ways to stop an attack is by **disrupting the command and control channel**. Zscaler's **Advanced Threat Protection (ATP)** actively identifies and blocks these channels, preventing attackers from maintaining control over infected devices and mitigating potential damage.

Zscaler Cloud Sandbox: AI-Driven Malware Detection and Prevention

Zscaler **Cloud Sandbox**, an integral part of **Zscaler Internet Access (ZIA)** and the **Zero Trust Exchange**, is the **industry's first AI-driven malware detection, prevention, and quarantine engine** designed to identify and neutralize advanced threats before they can infiltrate an organization's network.

How Does Cloud Sandbox Work?

Zscaler Cloud Sandbox **inspects all content, with a strong focus on files, to detect and prevent ransomware, malware, and patient-zero infections**. By detonating and analyzing suspicious files in a controlled environment, it provides deep visibility into **malicious activity, adversary infrastructure, and command-and-control (C2) networks**.

Driving Threat Intelligence for SOC Teams

As files are continuously analyzed, the Cloud Sandbox generates **real-time threat intelligence** that **Security Operations Center (SOC) teams** can leverage to understand the behavior of **new and emerging threats**. By mapping out **C2 servers and attacker infrastructure**, security teams gain valuable insights into the evolving cyber threat landscape.

Cloud-Powered Protection at Scale

Through **Zscaler's cloud effect**, intelligence gathered from sandboxing activities is **instantly shared across the entire Zscaler security ecosystem**. This enables the **automatic reprogramming of other security capabilities**, such as **Advanced Threat Protection (ATP) and Malware Protection**, enhancing their effectiveness and ensuring **instant, scalable protection against sophisticated cyber threats**.

Intrusion Prevention System (IPS): Cloud-Based Threat Protection

Zscaler **Intrusion Prevention System (IPS)** is a **cloud-delivered security solution** that detects and blocks malicious network activity in real time, ensuring **continuous threat prevention across all users and locations**. Unlike traditional **Intrusion Detection Systems (IDS)**, which only monitor network traffic for unauthorized activity, an **IPS actively prevents** threats by analyzing packets—including their headers and payloads—against a database of known attack signatures.

How Zscaler IPS Works

Operating **inline with network traffic**, Zscaler IPS can **detect and block malicious activity** by resetting connections or dropping harmful packets. Integrated within the **Zero Trust Exchange (ZTE)**, it provides **always-on threat prevention** for all traffic, whether **encrypted or unencrypted**, and **follows users regardless of their location or connection type**.

Key Benefits of Zscaler Cloud IPS

Always-On Protection for All Users

Traditional IPS solutions struggle to protect remote and hybrid users effectively. **Zscaler Cloud IPS provides full threat protection anywhere users connect, ensuring continuous security across all locations and devices.**

Comprehensive Threat Defense

Zscaler IPS integrates with **firewall, sandboxing, CASB, and DLP technologies** to provide **multi-layered defense** against **botnets, zero-day threats, and advanced attacks**. It delivers **context-aware security**, analyzing the **user, application, and threat activity** for enhanced protection.

Scalable Inspection Without Hardware Limitations

Unlike traditional on-premises IPS solutions that require constant **hardware refreshes and capacity upgrades**, **Zscaler IPS scales automatically in the cloud**. This ensures organizations can **inspect all TLS/SSL traffic** without performance degradation, eliminating the risk of hidden threats in encrypted traffic.

How Zscaler Deception Works: Proactive Threat Detection & Attack Disruption

Zscaler Deception is an advanced cybersecurity capability designed to **detect, disrupt, and gather intelligence on active attacks** before they cause harm. By deploying **decoys and lures** across your environment, Deception creates **fake attack paths** that **trap adversaries**, preventing lateral movement and providing **real-time threat intelligence**.

How Deception Detects and Responds to Threats

When an attacker infiltrates the network and interacts with a decoy, **Zscaler Deception detects the activity, analyzes the attack patterns, and generates high-fidelity alerts**. Security teams can monitor these **real-time alerts on the Deception Admin Portal**, where **threat intelligence is captured, analyzed, and leveraged to deploy additional decoys**, validating the attacker's intentions while containing the threat.

Key Capabilities of Zscaler Deception

- **Pre-Breach Threat Detection**

Zscaler Deception provides **early warning signals** when adversaries—such as **organized ransomware groups or APT (Advanced Persistent Threat) actors**—are

conducting reconnaissance. **Perimeter decoys** detect stealthy **pre-breach activities** that traditional defenses might miss.

- **Prevent Lateral Movement**

Attackers who bypass **perimeter defenses** and attempt **lateral movement** within an environment are intercepted through **application decoys and endpoint lures**. These traps limit their ability to **discover valuable targets or expand their foothold**.

- **Disrupt Ransomware at Every Stage**

Decoys placed across cloud environments, endpoints, networks, and Active Directory serve as **landmines**, detecting **ransomware at every phase of the attack chain**. The presence of decoys alone discourages ransomware from spreading further.

- **Real-Time Threat Containment & Automated Response**

Zscaler Deception integrates seamlessly with **Zscaler's security platform** and third-party **SIEM, SOAR, and SOC** tools. **Automated response actions** allow security teams to **contain and mitigate threats in real-time**, preventing further damage while gathering **actionable intelligence** for proactive defense.

By **leveraging deception-based security**, organizations can **proactively detect hidden threats, stop sophisticated attacks before they escalate, and gain deeper insights into adversary tactics**—enhancing their **Zero Trust security posture** and overall threat resilience.

Identity Threat Detection and Response (ITDR)

Overview of Zscaler ITDR

Zscaler **Identity Threat Detection and Response (ITDR)** is a fully integrated solution within the Zscaler platform, designed to **identify, monitor, and mitigate identity-based risks**. It continuously scans **Active Directory (AD) infrastructure** for **compromised credentials, suspicious permissions, and vulnerabilities**, helping security teams take proactive measures against threats.

By **leveraging automated remediation and user-specific threat intelligence**, Zscaler ITDR enhances an organization's **Zero Trust security posture**, providing **real-time detection, risk mitigation, and step-by-step guidance** to safeguard identities from cyber threats.

The Growing Threat of Identity-Based Attacks

Identity-based attacks have become one of the **most pressing cybersecurity challenges**. **User credentials, identifiers, and identity systems** serve as primary entry points for attackers. Once adversaries gain access to a compromised identity, they can **escalate privileges, move laterally across systems, and access critical data**.

Key concerns related to identity threats include:

- **Problem Information** – Identifying identity-related risks
- **Problem Description** – Understanding attack vectors and vulnerabilities
- **Configuration Overview** – Reviewing misconfigurations and gaps
- **Error Messages** – Identifying system weaknesses exploited by attackers

Why ITDR is Critical for Organizations

Zscaler ITDR provides **essential identity protection** by:

- **Reducing identity-related risks** by proactively detecting compromised credentials and privilege escalations
- **Preserving a strong security posture** through continuous monitoring and real-time threat response
- **Providing security teams with actionable intelligence** to mitigate identity-based threats efficiently
- **Minimizing exposure risks** by enforcing security policies on compromised accounts
- **Protecting organizations** from unauthorized access and lateral movement attacks

Key Benefits of Zscaler ITDR

- **No Additional Agents or Virtual Machines Required**

ITDR is **built into the Zscaler Client Connector**, enabling **out-of-the-box identity protection** without requiring additional software deployments.

- **Seamless Integration with Access Policies**

The **Zscaler Zero Trust Exchange** dynamically enforces **access control policies**, blocking **compromised users** in real time when an identity-based attack is detected.

- **Credential Exposure Monitoring & Policy Enforcement**

ITDR **detects exposed credentials on endpoints**, allowing security teams to **remediate threats and enforce policies**, reducing the risk of further compromise.

- **SOC and Security Tool Integrations**

Strengthens **investigation and incident response** through integrations with **leading Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) solutions**, including: **CrowdStrike, Microsoft Defender, VMware CarbonBlack**, and other top-tier security platforms.

By **securing identity infrastructure and preventing unauthorized access**, Zscaler ITDR **reduces attack surfaces, stops identity-based attacks in real time, and reinforces Zero Trust security across the enterprise.**

Private AppProtection Overview

Zscaler **Private App Protection** provides **visibility into traffic** accessing **private applications**, regardless of user location. It protects against **evasive vulnerabilities and attacks** such as:

- **Cross-Site Scripting (XSS)**
- **Cookie Poisoning**
- **SQL Injection**
- **Remote Code Execution**

By implementing **full in-line inspection**, Zscaler ensures that only **legitimate traffic** reaches private applications while **blocking malicious activity** to prevent application-layer attacks.

Application Segmentation and Attack Surface Reduction

Zscaler **hides private applications** from unauthorized users, minimizing the attack surface. Application segmentation ensures that only authorized users can access specific apps and services.

Additionally, **inbound traffic inspection** provides another security layer, allowing only **approved traffic** to reach internal applications, **blocking threats before they can exploit vulnerabilities**.

Virtual Patching and Custom Security Controls

Zscaler **Private AppProtection** also offers **virtual patching**, allowing security teams to **mitigate vulnerabilities** while IT teams work on **fixing the CVE at its root**.

For private applications requiring **specific compliance and user behavior enforcement**, the **App Protection module** enables:

- **Custom signature creation** for security policy enforcement.
- **Custom header value enforcement in web traffic.**
- **Query string inspection and other transaction-based security measures.**

With these capabilities, Zscaler **secures private applications, reduces risk, and ensures that only authorized traffic reaches critical internal services.**

Browser Isolation Overview

Zscaler **Browser Isolation**, a key feature of the **Zero Trust Exchange**, isolates users and endpoints from **active web content**, protecting enterprises from **zero-day vulnerabilities**, **ransomware**, **unsanctioned plugins**, and **other advanced threats**.

How Browser Isolation Works

When a user accesses a potentially **malicious website**, traditional browsing exposes their device to **active threats**, such as **malicious JavaScript or ActiveX controls**. However, with **Cloud Browser Isolation enabled**, the website opens within a **containerized, isolated environment in the cloud**. Instead of allowing direct interaction, **a pixelated stream of the website is delivered to the user**, ensuring that **no active content executes on their local device**, effectively **neutralizing any potential attack**.

Cybersecurity Use Case: File Protection

Attackers frequently **embed malicious macros** in files like **Google Docs or Word (Docx)**, which can **compromise a system upon execution**. With **Browser Isolation technology**, instead of **delivering the original document**, a **PDF version is shown to the user**, eliminating active content while still allowing file viewing.

By ensuring **all websites open in a cloud-isolated environment** and sending only a **safe pixel stream** back to the user's browser, Zscaler **creates an air gap between users and potential threats**, significantly reducing the risk of malware and cyberattacks.

Detection & Response

Zscaler Detection & Response Overview

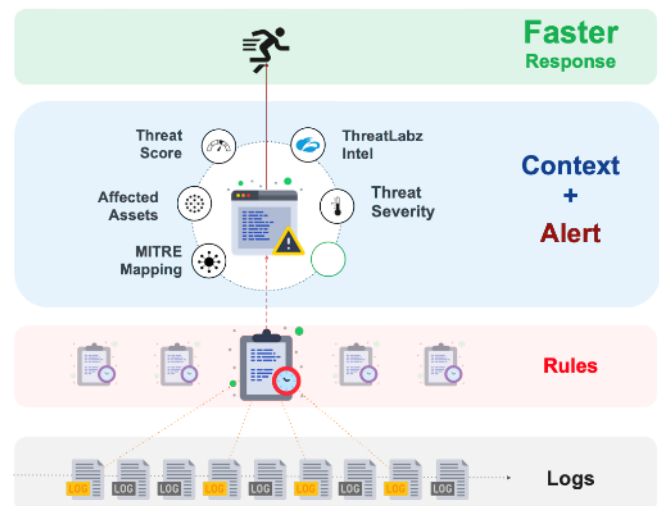
Zscaler's **Detection & Response** capability is designed to **protect endpoint devices** from **ransomware, fileless malware, and other cyber threats**. It continuously **monitors and detects** suspicious activities in **real-time**, while also providing **investigation, threat hunting, triage, and remediation** functionalities. This capability generates **high-fidelity alerts**, ensuring rapid response to potential threats.



How Zscaler Enables Detection & Response

Zscaler's **Detection & Response** is built within **Zscaler Internet Access (ZIA)** and leverages **correlated threat insights and an alerting framework**. The system **analyzes logs, correlates events**, and generates **actionable alerts** that help **security teams detect and respond to cyber threats efficiently**.

Instead of requiring security teams to manually sift through disparate logs, Zscaler's **correlation engine** automatically **links atomic log events** to identify **complex attack patterns**. For example, when a **TrickBot campaign** is detected in an organization's environment, Zscaler **provides a threat summary**, maps it to the **MITRE ATT&CK framework**, and lists **impacted systems**, enabling **quick investigation and response**. These insights can be **integrated with SIEM and SOAR platforms** for further automation and orchestration.



Detection & Response Workflow

1. Alert Generation:

- The security admin accesses the **alert dashboard** displaying **predefined security alerts** created using insights from **ThreatLabz, engineering, and product teams**.
- Alerts cover a range of threats, such as **TrickBot, Emotet, and Bitrep**, with new **correlation rules continuously added**.

2. Threat Investigation:

- Each alert includes **detailed contextual information** about the threat (e.g., TrickBot is a **banking trojan**).
- The security team can **trace the origin of the attack**, identifying **impacted users, departments, and locations**.

3. Impact Analysis:

- The system displays the **total number of affected endpoints**, along with **usernames, client IPs, department details, and timestamps** of the first detection.
- Security teams can **quickly identify and contain the threat** before it spreads further.

4. Custom Alert Rules & Notifications:

- Admins can **create custom alert rules** in addition to the **predefined security alerts** provided by Zscaler.
- Alert notifications can be **sent externally** via **email, webhooks, or integrations** with third-party platforms like **ServiceNow, Slack, Teams, OpsGenie, PagerDuty, and Splunk**.

Email Notification

⚠ Sep 25, 2022, 11:49 PM
#728101

Alert

Alert Rule Name: SOC Tier 1 - Executive Department
Indexed By: Threat Name - Win32.Backdoor.Emotet.!!

Event Type	Users Impacted - Last Interval
Botnet Callback	5

Alert Timeline
🕒 Started On: Mon Sep 7 15:14:27 2022 GMT 🕒 Ended On: Mon Sep 25 12:08:11 2022 GMT

Evaluation Status
Ended

[View Alert](#)

Webhook 3rd party support:

- ServiceNow
- Slack Teams
- OpsGenie
- PagerDuty
- Splunk

Conclusion: Zscaler's Detection & Response Capability

Zscaler's **Detection & Response** capability provides real-time **threat detection, automated correlation, and high-fidelity alerts**, enabling **Security Operations Center (SOC) teams** to quickly detect, investigate, and mitigate cyber threats. By seamlessly integrating with existing security tools, it enhances an organization's **cyber defense posture** while reducing response times to incidents.

Key Takeaways

- **Detection & Response Capability**

Zscaler's Detection & Response solution safeguards endpoint devices from **cyberthreats like ransomware and fileless malware**. By continuously **monitoring and detecting** suspicious activity in real time, it enables rapid threat investigation and mitigation.

- **How Zscaler Provides Detection & Response**

Zscaler's **correlation engine** analyzes security logs, correlates disparate events, and generates **actionable alerts** that drive **meaningful detection and response activities**. These alerts help SOC teams prioritize and respond to threats faster, ensuring **proactive cybersecurity protection**.

By leveraging **automated intelligence, real-time monitoring, and seamless integrations**, Zscaler delivers an advanced Detection & Response framework that strengthens enterprise security and minimizes cyber risk.

Data Protection Services

This chapter provides an overview of the **current data protection landscape** and explores how Zscaler's **Data Protection services** safeguard **sensitive information** through the **Zero Trust Exchange platform**. We will take a deeper look into the key components of **Zscaler's Data Protection suite** and how they work together to ensure **continuous security and compliance**.

By the end of this chapter, you will be able to

1. Identify the need for a new data protection approach
2. Explain how Zscaler provides data protection to users through the Zero Trust Exchange framework
3. Identify the data protection services Zscaler has in place to protect the data in motion and data at rest
4. Describe the Ai-driven Auto Data Discovery and Classification
5. Describe how to configure Zscaler data protection services and capabilities

Zscaler Data Protection: Ensuring Secure and Compliant Cloud Data

The Need for Data Protection in a Cloud-First World

As organizations increasingly adopt **Software as a Service (SaaS)** and **public cloud solutions**, securing enterprise data has become more challenging than ever. **Zscaler Data Protection** provides **comprehensive security solutions** to safeguard sensitive information, ensuring **compliance and protection** against modern threats.

Zscaler's approach secures **data in motion, at rest, in cloud applications, and on endpoints**, while also addressing risks from **unmanaged or BYOD devices**. Organizations today face two primary risks:

- **Data theft by malicious actors** (e.g., cybercriminals, insider threats)
- **Accidental or intentional data loss** (e.g., human error, misconfigurations)

Modern **ransomware attacks** often employ **double extortion tactics**, where attackers **steal and encrypt data**, threatening to **leak it publicly** unless a ransom is paid. As a result, **an effective cybersecurity strategy must include strong data protection measures** to minimize the impact of **breaches, leaks, and compliance violations**.

Challenges with Traditional Data Protection Approaches

Over the years, organizations have adopted various **point solutions** to prevent **data loss** across different environments:

- **Inline DLP** to prevent sensitive data from leaving the organization
- **CASB (Cloud Access Security Broker)** to monitor data shared via SaaS applications
- **Email and Endpoint DLP** to track and prevent unauthorized data movement

While these tools address specific challenges, managing **multiple DLP solutions** creates **complexity and operational inefficiencies**:

- **Multiple, inconsistent policies** lead to **gaps in enforcement** across email, cloud apps, and endpoints.
- **Redundant configurations** require security teams to manually update each DLP policy separately.
- **Disparate alerts** from CASB, email, and endpoint security tools create **visibility gaps**, making it difficult to **correlate security events** and detect insider threats.

To solve this, **Zscaler consolidates data protection into a single DLP engine**, ensuring that:

- **A single policy** consistently identifies and classifies sensitive data across all cloud and endpoint channels.
- **Alerts are unified** to provide a **clear, centralized view** of data security events.

- **Security teams can correlate insights** more effectively, reducing **manual investigations and response times**.

Key Use Cases for Zscaler Data Protection

1. Preventing Data Loss to the Internet & Cloud Applications

Zscaler acts as a **proxy**, inspecting **all outbound traffic**, including **encrypted transactions**. Using **advanced DLP classification techniques**, Zscaler enforces policies based on:

- **User groups and departments**
- **URL categories and destinations**
- **Cloud application activities**

This allows organizations to **block, monitor, coach, or notify users** about **policy violations** in real time, ensuring **comprehensive data protection** at **enterprise scale**.

Additionally, **Zscaler Email DLP** prevents data leaks via **outbound emails**, securing **sensitive communications** and ensuring **regulatory compliance**.

2. Securing Data on BYOD & Unmanaged Devices

With **remote work and BYOD adoption** increasing, **securing unmanaged devices** has become a critical challenge. Zscaler:

- **Identifies untrusted devices** during authentication
- **Applies Cloud Browser Isolation** to prevent unauthorized data access
- **Enforces conditional access policies** to ensure only authorized devices can interact with sensitive data

3. Protecting Data with Endpoint DLP

Zscaler Endpoint Data Loss Prevention (DLP) monitors and controls data movement on **user devices**, preventing sensitive data from being leaked via:

- **Printing confidential documents**
- **Saving files to removable storage (USB drives)**
- **Uploading corporate data to personal cloud storage**
- **Copying data to unauthorized network shares**

4. Securing Data Stored in Cloud Applications

Enterprises using cloud-based tools like **Microsoft 365, Google Drive, and AWS** often store vast amounts of sensitive data. **Zscaler scans, identifies, and classifies critical assets**, preventing:

- **Accidental data exposure**
- **Unauthorized sharing of sensitive information**
- **Compliance violations**

5. Preventing Data Exfiltration from Cloud Misconfigurations

Cloud misconfigurations can lead to **unintended data exposure**. **Zscaler's Security Posture Management (SSPM)** and **third-party integrations** continuously:

- **Monitor for cloud misconfigurations**
- **Identify security violations**
- **Trigger automated remediation actions** when risks are detected

Conclusion

Zscaler's **Data Protection services** provide a **unified, scalable approach** to securing enterprise data across **cloud applications, endpoints, and networks**. By eliminating **siloed DLP solutions** and implementing **centralized policies**, Zscaler ensures:

- **Consistent data security enforcement** across all environments
- **Real-time visibility into data movement and risks**
- **Simplified compliance management** for cloud-first enterprises

With **Zscaler Data Protection**, organizations can effectively **prevent data leaks, secure cloud assets, and reduce the risk of breaches**, all while ensuring seamless business operations.

AI-driven Auto Data Discovery and Classification

The **AI-driven auto data discovery** feature integrated into the **Zscaler Data Protection platform** enables automatic identification and classification of **all data**, whether **inline or at rest**. This ensures robust data classification and enhances an organization's ability to **manage and protect sensitive information effectively**.

Shadow IT and Generative AI Security

Shadow IT presents significant risks as employees use **unauthorized applications**, increasing the likelihood of **data breaches and compliance violations**. **Zscaler's Shadow IT Discovery solution** identifies over **40,000 applications**, providing:

- **Detailed risk profiles** for a better understanding of unauthorized app usage
- **Scheduled reports and dynamic policies** to regulate application risks
- **Monitoring of unauthenticated traffic** to **detect and control shadow IT activities**

For **Generative AI (Gen AI) Security**, Zscaler employs **DLP Inspection, Cloud App Control, and Browser Isolation** to **restrict data sharing and protect sensitive information**. The **Generative AI Security Report** tracks **AI tool usage and trends**, helping organizations **monitor and regulate** interactions with **generative AI platforms**. **URL Filtering** further enhances security by **controlling access to AI-related websites**.

Inline Data Discovery

Zscaler's **AI-powered insights** reveal sensitive data **leaving the company** by categorizing information such as **financial documents, legal records, and resumes**, identifying up to **8,000 files**.

- **Data Timelines** track **data movement trends** to analyze security risks over time.
- **Top Users** highlight **employees with the highest data activity**, identifying potential **insider threats**.
- **Top Data Destinations** indicate where sensitive data is moving (e.g., **Google Drive, OneDrive**), helping distinguish **authorized from unauthorized** data transfers.
- **Risk Assessments** focus on **unauthorized applications and content types**, aiding in **risk management and policy enforcement**.

Endpoint Data Discovery

Zscaler's AI scans **endpoint devices** to detect **private and sensitive data** without **disrupting functionality**. It provides **visibility into high-risk users and files** by generating a **risk summary** that includes:

- **Metrics on the number of people and files containing sensitive data**

- **Top data categories** (e.g., **PII, invoicing data**) that require protection
- **Department-specific data exposure analysis**, identifying **which teams** (e.g., **Sales, Finance**) have the highest risk

Cloud Data Discovery

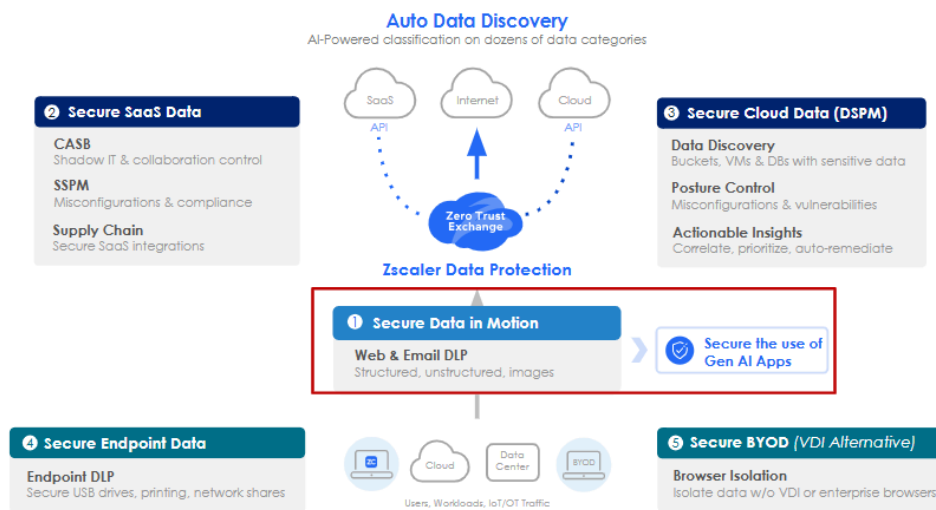
Zscaler's **Zero Trust Exchange** leverages **AI to classify cloud-stored data** according to compliance standards such as **GLBA, PCI, and HIPAA**. The system has detected **879,000 sensitive data matches within 2 million records**.

- The **Top Risk Data Stores** section identifies cloud resources with significant **exposure risks**.
- The dashboard details **data distribution by storage type**, covering areas like **storage buckets, virtual machines, and databases** across different geographical locations.
- A **Risk by Category** chart categorizes security concerns, such as **dangerous credentials, data governance violations, and public data exposure**, helping organizations manage cloud data risks more effectively.

Secure Data in Motion

Securing Data in Motion with Inline Data Protection

At Zscaler, protecting data in motion is a critical priority, ensuring that sensitive information remains secure from interception and unauthorized access as it moves across networks. By leveraging encryption, real-time threat detection, and the Zero Trust Exchange framework, Zscaler provides comprehensive security measures that safeguard sensitive data throughout its journey.



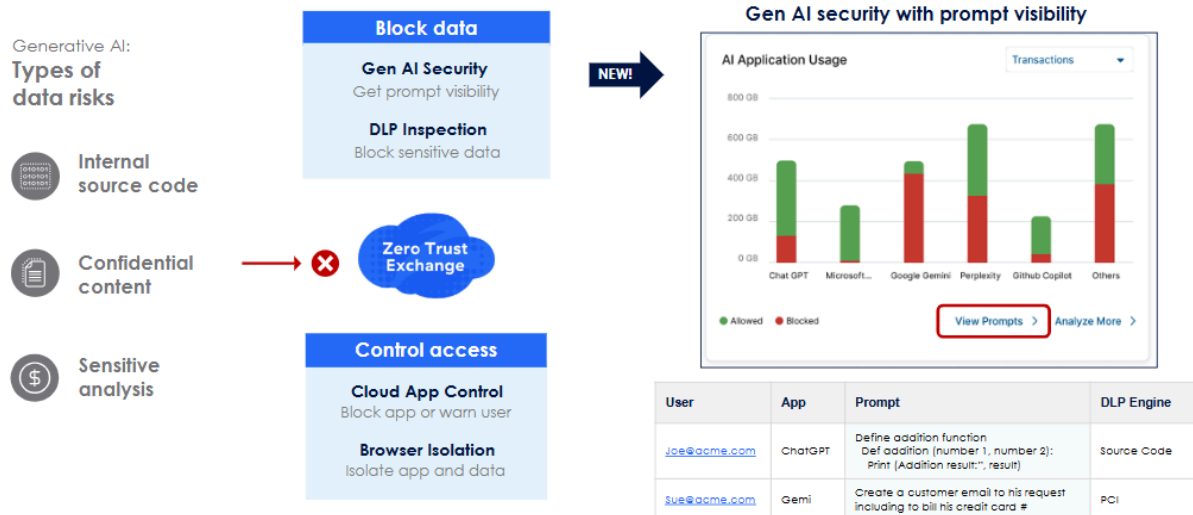
Zscaler's Data Loss Prevention (DLP) engine plays a central role in data security, using advanced techniques such as:

- **Exact Data Match (EDM):** Identifies and protects structured sensitive data, like customer records and financial details.
- **Index Document Matching (IDM):** Detects sensitive content within unstructured documents to prevent leaks.
- **Optical Character Recognition (OCR):** Scans and analyzes text within images and scanned documents to prevent unauthorized data sharing.

These capabilities integrate seamlessly with Microsoft tools and custom dictionaries, enabling organizations to enforce granular security policies across various data channels for real-time monitoring and protection.

Protecting Data from Generative AI (Gen AI) Risks

As organizations increasingly adopt AI-driven tools, securing data interactions with Generative AI (Gen AI) applications is crucial. Employees may unknowingly upload sensitive data into AI platforms like ChatGPT, increasing the risk of data leaks and compliance violations.



Zscaler provides Gen AI security with:

- A real-time dashboard to identify shadow applications and track sensitive data usage.
- User prompt monitoring with DLP triggers to control AI-related data interactions.
- Policy enforcement options, including blocking AI apps entirely, warning users before accessing AI tools, or using Browser Isolation to control copy-pasting or restrict sensitive data transfers.

By leveraging Browser Isolation, organizations can securely allow AI tool usage while ensuring corporate data remains protected from unauthorized sharing.

Zscaler's Inline Data Protection Capabilities

Zscaler offers four key Data Protection capabilities through the Zero Trust Exchange to secure data in motion:

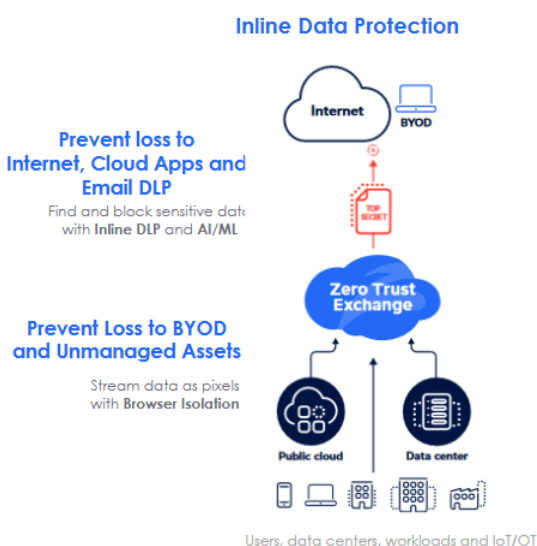
1. **Cloud Data Loss Prevention (DLP)** – Secures data moving to and from cloud applications.
2. **Endpoint DLP** – Protects sensitive data on user devices.
3. **Email DLP** – Secures outbound emails in corporate Exchange and Gmail environments.
4. **DLP for Private Apps** – Ensures secure data handling within private enterprise applications.

Zscaler's Cloud Access Security Broker (CASB) operates in inline forward proxy mode, ensuring visibility and security for real-time data traffic.

Critical Use Cases for Inline Data Protection

Inline Data Protection

Unified data protection for users, workloads, servers and IoT/OT



Top Inline Use Cases:

Shadow-IT & Data Discovery

40K Apps & 75 Risk attributes
ML powered auto classification & data discovery

Cloud App Control

Access Control – 16 Categories, 40k Apps

Tenancy Restrictions

Personal vs Corporate – Granular Policies
Tenancy Restrictions for Sanctioned apps

DLP inline for Web and SaaS

Dictionaries, EDM, IDM, OCR, AIP/MIP Labels

UEBA & Adaptive Access

Bulk upload, download, impossible travel, MFA

Data Security on BYOD

Isolation Proxy

1. **Shadow IT & Data Discovery:** Organizations must identify unsanctioned applications (Shadow IT) where employees store, share, or access corporate data. Zscaler provides automatic discovery and classification of cloud applications to detect potential risks.
2. **Contextual Data Protection:** Before enforcing content-based DLP policies, organizations should first implement contextual controls using Cloud App Control to restrict data movement based on application behavior.
3. **Tenancy Restrictions:** Ensures employees use only corporate-sanctioned versions of cloud applications, blocking access to personal accounts to prevent unauthorized data sharing.
4. **User & Entity Behavior Analytics (UEBA):** Detects anomalous data activity, flagging potential insider threats and triggering adaptive security actions.
5. **BYOD & Unmanaged Device Protection:** Enforces data access restrictions for unmanaged endpoints using Browser Isolation and conditional access policies to prevent unauthorized data exposure.

Content Inspection for Advanced Data Protection

After implementing contextual policies, Zscaler enables deep content inspection to enforce granular data protection.

Three Levels of Inspection File Type Identification

Policies for more file types, including undecodable files

Archive

Bzip2 (bz, bz2)
Cab Archive (Cab)
GZIP (gzip, gz)
ISO Archive (iso)
RAR Files (rar)
Stuffit Archive (stuffit_sit, stuffit)
Tar (tgz, gltar, tar)
ZIP (zip)

Image

Bitmap (bmp)
Gif Files
Jpeg Files
Photoshop (psd)
Png Files
Window Meta Files (wmf)

Microsoft Office

Microsoft Excel (xls,xlsx,xlsm,xlsm,xlsb,slk)
Microsoft MDB (mdb)
Microsoft Outlook Message (msg)
Microsoft PowerPoint (ppt, pptx, pptm, potx, ppax)
Microsoft RTF (rtf)
Microsoft Word (doc, docx, docm, dotx)

Other Documents

HTTP Form data
PDF Documents (pdf)

Other

Password Protected / Encrypted
Web Content
Adobe Flash (swf)
Java Applet (jar, class)
JavaScript (js)
Text File

The screenshot shows the 'Outbound Data' configuration section of a Zscaler policy. It includes a 'Cloud Applications' dropdown set to 'Any', a 'File Type' dropdown set to 'None', a 'Data Size (KB)' dropdown set to '0', and a 'Users' dropdown set to 'Any'. A 'Select File Types' button is visible next to the 'File Type' dropdown.

Applicable to any
Outbound Data

Make the Internet read only
with Outbound Data blocks

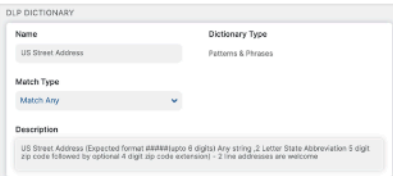
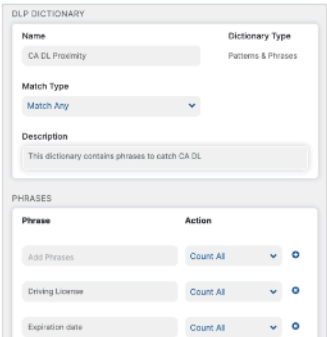
File Type-Based Data Protection

Zscaler DLP policies can block or allow specific file types from being uploaded to cloud applications. Instead of relying on file extensions (which can be modified), Zscaler performs three levels of inspection:

- **Magic Bytes Analysis:** Examines the file's first few bytes to determine its true format.
- **MIME Type Verification:** Ensures the file type aligns with its intended use.
- **File Extension Validation:** Confirms the correct extension usage.

Example: Blocking Office documents from being uploaded to applications like Pdfconverter.com while allowing them in Microsoft OneDrive.

Zscaler Content Inspection Capabilities & Custom Dictionaries

Inspection Category	Inspection Technique	
Described content	Predefined Dictionaries	<ul style="list-style-type: none"> • PII (US and International) • PCI (CC#, ABA Bank routing) • PHI (Patient Records, ICD10) • Source Code • Adult Language/Profanity • GDPR Data
	Single & multi word keywords and phrases	
	Regex	

Granular DLP policy based on users, groups, dept and location

What sets Zscaler Data Protection apart?

Extended boolean logic for building exceptions

Incident Mgmt. via SIEM, email, ticketing & on-prem incident receiver

Zscaler DLP provides hundreds of predefined dictionaries for sensitive data classification, including:

- PCI (Credit Card Numbers)
- PII (Personally Identifiable Information)
- PHI (Protected Health Information)
- Financial Data & Source Code Detection

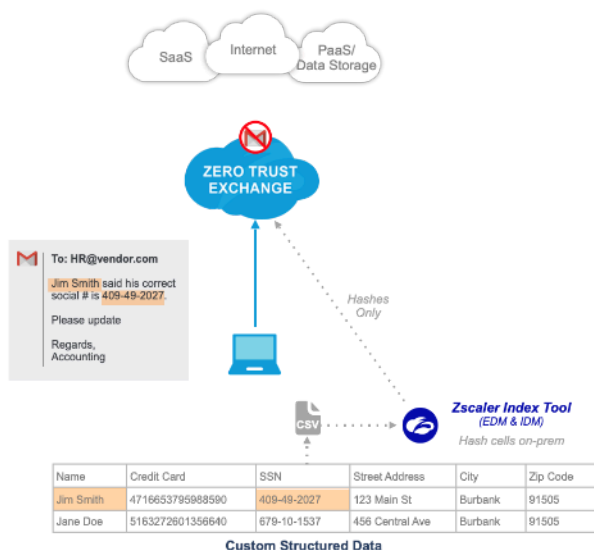
For more customization, organizations can build custom dictionaries to identify and protect proprietary data, such as documents labeled “Company Confidential.”

Boolean Logic for Advanced DLP Policies

Zscaler allows combining multiple detection methods using Boolean logic:

- Example: A DLP policy may trigger only when a document contains 50+ credit card numbers, employee first names, and a “Company Confidential” label.

Secure Custom Data with Exact Data Match



How Exact Data Match Works

- 1 Structure custom data you want to secure
- 2 Index data and send only hashes to Zscaler
- 3 Zscaler ready to find custom data
- 4 Prevent data loss with DLP block policies

Benefits of Zscaler EDM

- **Secure high value sensitive data**
PCI, PII, HIPAA, Inventory Codes, Membership #s, ect.
- **Reduce DLP False Positives**
Ex: Trigger on meaningful SSNs, not all SSNs
- **VM-based Index tool keeps things simple**
High-value data doesn't leave premises
Used for both Exact Data Match & Index Document Matching

Many large enterprises require high-precision data protection, which is why Exact Data Match (EDM) is a powerful Zscaler feature.

Instead of detecting generic credit card numbers, EDM ensures policies only trigger for an organization's exact data records (e.g., customer SSNs, corporate IDs).

How EDM Works:

1. Structured data (e.g., customer records) is indexed on-premises using a secure Zscaler EDM appliance (not uploaded to the cloud).
2. The indexing tool converts sensitive data into hashes and pushes only the hashed values to Zscaler's cloud.
3. Zscaler inspects all transactions, matching hashes against live traffic to enforce DLP policies in real time.
4. When an exact match is found, appropriate security actions (block, alert, quarantine) are triggered.

Example Use Case: Blocking the exfiltration of specific customer records (e.g., Jim Smith's credit card details) without triggering on generic numbers.

Review: Zscaler's Content Inspection Capabilities

In this section, you explored the various content inspection capabilities that Zscaler offers to protect sensitive data and enforce security policies effectively.

File Type Identification

To enforce policies based on file type, administrators use Zscaler's policy engine to specify allowed or blocked file types and sizes across applications, actions, and activities. To prevent false positives, Zscaler performs a three-layer inspection:

1. **Magic Bytes Analysis** – Examines the file's initial bytes to determine its true format.
2. **MIME Type Validation** – Verifies the file type against standard classifications.
3. **File Extension Check** – Confirms the file's extension for consistency.

Predefined Dictionaries

Zscaler provides hundreds of predefined classifiers to detect and protect sensitive data, including:

- **Payment Card Industry (PCI) Data** – Credit card numbers and financial records.
- **Personally Identifiable Information (PII)** – National IDs, Social Security numbers, tax IDs.
- **Protected Health Information (PHI)** – Medical records, ICD-10 codes, CPT codes.

These predefined dictionaries leverage standard regex and **Perl Compatible Regular Expressions (PCRE)** engines, along with **AI and ML-powered** detection to improve accuracy and reduce false positives.

Custom Dictionaries

Organizations can create custom dictionaries tailored to their specific security needs. Custom dictionaries enable identification and protection of proprietary data, such as documents labeled with "**Company-Confidential**" or "**Internal-Use Only**." These dictionaries support **custom phrases, keywords, patterns, and regular expressions** to enforce compliance and security policies.

Exact Data Match (EDM)

EDM enables precise tracking and protection of structured data by learning from existing enterprise datasets. For example, if an organization maintains a **CSV file with 200 million rows of employee PII**, the EDM engine can index this data securely and monitor cloud transactions to detect exact matches. When a match is found, Zscaler triggers **predefined security actions**, such as blocking data exfiltration, alerting administrators, or enforcing encryption policies.

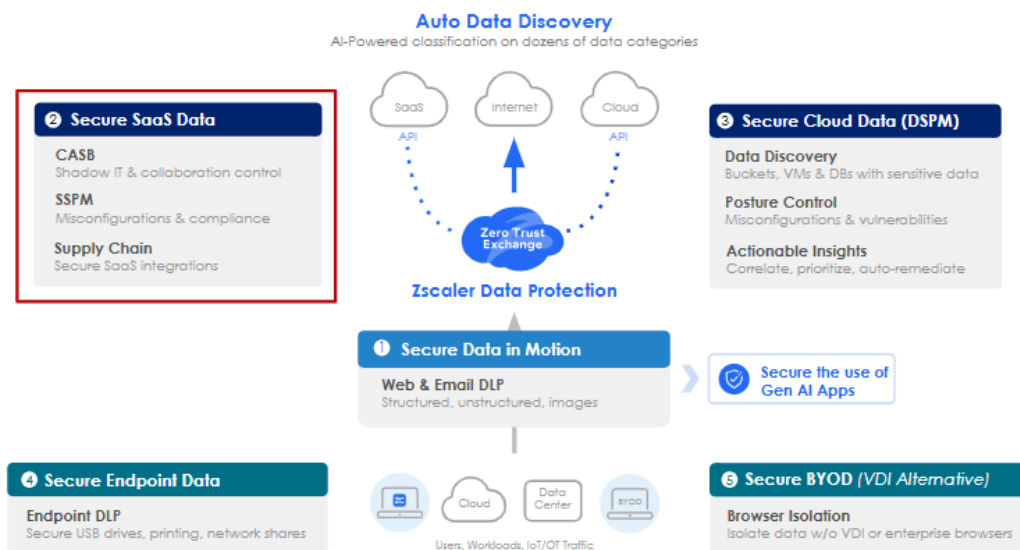
By integrating these advanced content inspection capabilities, Zscaler ensures organizations can effectively **monitor, classify, and secure** their most sensitive data across **cloud applications, endpoints, email, and private applications**.

Securing SaaS Data

As organizations increasingly rely on **Software as a Service (SaaS)** platforms, securing sensitive data across cloud applications has become more critical than ever. With the **evolving cyber threat landscape** and the rise in cloud adoption, businesses need **robust security strategies** to protect against data breaches, unauthorized access, and compliance risks.

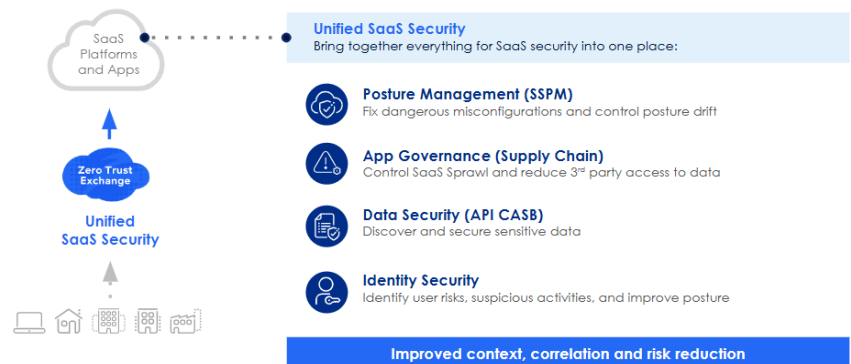
Zscaler provides **comprehensive data protection capabilities** through its **Zero Trust Exchange**, ensuring end-to-end security for SaaS applications. By leveraging **advanced visibility, access controls, and threat prevention mechanisms**, Zscaler helps organizations mitigate data loss risks effectively.

This section explores the key **SaaS security strategies and tools** that Zscaler offers, enabling organizations to **monitor, classify, and secure** their sensitive information across cloud applications.



Reduce Risks with a SaaS Security Platform

Securing **SaaS data** involves protecting sensitive information stored within cloud applications from unauthorized access, misconfigurations, and external threats. Over time, various security approaches have evolved to address these risks effectively:



- **Cloud Access Security Broker (CASB):** Initially, CASB solutions were introduced to control data sharing, ensuring that sensitive information could not be shared externally without oversight.
- **Posture Management:** This approach helps prevent **misconfigurations** in platforms like **Office 365**, reducing the risk of unauthorized data exposure.
- **Supply Chain Risk:** Third-party applications can integrate with **Office 365**, potentially gaining access to emails, contacts, and data. Without proper controls, any user can unknowingly authorize an app, creating a security gap.
- **Identity and Access Management:** With numerous users, administrators, and service accounts interacting across SaaS environments, securing identities has become a critical challenge.

To **mitigate these risks**, Zscaler provides a **comprehensive SaaS security platform** that **integrates all these security functions into a unified interface**. This **centralized view** offers enhanced context and correlation, allowing organizations to **monitor and control** misconfigurations, data sharing, third-party app access, and user behaviors more effectively.

Top Out-of-Band Use Cases

1. **Data Discovery & Data at Rest Introspection**
 - Identifies sensitive data stored in cloud applications
 - Helps enforce security policies to prevent data leaks
2. **Prevent Data Exposure**
 - Detects and restricts **public** and **external sharing** of sensitive files
3. **Secure Apps from Threats**
 - Protects against **known and unknown malware** infiltrating SaaS platforms
4. **Secure Corporate Email (Exchange & Gmail)**
 - **Inbound emails:** Blocks phishing and malware threats

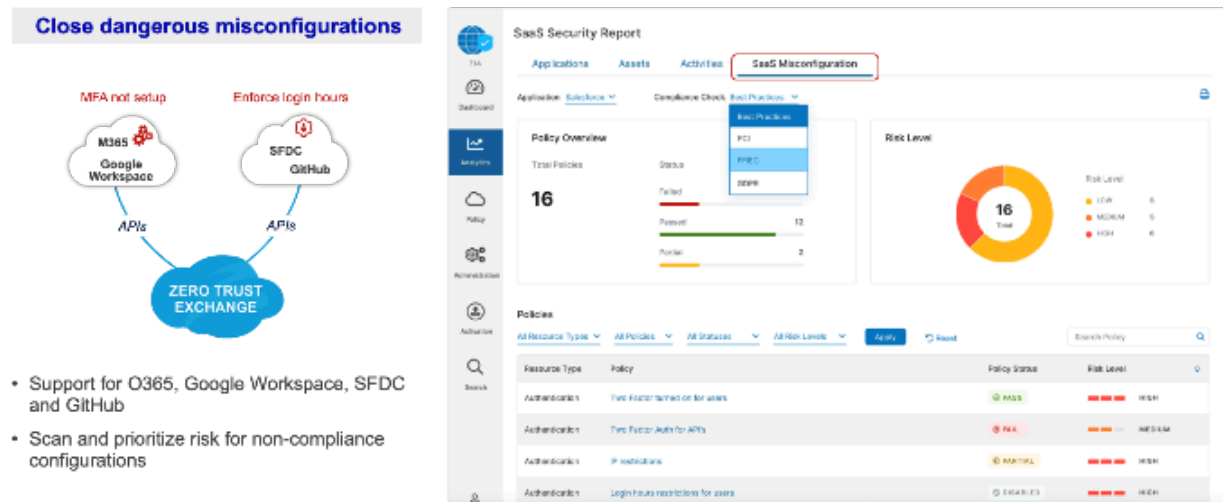
- **Outbound emails:** Enforces **data loss prevention (DLP)** policies

5. SaaS Security Posture Management (SSPM)

- Ensures compliance and prevents cloud misconfigurations
- Monitors third-party apps for potential security risks

How SaaS Security Posture Management (SSPM) Works

Protect Data with SSPM (SaaS Security Posture Management)



1. Cloud Misconfiguration Detection

Cloud misconfigurations often lead to data leaks and security breaches. Many organizations have multiple administrators managing different SaaS applications like **Office 365** and **Salesforce**, leading to inconsistent security settings.

- Zscaler's **SSPM continuously scans cloud configurations**, identifying potential vulnerabilities.
- Using **predefined security signatures**, SSPM **automatically evaluates security settings** upon onboarding new applications.

Example: If **multi-factor authentication (MFA)** is **not enabled** for Office 365, SSPM detects this misconfiguration and alerts administrators.

2. Compliance Mapping

Zscaler's SSPM aligns misconfigurations with various **compliance frameworks**, including:

- **PCI DSS** (Payment Card Industry Data Security Standard)
- **GDPR** (General Data Protection Regulation)
- **FFIEC** (Federal Financial Institutions Examination Council)
- **Cloud Security Best Practices**

This capability ensures that security teams can **identify and remediate misconfigurations** while maintaining compliance with industry standards.

3. Third-Party Application Risk Management

Many **third-party applications** integrate with corporate SaaS environments through **API tokens and service accounts**. These apps can gain access to critical business applications like **Exchange, Gmail, OneDrive, and SharePoint**, posing a potential security risk.

- SSPM provides **full visibility into all connected third-party apps**.
- Administrators can build policies to **block unauthorized applications** from accessing corporate data.

Example: If an application like **Calendly** connects to **corporate email**, administrators can **revoke its access** automatically.

By **combining data protection, cloud security posture management, and third-party risk visibility**, Zscaler's **SaaS Security Platform** offers a **comprehensive solution** to safeguard **sensitive cloud data**, ensuring compliance and reducing security risks across the enterprise.

Review: Key Takeaways on Zscaler Data Protection

In this section, you explored **Zscaler's Data Protection capabilities** designed to **secure an organization's data at rest** across **SaaS applications and public cloud environments**. Key areas covered include:

Out-of-Band CASB Overview & Use Cases:

- Zscaler's **Out-of-Band Cloud Access Security Broker (CASB)** is designed to **secure data at rest** within SaaS applications and public cloud storage.
- By leveraging **Zscaler's Data Loss Prevention (DLP) capabilities** and **Cloud Sandbox**, it ensures **sensitive data remains protected** against exposure and cyber threats.

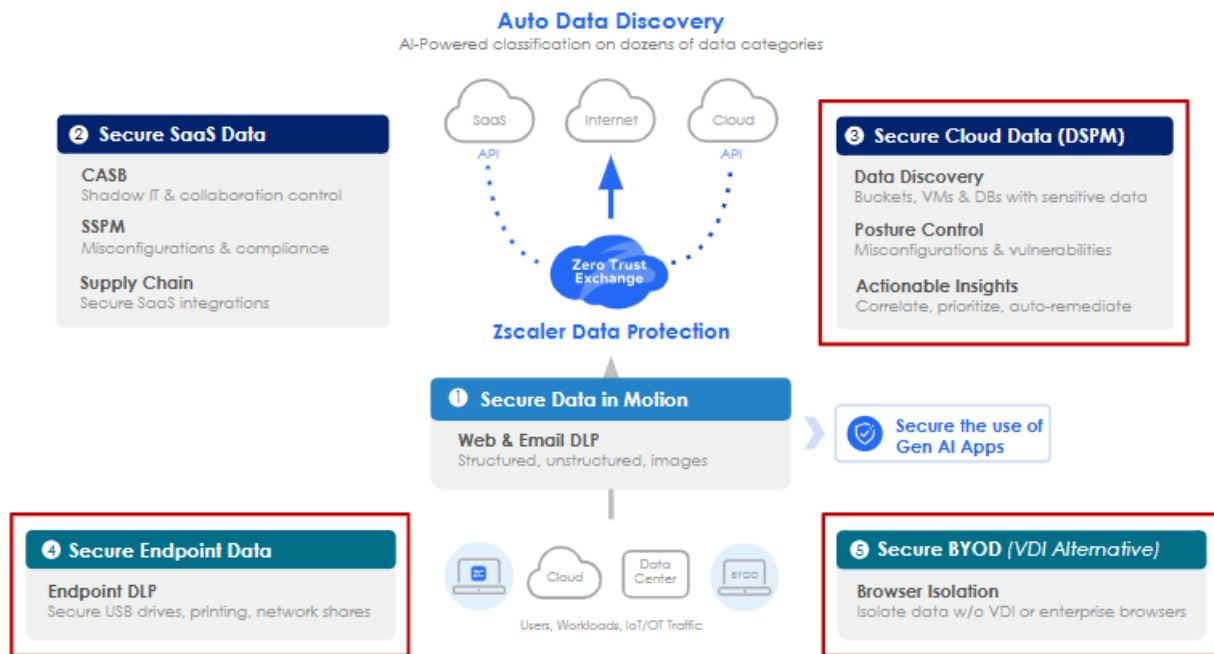
SaaS Security Posture Management (SSPM):

- **SSPM continuously scans SaaS applications for misconfigurations**, identifying potential security risks.
- Using a **comprehensive set of predefined security signatures**, Zscaler evaluates **cloud configurations** upon onboarding a new application.

Example: If **multi-factor authentication (MFA) is not enabled** for Office 365, SSPM detects the misconfiguration and alerts administrators.

Zscaler's **unified approach** to data protection helps organizations **safeguard sensitive information, prevent misconfigurations, and maintain compliance** while reducing security risks across cloud environments.

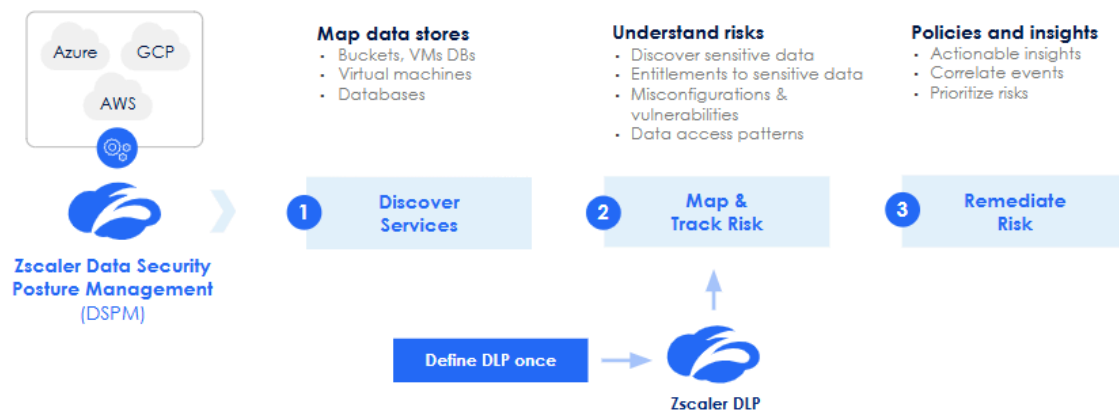
Secure Cloud Data, Endpoint Data, and BYOD



Secure Cloud Data with DSPM

Securing **data at rest** within **public cloud environments** is critical, as these platforms host vast amounts of sensitive and dynamic information. Often, organizations **lack visibility into where data is stored** and **overlook potential misconfigurations**, increasing security risks. **Zscaler Data Security Posture Management (DSPM)** enhances cloud data security by providing **comprehensive visibility, risk assessment, and remediation** for data stored in public cloud infrastructures.

Secure Cloud Data: Protect Clouds and Stop Breaches with DSPM



Integrated DLP to secure structured & unstructured data in public cloud

Step 1: Discover and Map Cloud Data Stores

The first step in securing cloud data is identifying and mapping where **data is stored across the organization's infrastructure**. This includes discovering:

- **Storage Buckets**
- **Virtual Machines**
- **Databases**

Step 2: Assess Risks and Identify Threats

Once data locations are mapped, the next step is to analyze **potential risks associated with these data stores**, including:

- **Identifying and classifying sensitive data** within mapped storage.
- **Assessing access permissions** to determine who can view or modify the data.
- **Detecting misconfigurations or vulnerabilities** that could lead to unauthorized access or data breaches.
- **Monitoring data access behaviors** to identify suspicious or unusual patterns.

Step 3: Remediate Risks with Actionable Insights

To strengthen cloud security, DSPM enables organizations to take **proactive remediation measures**, such as:

- **Providing actionable insights** to address security risks.
- **Correlating security events** for a broader understanding of potential threats.
- **Prioritizing risks** based on severity and impact for efficient mitigation.

Integrating **DSPM into your data protection and DLP platform** ensures **continuous security monitoring, compliance, and proactive risk management**. By leveraging **comprehensive cloud visibility and automated risk remediation**, organizations can **effectively secure their cloud data and minimize exposure to threats**.

Secure Endpoint Data: A Streamlined Approach to Endpoint DLP

Protecting **endpoint data** is essential, as large volumes of sensitive information can be **downloaded, stored, and shared** across devices. **Zscaler's Endpoint Data Loss Prevention (DLP)** offers a **seamless, high-performance solution** by leveraging the existing **Zscaler agent**, ensuring effortless deployment for customers who have already integrated it into their infrastructure. This **lightweight, cloud-based approach** scans data in real time **without disrupting user experience**.

Comprehensive Data Loss Control

Zscaler's **Endpoint DLP** provides **granular control** over common **data exfiltration channels**, including:

- **USB drives and removable storage** (flash drives, external hard drives).
- **Local and network printing** (to prevent unauthorized hard copies).
- **Network shares** (to control internal file transfers).
- **Personal cloud storage accounts** (e.g., Dropbox, OneDrive).
- **Endpoint-installed applications** that may covertly transfer data using certificate pinning.

Key Benefits of Zscaler Endpoint DLP

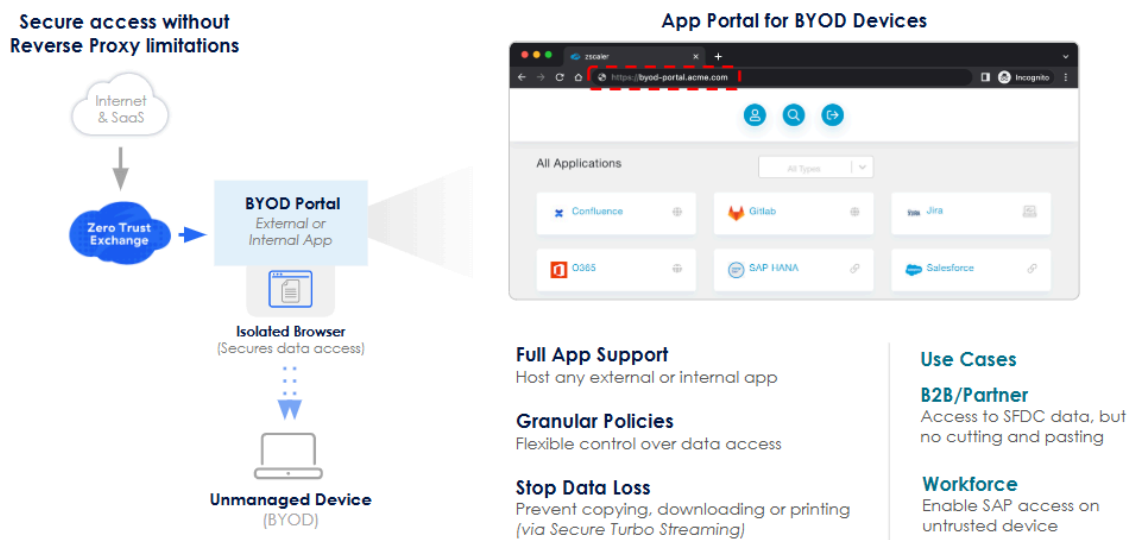
- **Unified Policy Enforcement:** Uses **existing Zscaler DLP policies**, ensuring consistency across cloud, network, and endpoints.
- **Seamless Deployment:** Instantly activates **without additional agents** for customers using Zscaler's platform.
- **Lightweight, High-Performance Agent:** Operates with **minimal system impact**, ensuring smooth user experience.
- **Advanced Forensics & Automation:** Provides **real-time insights, dashboards, and automated workflows** for faster incident response.

With **Zscaler Endpoint DLP**, organizations gain **enhanced visibility, control, and protection** over sensitive data, **preventing unauthorized access and reducing data loss risks** across endpoint devices.

Securing Unmanaged Devices (BYOD) with Browser Isolation

Unmanaged devices, commonly referred to as **BYOD (Bring Your Own Device)**, include **personal devices used by employees, contractors, or business partners** to access corporate data. The challenge with BYOD is that while these devices may require access to company resources, they are **not owned or controlled by the organization**. This means security teams **cannot enforce policies, perform remote wipes, or manage configurations** as they would with corporate-owned devices.

Secure BYOD: Protect Data going to Unmanaged devices



The Challenge with Traditional Approaches

Some vendors attempt to secure BYOD access using **reverse proxies**, but this method is often **complex, difficult to manage, and prone to compatibility issues**. A more **seamless and secure** approach is **browser isolation**, which ensures corporate data never resides on an unmanaged device.

How Browser Isolation Works

With **Zscaler Browser Isolation**, users can securely access applications **without installing an agent** on their personal devices. Instead, they log into a **secure web portal**, where the applications they need are **rendered in an isolated browser environment**.

- **No Data Storage on the Device:** Instead of directly accessing the corporate network, the user **interacts with applications through a pixel-streamed session**. This ensures that **no files, sensitive data, or downloads** reside on the personal device.

- **Restricted User Actions:** Features like **cut, copy, paste, print, and download are disabled**, preventing data from being exfiltrated.
- **Seamless and Secure Experience:** Users can work as usual, but all interactions remain within the **isolated browser session**, significantly reducing security risks.

Ideal Use Cases

Browser Isolation is particularly valuable for:

- **Third-party contractors** accessing corporate applications.
- **B2B interactions** where external users need temporary or controlled access.
- **Remote employees** using personal devices without compromising security.

By leveraging **Zscaler Browser Isolation**, organizations can enable **secure access to corporate applications** while ensuring that **sensitive data remains fully protected, even on unmanaged devices**.

Risk Management

Understanding Risk Management in Cybersecurity

Risk management is a **strategic process** aimed at protecting an organization's **sensitive data, systems, and operations** from potential threats. In the context of **cyber risk management**, the primary objective is to **minimize potential damage** by continuously **enhancing security controls, reducing vulnerabilities, and ensuring operational continuity** even in the face of cyber threats.

Types of Cybersecurity Risks

1. **Strategic Risk** – Occurs when cybersecurity decisions are **misaligned** with the organization's long-term objectives, leading to **inefficient investments** and potential security gaps.
2. **Cyber Risk** – Represents the possibility of **financial, operational, or reputational damage** due to **cyberattacks or data breaches** that compromise sensitive information.
3. **Operational Risk** – Involves **disruptions** in cybersecurity operations caused by **system failures, human errors, or misconfigurations**, potentially exposing vulnerabilities.
4. **Financial Risk** – Refers to **monetary losses** resulting from cyber incidents, including the costs of **incident response, legal actions, regulatory fines, and brand recovery efforts**.
5. **Compliance Risk** – The risk of **failing to meet cybersecurity regulations and industry standards**, which can lead to **legal penalties, audits, and loss of business trust**.
6. **Reputational Risk** – The potential harm to an organization's **brand image and customer trust** following a security breach, often leading to **long-term business impact**.

By implementing **proactive risk management strategies**, organizations can **identify, assess, and mitigate risks** effectively, ensuring **resilience against evolving cybersecurity threats** while maintaining **regulatory compliance and business continuity**.

Zscaler Comprehensive Risk Management Suite

Zscaler provides a **holistic approach** to risk management with a suite of **advanced security solutions** designed to identify, quantify, and mitigate cyber threats.

- **Risk360** delivers **insights into your Zscaler environment**, highlighting areas that need improvement. It **quantifies risks** using cyber insurance benchmark data and provides **remediation guidance** to reduce potential threats.
- **Unified Vulnerability Management** consolidates security findings from multiple tools, **prioritizes high-risk threats**, automates remediation workflows, and **monitors security posture over time** while ensuring SLA compliance.
- **External Attack Surface Management** continuously scans public-facing assets to **identify potential exposures**, ensuring vulnerabilities are discovered before attackers can exploit them.
- **Zscaler Deception** enables **quick deployment of honeypots** to lure malicious users, allowing security teams to detect and neutralize threats as soon as they infiltrate the environment.
- **Identity Protection** proactively scans **Active Directory** for misconfigurations, **excessive permissions, and exposed credentials**. It also detects malicious activity such as **kerberoasting attacks**, adjusting access rights to **limit attacker movements**.
- **Breach Predictor** leverages **machine learning to analyze logs** for early indicators of compromise, **assessing attack probabilities** and identifying emerging threats before they escalate.

By integrating these capabilities, Zscaler's **Risk Management Suite** provides a **proactive defense strategy**, helping organizations **strengthen security posture, minimize attack surfaces, and mitigate threats before they cause damage**.

Zscaler Risk360: Advanced Cyber Risk Quantification & Management

Zscaler **Risk360** is a comprehensive **risk quantification and visualization platform** designed to help organizations **identify, measure, and mitigate cybersecurity risks** effectively. By ingesting **real-world data** from both **external sources and Zscaler's environment**, Risk360 provides a **detailed and data-driven assessment** of an organization's **risk posture**. The platform evaluates over **100+ risk factors** spanning the **four stages of an attack** to deliver actionable insights.

Key Benefits of the Risk360 Platform

- **Cyber Risk Quantification**
Tracks and measures **cyber risks across the attack chain** with **115+ risk factors** from both internal and external sources.

- **Cyber Risk Reporting**
Generates **board-ready reports**, **AI-driven security maturity assessments**, and **SEC-aligned insights** with just a click.
- **Financial Risk & Compliance Mapping**
Utilizes **Monte Carlo simulations** to quantify **financial exposure** and aligns security controls with frameworks like **NIST** and **MITRE**.
- **Risk Mitigation Workflows**
Provides **detailed investigative insights** to quickly **remediate risks** and **trigger security workflows** for proactive response.
- **Asset-Based Risk Analysis**
Offers a **bottom-up risk assessment** per **endpoint**, allowing security teams to **prioritize and mitigate risks** tied to specific assets.
- **Customizable Risk Alerting**
Enables **real-time alerting** based on **custom criteria** with **flexible throttling rules** and **multiple delivery mechanisms** for seamless incident response.

By integrating **risk visualization**, **financial impact analysis**, and **automated workflows**, Zscaler **Risk360** empowers security teams to **proactively manage cyber risks**, **strengthen compliance**, and **enhance overall resilience** against emerging threats.

Vulnerability Management: A Critical Component of Cybersecurity

Vulnerability management and risk management are often used interchangeably, but they serve **distinct purposes** within an organization's **cybersecurity framework**. While both contribute to a robust defense strategy, understanding their differences is essential for implementing an **effective risk mitigation plan**.

Key Characteristics of Vulnerability Management

- **Prioritization**

Not all vulnerabilities carry the same risk level. Effective **vulnerability management** assesses each **threat's severity** based on factors such as the **Common Vulnerability Scoring System (CVSS) score**, **asset criticality**, and **exploitability** to **prioritize remediation efforts**.

- **Continuous Monitoring**

New vulnerabilities emerge **regularly**, making **vulnerability management an ongoing process** rather than a one-time fix. **Regular scanning and assessment** ensure that organizations stay ahead of evolving threats.

- **Identification**

The process begins with **scanning systems, networks, and applications** to uncover **known vulnerabilities**—such as **unpatched software, misconfigurations, and outdated protocols**—that could be exploited by attackers.

- **Remediation**

Once vulnerabilities are identified and prioritized, organizations take **appropriate remediation actions** such as **patching, mitigating risks, or accepting** the vulnerability based on its **potential impact** and the organization's **security resources**.

By implementing a structured **vulnerability management program**, organizations can **proactively reduce security risks, minimize exposure to cyber threats, and strengthen overall security posture**.

Zscaler Data Fabric for Security

The **Data Fabric for Security** serves as the **foundational layer** that powers current and future **Zscaler applications**. Designed specifically for **security use cases**, the data model is both **structured and flexible**, allowing organizations to integrate **any data source** to enhance their security operations.

Currently, the **data fabric** fuels Zscaler-built applications, but its future vision extends to enabling customers to **build their own applications** on top of this powerful security **data infrastructure**.

Key Capabilities of the Data Fabric for Security

Data Ingestion

- The data fabric **ingests data from any source**, supporting **multiple formats** including JSON, JSONL, CSV, ZIP, XML, ZST, and ZSTD.
- It includes **150+ pre-built connectors**, allowing seamless integration with various **security tools**.
- For **new sources**, data can be pulled in through a **data file**—for example, during a Proof of Value (PoV) assessment. **New connectors can be developed in just a few weeks**.

Harmonization & Mapping

- The data fabric **normalizes data** from different sources, ensuring that entities of the **same type** (but named differently) are **unified**.
- It **automatically maps** source data to predefined entity names in the **data model**, and customers can **add new entities** as needed.

Deduplication

- Security tools often **report on the same assets, vulnerabilities, and users**, leading to redundant data.
- The data fabric **identifies and removes duplicates**, providing an **accurate view** of asset counts, Common Vulnerabilities and Exposures (CVEs), and other security factors.
- It also **consolidates remediation tasks**, reducing redundant work and ensuring efficiency.

Correlation & Enrichment

- The data fabric **correlates related information** from different tools, enhancing the **overall understanding** of each entity.
- For example, an **EDR (Endpoint Detection & Response) tool** may report an **OS version** running on an endpoint, while an **asset management tool** provides the **device name**.
- The data fabric **aggregates and enriches** this information, giving security teams a **comprehensive view** of their environment.

By leveraging **Zscaler's Data Fabric for Security**, organizations can **unify, analyze, and optimize security data** across multiple tools, enabling **smarter decision-making** and **more effective risk management**.

Unified Vulnerability Management (UVM)

Zscaler takes a **modern and innovative approach** to vulnerability management, addressing **longstanding challenges** with a **data-centric strategy**. Unlike **traditional** or **second-generation vulnerability management solutions** that primarily focus on **CVE aggregation**, Zscaler expands the scope by **harnessing security data holistically**.

At the core of this approach is **Zscaler's Data Fabric for Security**, which enables organizations to **streamline and elevate** their **vulnerability management (VM) programs** with **greater efficiency and accuracy**.

Key Capabilities of Unified Vulnerability Management

Comprehensive Data Integration

- Zscaler's platform **aggregates and correlates** security data from **multiple sources**, providing a **unified** and **holistic** view of an organization's security landscape.
- This broad integration enhances **visibility** and enables **better-informed decision-making**.

Rich Contextual Insights

- Security findings are **enriched with contextual data** from multiple security tools and business systems.
- This approach **identifies security gaps** based on an organization's **specific risk profile**, allowing for **targeted** and **effective risk mitigation**.

Dynamic Risk Assessment

- Zscaler provides **multi-factor risk scoring**, which incorporates **mitigating controls** and aligns with **industry best practices**.
- These **customizable risk scores** allow teams to **prioritize** vulnerabilities based on their **unique environment** and **business impact**.

Automated Workflows

- Zscaler enables **automated ticket assignment and tracking**, integrating seamlessly with an organization's **existing structure and systems**.
- By automating vulnerability response workflows, security teams can **swiftly address** critical risks before they can be **exploited**.

Customizable Dashboards & Reporting

- A **dynamic, real-time reporting system** consolidates data from **multiple sources**, providing **clear insights** into security posture, KPIs, SLAs, and team performance.
- Organizations can create **custom dashboards** tailored to their **specific needs**, ensuring **better oversight** of security operations.

Enhancing Security Posture with Zscaler UVM

By leveraging **Zscaler's Unified Vulnerability Management (UVM)**, organizations can **streamline their security efforts, reduce risk exposure, and enhance overall cyber resilience**—all with **less complexity and greater efficiency**.

External Attack Surface Management (EASM)

External Attack Surface Management (EASM) is the **continuous discovery, inventory, classification, and monitoring** of an organization's **internet-exposed digital assets**. These assets include **domains, IP addresses, subdomains, SSL/TLS certificates, cloud instances, and third-party integrations**. EASM is essential for **identifying and mitigating vulnerabilities** before cyber attackers can exploit them.

How Zscaler EASM Enhances Security

Zscaler's **EASM** sets itself apart by integrating **advanced scanning techniques** and **threat intelligence** within **Zscaler's Zero Trust Exchange (ZTE) platform**. This integration not only helps **identify exposed assets** but also **prioritizes risks** based on **exploitability likelihood and potential business impact**.

Key Benefits of Zscaler EASM

Comprehensive Asset Discovery

- Uses **passive and active scanning** to continuously **detect and inventory all internet-facing assets**.
- Identifies not only **known** assets but also **forgotten, orphaned, or shadow IT** assets that may have been overlooked.

Risk-Based Prioritization

- Goes beyond traditional **vulnerability severity scoring** by considering **real-world exploitability factors**.
- Leverages intelligence from sources like the **CISA Known Exploited Vulnerabilities (KEV) catalogue** to **prioritize remediation efforts** effectively.

Real-Time Monitoring & Alerts

- Continuously monitors **new exposures, misconfigurations, and emerging vulnerabilities**.
- Provides **real-time alerts** to security teams, enabling **swift incident response** and risk mitigation.

Actionable Remediation Insights

- Offers **detailed, step-by-step remediation guidance** for addressing risks.
- Helps mitigate threats from **misconfigurations, outdated software, expired certificates, and other security gaps**.

Proactive Defense with Zscaler EASM

By leveraging **Zscaler EASM**, organizations gain **complete visibility** into their **external attack surface**, ensuring **continuous monitoring, proactive risk prioritization, and rapid remediation**—reducing the likelihood of **exploits and security breaches**.

Deception: Proactive Threat Detection & Disruption

Zscaler Deception is an advanced **targeted threat detection solution** designed within the **Zscaler Zero Trust architecture**. It utilizes **high-interaction decoys and lures** to detect, contain, and disrupt **sophisticated cyber threats** that evade traditional security measures. These include **advanced persistent threats (APT)**, **exploits**, **reconnaissance**, **lateral movement**, **Active Directory compromise**, **supply chain attacks**, **human-operated ransomware**, and **attacks on SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control Systems)**.

How Zscaler Deception Works

Zscaler Deception **tricks attackers into engaging with decoys** instead of real assets, enabling early detection and **rapid threat containment**. This approach helps prevent attackers from **gaining access, moving laterally, or exfiltrating data**.

Deception Stages & Benefits

Detect Pre-Breach Warnings

- Identifies early attack signals from **ransomware operators, APT groups, and other adversaries** conducting **stealthy reconnaissance**.
- **Perimeter decoys** expose and flag **suspicious pre-breach activities** that traditional defenses may overlook.

Stop Lateral Movement

- Detects **compromised accounts and devices** attempting to move laterally within the network.
- Uses **application decoys and endpoint lures** to intercept attackers and prevent unauthorized access to critical systems.

Disrupt Ransomware Spread

- Deploys **decoys across cloud environments, networks, endpoints, and Active Directory** to serve as **traps** for ransomware.
- Limits the ability of **ransomware operators to escalate privileges, encrypt files, or propagate within the network**.

Real-Time Threat Containment & Automated Response

- **Seamless integration** with **Zscaler security solutions and third-party security tools** such as **SIEM, SOAR, and SOC platforms**.
- Enables **automated threat containment**, allowing security teams to **mitigate attacks in real time** before damage occurs.

Zscaler Deception: A Game-Changer for Cyber Defense

By deploying **decoys and lures** across the **entire attack surface**, Zscaler Deception **proactively detects, delays, and neutralizes** threats before they cause harm—ensuring **stronger protection** against **advanced cyberattacks, data breaches, and ransomware**.

ITDR: Identity Threat Detection & Response

As **identity systems become prime targets** for cyber attackers, organizations must **fortify their defenses** against identity-based threats. With the increasing reliance on digital ecosystems, the risk of **compromised credentials, unauthorized access, and identity-based breaches** has grown exponentially. **Zscaler Identity Threat Detection and Response (ITDR)** provides **proactive protection** by continuously **monitoring, detecting, and mitigating identity threats** before they escalate.

Why ITDR is Crucial

Preserve Strong Security

ITDR **monitors identity systems for misconfigurations and vulnerabilities** that could be exploited by attackers.

Reduce Identity-Related Risks

Detects and **remediates identity threats in real time**, minimizing the risk of credential abuse, privilege escalation, and unauthorized access.

Mitigate Organizational Risk

Without ITDR, organizations face **potential data breaches, financial losses, and reputational damage** due to **compromised identity systems**.

Lower Risk of Unauthorized Access

ITDR actively **blocks identity threats and prevents lateral movement**, unlike traditional security solutions that focus only on perimeter-based defenses.

Key Benefits of Zscaler ITDR

No Additional Agents or Virtual Machines Required

Built directly into the Zscaler Client Connector, ITDR **seamlessly integrates** without requiring additional software or infrastructure.

Integrated with Access Policy Controls

Zscaler Zero Trust Exchange dynamically applies **access control policies** to **block compromised users** upon detecting an identity attack.

Credential Exposure Visibility

ITDR **identifies exposed credentials** on endpoints, allowing organizations to **clean up and enforce policies**, reducing the risk of post-compromise exploitation.

Seamless SOC and Security Tool Integrations

ITDR integrates with **leading security platforms** such as **CrowdStrike, Microsoft Defender, VMware Carbon Black, and SIEM solutions**, enhancing **threat investigation and response** capabilities.

Enhancing Identity Security with Zscaler ITDR

By **proactively monitoring and mitigating identity threats**, Zscaler ITDR helps **organizations** maintain **strong identity security**, **prevent unauthorized access**, and **minimize risks associated with compromised credentials**—ensuring a **robust Zero Trust security posture**.

Breach Predictor: Preemptive Detection and Response (PreDR)

Zscaler Breach Predictor is the industry's **first Preemptive Detection and Response (PreDR) solution**, designed to **identify ongoing cyberattacks** and **anticipate potential future threats** before they materialize. By leveraging **advanced AI and machine learning (ML) analytics**, Breach Predictor provides **real-time visibility** into **attacker tactics, techniques, and procedures (TTPs)** mapped to the **MITRE ATT&CK framework**. This **proactive approach** helps organizations **detect evolving attack patterns**, **assess breach probabilities**, and **strengthen security defenses before exploitation occurs**, ultimately **simplifying security operations** and **reducing cyber risk**.

Key Benefits of Zscaler Breach Predictor

1. Improve Attack Awareness

- Gain **real-time insights** into **attack pathways** and **malicious activities**.
- Identify impacted users and contain threats **before damage occurs**.

2. Strengthen Preemptive Security

- Utilize **AI-powered breach probability scoring** to **identify and mitigate potential attack paths**.
- Proactively **reduce cyber risk** by addressing vulnerabilities **before they can be exploited**.

3. Enhance Security Operations Center (SOC) Efficiency

- Reduce **false positives** and streamline **incident triage** with optimized workflows.
- Decrease the number of security events requiring **manual SOC intervention**, improving **incident response time and efficiency**.

Empowering Proactive Cyber Defense

By integrating **predictive analytics**, **AI-driven threat intelligence**, and **real-time attack visualization**, **Zscaler Breach Predictor** enables organizations to **stay ahead of evolving threats**, proactively **reduce security vulnerabilities**, and **enhance cybersecurity resilience** in a dynamic threat landscape.

Zscaler Digital Experience

Understanding ZDX: Enhancing Digital Experiences

This chapter serves as a **comprehensive guide** to understanding **how ZDX operates** and the **process behind delivering seamless and secure digital experiences** for users across various environments.

To build a **strong foundational understanding**, the chapter is structured into two key sections:

1. Introduction to ZDX & Architectural Overview

- Gain an **understanding of ZDX** and how it optimizes digital experiences.
- Explore its **architecture**, the core framework that enables its functionality.

2. Key Features, Use Cases, and Dashboard Insights

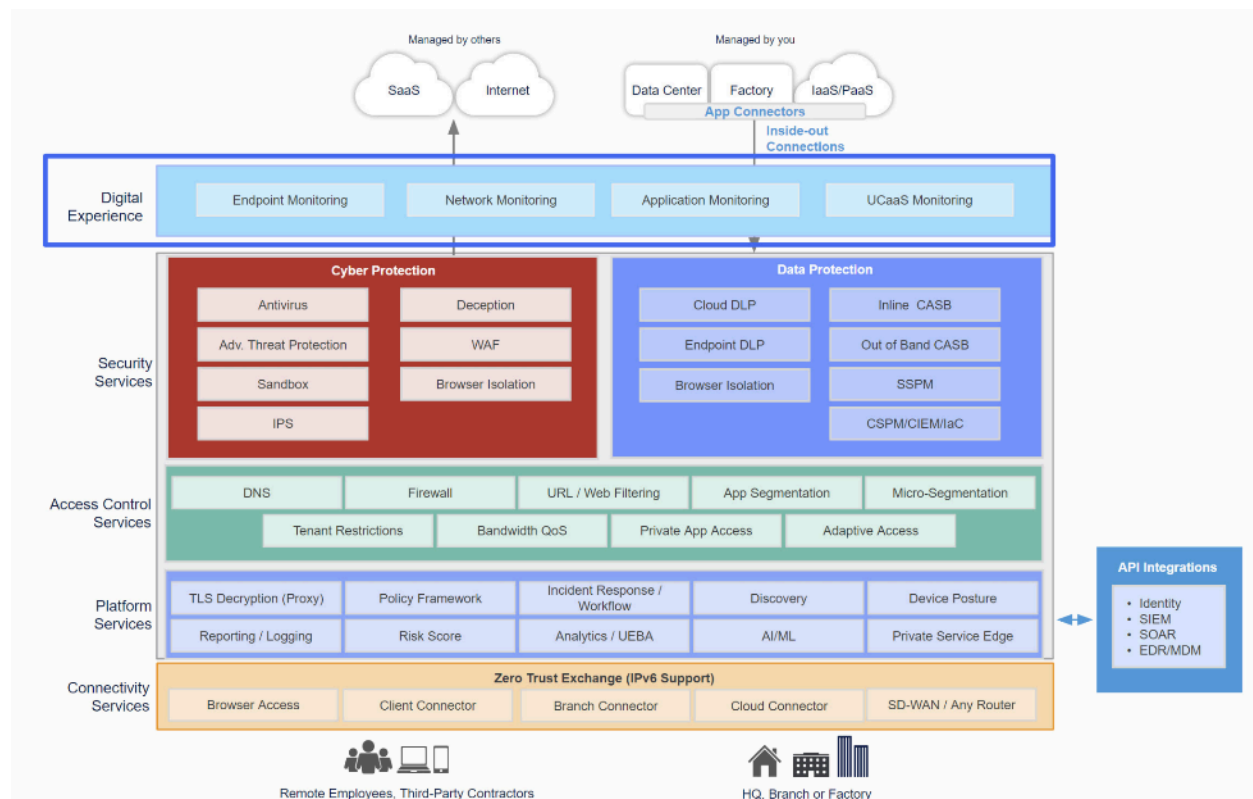
- Delve into the **critical features** of ZDX and how they work together to enhance performance.
- Discover **real-world use cases** demonstrating its impact.
- Navigate the **ZDX Dashboard** to understand monitoring, analytics, and reporting capabilities.

By the end of this chapter, you will have a **strong grasp of ZDX, its architecture, key capabilities, and practical applications**, equipping you with the knowledge needed to leverage ZDX for optimized digital experiences.

By the end of this chapter, you will be able to

1. **Describe** the primary function of ZDX and how it enhances digital experiences for users
2. **Identify** the components that constitute the architecture of ZDX
3. **List** key features of ZDX that contribute to seamless digital experiences
4. **Categorize** ZDX features to their corresponding use cases to demonstrate how they address specific digital experience challenges
5. **Navigate** the ZDX Dashboard

Introduction to Zscaler Digital Experience (ZDX)



In today's hybrid work environment, where employees frequently switch between remote and office settings, ensuring a seamless digital experience is more critical than ever. The growing reliance on cloud-based applications and distributed workforces has made real-time performance monitoring an essential aspect of IT operations. **Zscaler Digital Experience (ZDX)** is built on the **Zero Trust Exchange**, offering **comprehensive, end-to-end digital experience monitoring**.

Throughout this chapter, we will explore the key functionalities of ZDX, including:

- **Endpoint Monitoring**
- **Network Monitoring**
- **Application Monitoring**
- **UCaaS (Unified Communications as a Service) Monitoring**

We begin by examining the challenges of traditional monitoring approaches and how **ZDX provides a more efficient solution**, followed by an overview of its core features and capabilities.

Challenges with Traditional Monitoring Approaches

For many years, organizations primarily focused on **optimizing the digital experience for employees working in corporate offices**. IT investments were centered on securing and

enhancing productivity within office environments, regardless of where applications and data resided. However, with the shift to **remote work**, employees now **rely on home Wi-Fi networks and local ISPs** to access **SaaS and cloud applications directly**.

This shift has placed significant pressure on:

- **Network operations** that now need to manage a **highly distributed workforce**
- **Service desks** that have seen a **35% increase in support tickets** related to connectivity and performance issues
- **Security teams** that must balance providing access with maintaining **strict security policies**

New Reality: Work From Anywhere Using Apps Everywhere



63% of employees prefer **hybrid or remote working** model, post pandemic
McKinsey&Company

Impact on IT Teams

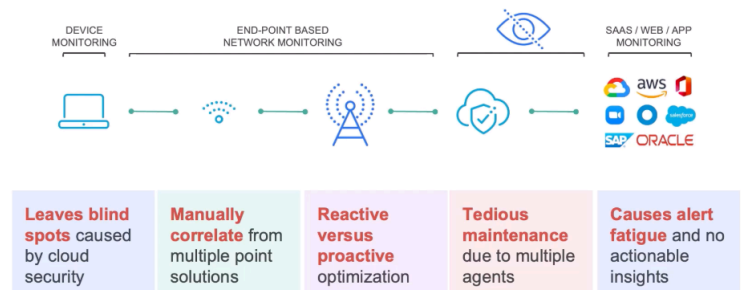
90% or more, of enterprise networks carry technical debt, and struggle to support hybrid workforce
Gartner

35% or more, increase in number of support tickets raising costs by more than 30%
MetricNet

Traditional monitoring tools **fail to provide full visibility** because they are often **siloed**, focusing on only one area:

- **Device Monitoring:** Tracks only endpoint health without understanding network conditions
- **Network Monitoring:** Captures network traffic but lacks insight into user experience
- **SaaS Monitoring:** Monitors applications but not the **end-to-end user journey**

Point Tools Fail to Equip IT Teams in the Hybrid Workplace



As a result, IT teams **lack a unified view of performance issues**, forcing them to **manually correlate disparate metrics**, slowing down troubleshooting and increasing operational costs.

How ZDX Solves These Challenges

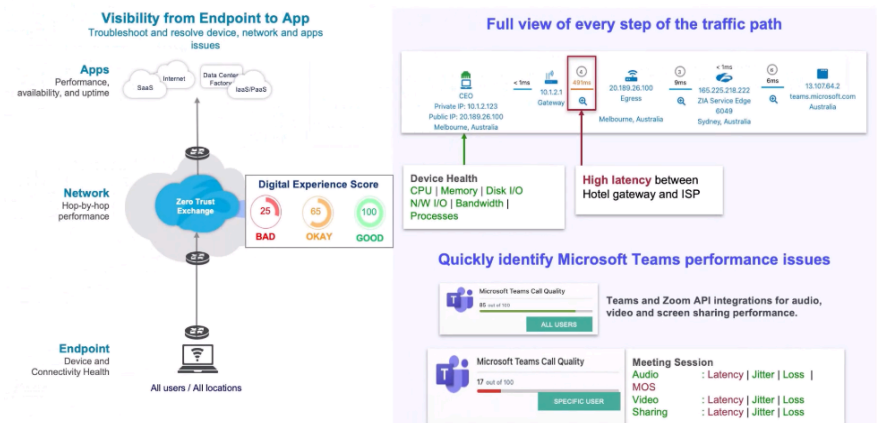
ZDX is uniquely positioned to bridge these gaps by providing a **holistic monitoring approach**, covering:

- **Application performance:** Ensures SaaS applications are accessible and performing optimally
- **Network performance:** Monitors hop-by-hop network behavior for bottlenecks
- **Endpoint health:** Identifies device issues that impact user experience

ZDX enhances monitoring capabilities by integrating data from ecosystem partners like Microsoft and Zoom, allowing IT teams to quickly pinpoint performance issues. Machine learning (ML) algorithms analyze past incidents to expose root causes, helping IT teams resolve problems at their source, rather than just addressing symptoms.

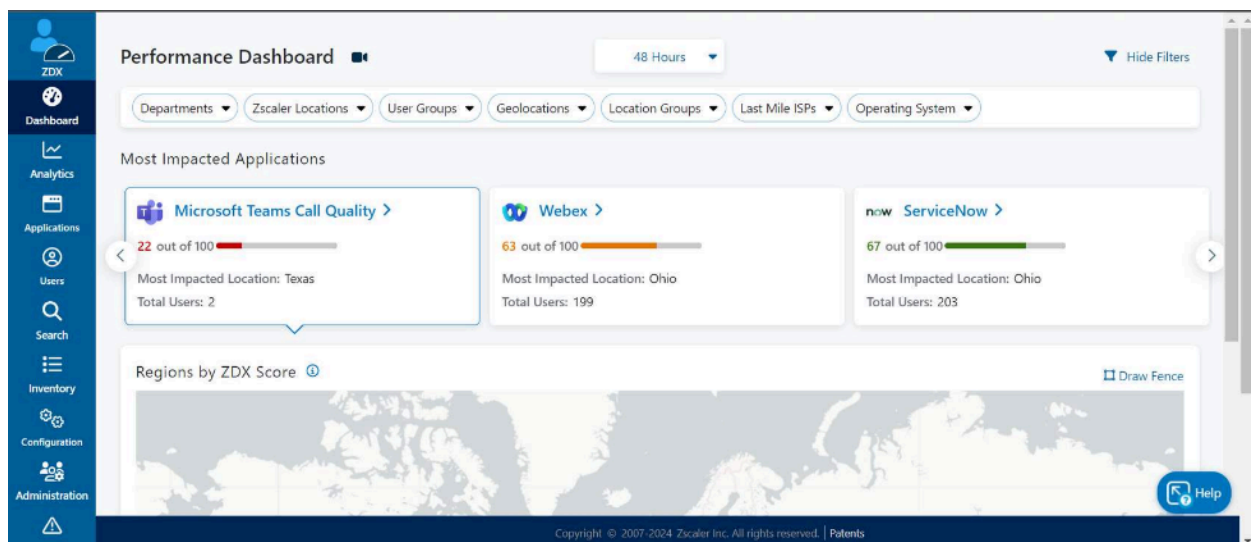
ZDX Digital Experience Scoring

Proactively Identify and Resolve Performance Issues



ZDX calculates a real-time performance score for every user, application, and location based on telemetry data collected. These scores help IT teams:

- **Assess overall organizational performance** (e.g., company-wide Microsoft Teams Call Quality Score)
- **Drill down into individual user issues** (e.g., a specific employee's Teams call quality is poor)
- **Pinpoint bottlenecks** (e.g., identifying high latency between an ISP gateway and the application's front door)



Example: Microsoft Teams Call Quality

ZDX provides a comprehensive, organization-wide assessment of Microsoft Teams call quality by generating a performance score. For instance, an organization may have an overall **Teams Call Quality Score of 85/100**, indicating good performance across the board. However, when analyzing an individual user's experience, ZDX may reveal that a specific employee has a **Teams Call Quality Score of 17/100**, signifying poor performance. By drilling down into the data, IT teams can analyze **audio, video, and screen-sharing quality** for that user's meeting, identifying the exact cause of degradation. This ability to **historically track and pinpoint specific moments of poor performance** enables IT teams to **proactively resolve issues** and improve overall digital experience.

Example: CEO's Laptop Latency Issue

In another scenario, a CEO experiences **latency while connecting to an application** despite their laptop showing optimal **CPU, memory, and disk performance**. ZDX's telemetry data quickly identifies the root cause as **high latency between the gateway and the ISP's egress service provider**. With this level of granularity, IT teams can **swiftly diagnose and address network-related performance bottlenecks**, ensuring that executives and other key personnel experience seamless connectivity. This proactive approach reduces frustration, minimizes downtime, and enhances overall user experience.

ZDX Dashboard and Telemetry Data

ZDX telemetry data is processed into interactive dashboards within the **ZDX Admin Portal**, providing:

- **A global view of all employees and key applications**
- **ZDX Scores for individual users, applications, locations, or the entire organization**
- **Drill-down capabilities to investigate performance drops**
- **Live troubleshooting tools for real-time issue resolution**

When a significant **drop in ZDX Score** is detected, IT teams can **quickly investigate the root cause and initiate live troubleshooting sessions** to resolve issues proactively.

Deployment and Activation

Deploying ZDX is **quick and seamless**, especially for existing Zscaler customers with the **Zscaler Client Connector** installed.

ZDX deployment steps:

- **Enable monitoring profiles** for key applications
- Use **pre-built templates** for popular SaaS apps (e.g., Microsoft 365, Zoom)
- Configure **custom probes** for proprietary applications
- Zscaler Client Connector **automatically starts sending probes** and collecting telemetry data

Advantages of deploying ZDX:

- **Minimal impact on end-user devices**
- **No additional agents required** (ZDX is built into Zscaler Client Connector)
- **Flexible deployment:** Enable organization-wide or group-by-group using **Active Directory** policies

ZDX is Enabled through Zscaler Client Connector

Single end-point agent for ZIA/ZPA/ZDX

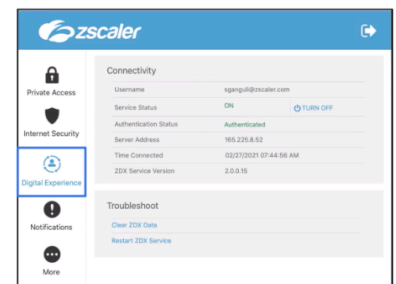
Eliminates agent sprawl (FW, VPN), simplifies IT

Lightweight and Extensible

Heavy lifting done in the Zscaler cloud, better device UX
Runs on Windows and MacOS

Easy Deployment

Just enable license for ZDX - no new deployment



Why ZDX is the Best Choice for Digital Experience Monitoring

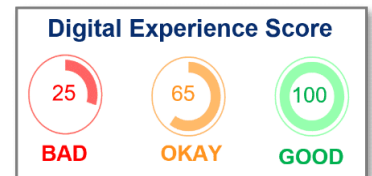
- **Unified visibility** across endpoints, networks, and applications
- **Real-time digital experience scoring** for proactive troubleshooting
- **AI-driven insights** to **identify root causes faster**
- **Seamless deployment with no disruption to end users**

By leveraging **ZDX**, organizations gain **unparalleled visibility into digital experience performance**, reducing troubleshooting time, improving IT efficiency, and enhancing employee productivity.

How the ZDX Score Works

The ZDX Score provides a quick and effective way to assess a user's digital experience and identify the root causes of any performance issues. By analyzing key performance metrics, it enables IT teams to **quickly diagnose and resolve problems** affecting user experience.

The ZDX Score is calculated by measuring the **Page Fetch Time** and **application availability** for a given user. These values are then compared against a baseline established from all users within the same geographic region (e.g., country) who are accessing the same application.



To maintain real-time accuracy, ZDX **sends a probe to an application every five minutes**. Each measurement is assigned a numerical value between **1 and 100**, representing performance quality. The **lowest recorded value within an hour** becomes the ZDX Score for that hour. This process is repeated for every defined application across all users, devices, and locations, ensuring a **comprehensive view of digital experience performance** across the organization.

One of the key advantages of ZDX is the ability to **drill down into specific performance issues** when a score appears lower than expected. By analyzing fluctuations in ZDX Scores, IT teams can proactively investigate and **determine what factors may be contributing to performance degradation**. Understanding why a good score might decline allows teams to take **immediate action** and optimize digital experiences for users.



The table below summarizes the potential causes of a low ZDX score and their corresponding descriptions.

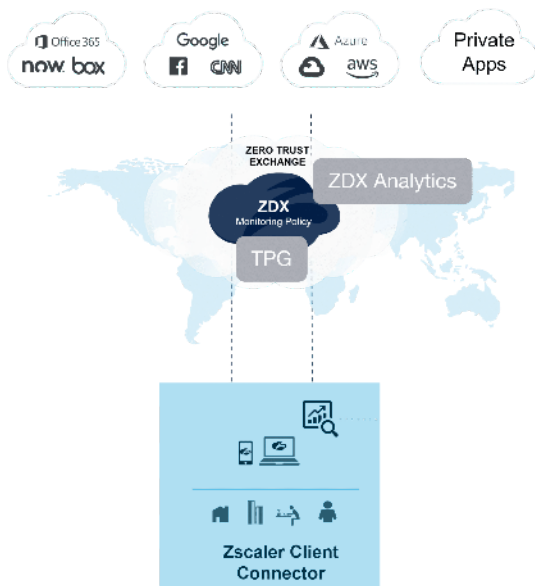
Issue Category	Possible Causes
App Issues	Typical indicators include long Page Fetch Time (PFT) and slow Server Response Time (SRT).
DNS	Use of sub-optimal DNS configurations leading to increased overall latency.
App Availability	Issues that impact application availability, often indicated by users encountering 5xx errors.
Local Wi-Fi	Weak signal strength or high latency between Wi-Fi and egress points, such as using 2.4Ghz frequency band instead of 5Ghz.
Egress Latency	Traffic backhauled through a VPN or taking too many hops before reaching the egress IP address.
Network Latency	Factors include sub-optimal routing or ISP issues up to Zscaler, high CPU/traffic on ZEN (Zscaler Enforcement Node) or ISP issues, and latency between Zscaler and the application.
Network Congestion	Manifests as latency issues, Wi-Fi problems, or high bandwidth utilization.
Device Metrics	CPU or memory spikes causing slower response times in client applications (e.g., web browsers), or CPU usage reaching 100%.
Device Events	Events that may trigger a bad score include VPN tunnel interface activities, Wi-Fi changes, or system restarts.

Review

- **Shift in Work Environment:** The transition from office-based work to remote and hybrid setups has increased the burden on network operations, service desks, and security teams. The rise in support tickets and higher service costs has made it more challenging to maintain a seamless digital experience for employees.
- **Challenges with Existing Tools:** Traditional monitoring tools operate in silos, focusing separately on **device monitoring, network monitoring, or SaaS monitoring**. This fragmented approach creates **blind spots** and forces IT teams to manually correlate data, making issue resolution slower and more complex.
- **ZDX Solution:** ZDX provides **integrated monitoring** by tracking **application performance, network performance, and device health** in a unified platform. It leverages data from key technology partners like **Microsoft and Zoom**, ensuring **comprehensive visibility** into user experiences.
- **Performance Scoring:** ZDX calculates detailed performance scores (**good, bad, or okay**) for **users, applications, and locations**. It offers drill-down capabilities to analyze individual user experiences, such as **Microsoft Teams Call Quality**, helping IT teams quickly identify and address performance issues.
- **Minimal Impact on End Users:** ZDX operates with **minimal-to-no impact** on system resources and end users. Deployment is flexible and can be customized for different **user groups via the Zscaler Client Connector Portal**, ensuring smooth activation without disruptions.

Now that you have a foundational understanding of **ZDX and the importance of the ZDX Score**, let's explore the **ZDX Architecture Overview** to see how it all comes together.

ZDX Architecture Overview



Understanding the architecture of Zscaler Digital Experience (ZDX) is essential for effectively navigating, configuring, and troubleshooting the various features and functionalities within the Digital Experience console. This section provides a high-level overview of ZDX architecture, its key components, and how it enables end-to-end monitoring of application performance.

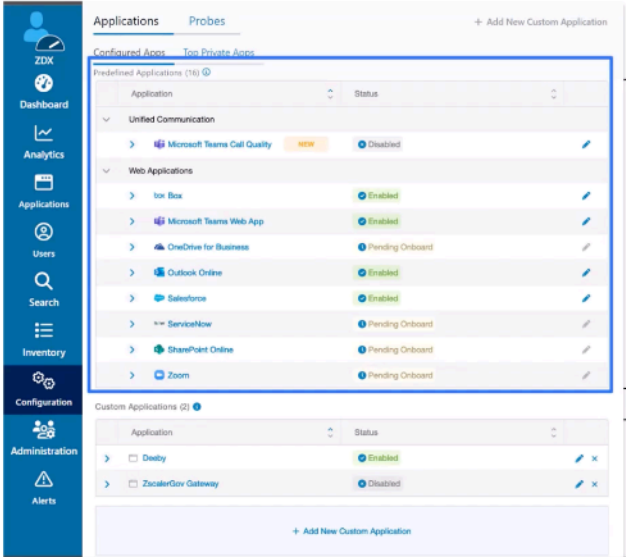
At a high level, ZDX architecture consists of three main components: destination applications, ZDX-enabled endpoints, and the ZDX infrastructure. Destination applications, such as **Box.com** or **Office.com**, are configured for monitoring within ZDX. Endpoints with **ZDX enabled** continuously probe these applications and

collect data. The core ZDX infrastructure includes essential elements like the **Telemetry and Policy Gateway (TPG)** and the **ZDX Analytics Engine**. Once a monitored application is set up in ZDX, the ZDX client probes it at a default interval of every **five minutes** and gathers performance metrics. These metrics are then sent to the **TPG**, which forwards the data to the **ZDX Analytics Engine** for processing and visualization in the **ZDX Dashboard**.

Application Monitoring in ZDX

ZDX allows for the monitoring of two types of applications: **Predefined Applications** and **Custom Applications**. Predefined applications include commonly used SaaS-based services such as **SharePoint Online, Box, and Salesforce**. When onboarded, ZDX automatically generates probes for these applications. In some cases, **tenant IDs** may need to be specified for accurate monitoring. Custom applications, on the other hand, are used to track performance for **internal or external private applications**. To monitor a custom application, at least **one web probe** must be created.

Applications



The screenshot displays the 'Applications' section of the ZDX Admin Portal. It features a sidebar with navigation options: ZDX, Dashboard, Analytics, Applications, Users, Search, Inventory, Configuration, Administration, and Alerts. The main content area is divided into two tabs: 'Configured Apps' and 'Top Private Apps'. Under 'Configured Apps', there are two sections: 'Predefined Applications (16)' and 'Custom Applications (2)'. The 'Predefined Applications' section lists various SaaS services with their status (e.g., 'Enabled', 'Pending Onboard', 'Disabled'). The 'Custom Applications' section lists user-defined applications with their status. A callout box on the right explains the difference between predefined and custom applications.

Application	Status
Unified Communication	
Microsoft Teams Call Quality	Disabled
Web Applications	
Box	Enabled
Microsoft Teams Web App	Enabled
OneDrive for Business	Pending Onboard
Outlook Online	Enabled
Salesforce	Enabled
ServiceNow	Pending Onboard
SharePoint Online	Pending Onboard
Zoom	Pending Onboard
Custom Applications	
Dealy	Enabled
ZacaterGov Gateway	Disabled

Predefined Applications: Predefined applications are available in the ZDX Admin Portal when you log in. The predefined applications provide quick and seamless application onboarding for admins.

Custom Applications: Customizable SaaS or web applications that you can create and onboard in the ZDX Admin Portal for your organization.

There are two primary components of **application monitoring** in ZDX: the **Web Probe** and the **Cloud Path Probe**. The **Web Probe** is responsible for pulling objects from the server and collecting key metrics such as **page fetch time, DNS resolution time, server response time, and application availability**. These metrics help in determining how efficiently an application is loading and performing for end users. The **Cloud Path Probe** maps the **network path** taken by traffic to reach the application. It provides insights into **network hops, latency, packet loss**, and other network performance indicators.

To enhance monitoring accuracy, ZDX also allows for **custom HTTP headers** to be configured, which is particularly useful for applications expecting specific headers during request validation. Additionally, **custom HTTP response codes** can be set, allowing organizations to define expected responses when probing applications. Default values work for most applications, but customization ensures tailored monitoring for unique environments.

Cloud Path and Network Probing

The **Cloud Path Probe** provides a deeper look into how network traffic flows to a given application. When configuring **Cloud Path**, users can specify the **protocol type** to be used. The **Adaptive Protocol** option enables ZDX to automatically determine the best protocol by selecting one with the **least latency and packet loss**. This selection process ensures that the optimal connection method is used for every network leg. If the default **ICMP protocol** is used, there is a possibility of rate limiting by certain network providers, which may affect results.

Cloud Path Probe - Protocols

- **Adaptive**
 - Best protocol for each leg in the cloud is selected via an auto-discovery process
- **ICMP**
 - Default value
 - Processed by router CPU
- **TCP**
 - Processed by router ASIC
 - Immune to rate limiting
- **UDP**
 - Some routers only respond to UDP packets
 - RFC recommended port of 33434

Cloud Path Probe Configuration

Probe Name	Application Name
SharePoint Online CloudPath Probe	SharePoint Online

Protocol: Adaptive (dropdown menu showing Adaptive, ICMP, TCP, UDP)

TCP Port: 443

Packet Count: 11

Interval (ms): 1000

Timeout (ms): 1000

Cloud Path Host: m365x167135.sharepoint.com

Probes (Web and Cloudpath)

WEB PROBE CONFIGURATION

Probe Name	Application Name
SharePoint Online Login Page Probe	SharePoint Online

Request Type: GET

Destination URL: https://m365x167135.sharepoint.com

Request Header

Name	Value
------	-------

HTTP Response Status Codes

Type to add new

- Informational responses (100-199)
- Successful responses (200-299)
- 300 Multiple Choices

HTTP Status Codes for successful availability

Number of Attempts: 1

Timeout (seconds): 60

Follow Redirect: Enable

Maximum Redirects: 5

CLOUD PATH PROBE CONFIGURATION

Probe Name	Application Name
Copy of SharePoint Online CloudPath Probe	SharePoint Online

Protocol: Adaptive (dropdown menu showing Adaptive, ICMP, TCP, UDP)

TCP Port: 443

UDP Port: 33434

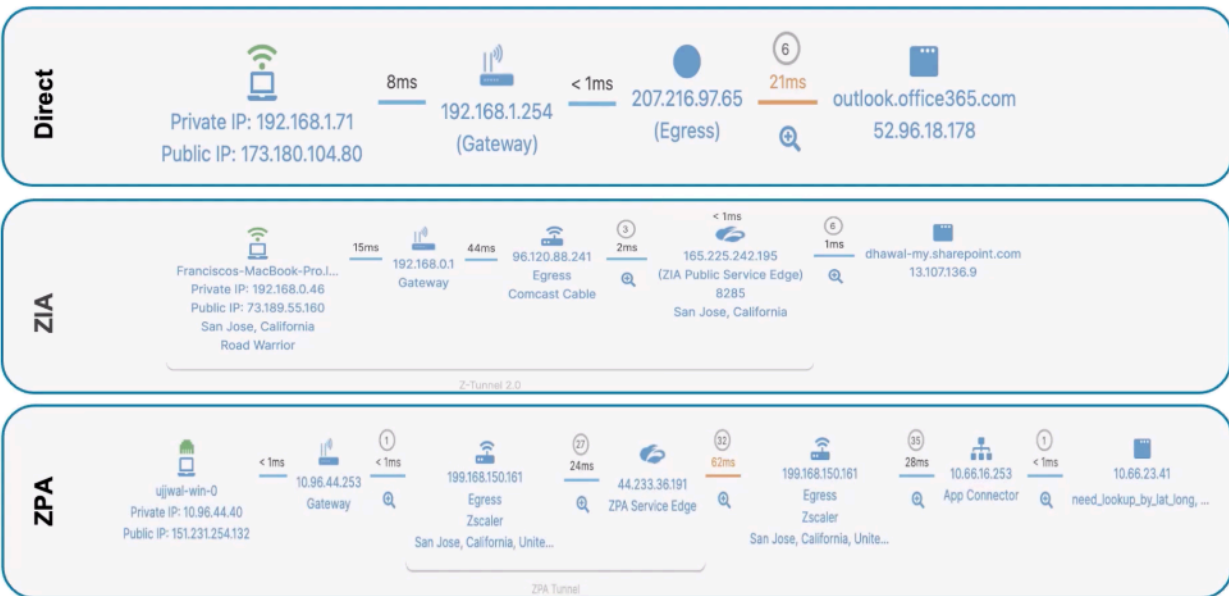
Packet Count: 11

Interval (ms): 1000

Timeout (ms): 1000

Cloud Path Host: m365x167135.sharepoint.com

What is Cloud Path - Common Scenarios



ZDX provides several **common cloud path scenarios** based on different ways applications are accessed. In a scenario where an application is accessed **directly**—bypassing **Zscaler Internet Access (ZIA)** and **Zscaler Private Access (ZPA)**—ZDX displays details such as **the local gateway, the egress ISP, the user’s IP address, and the number of hops to the destination**. When an application is accessed via **ZIA**, the **ZIA Service Edge** appears in the network path, providing visibility into the user’s route through the Zscaler cloud. Similarly, for applications accessed via **ZPA**, the **ZPA Service Edge** is included, detailing **the user’s network route from the local gateway to the application via Zscaler’s App Connector**.

Traceroute-Like Command Line View

ZDX provides **both graphical and command-line views** of the **Cloud Path Probe**. The command-line representation is similar to a **traceroute (tracert) command**, displaying **all network hops along the route** to an application. This output includes **IP addresses, ISP names, Zscaler locations**, and details derived from the **MaxMind database**. It also provides key network performance metrics, including **BGP ASN information, packet loss, latency, and jitter**. The graphical view allows IT teams to visually analyze network performance, while the command-line view offers a more detailed breakdown of each hop.

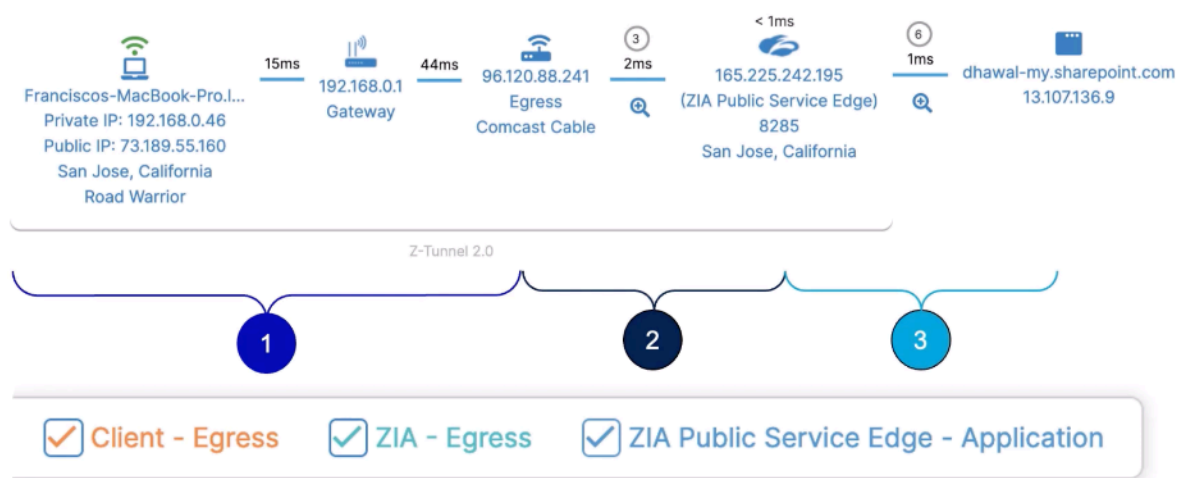
What is Cloud Path - Common Scenarios

IP Address	Hop Direction	Service Provider	Region	Geo	ASN	Assignee	Packet Loss	Packets Failed/	Differential	Average	Min.	Max.	StdDev
1 192.168.0.46	Client	-	San Jose, California	US	-	-	-	-	-	-	-	-	-
2 192.168.0.1	↓	-	-	-	-	-	0%	0/11	15	15	2	115	31.46
3 96.20.88.241	Egress	Comcast Cable	-	United States	7922	Comcast Cable	0%	0/11	44	59	43	75	7.58
4 141.36.105.130	↑	GTT Commu...	-	-	3257	GTT Communication...	0%	0/11	2	2	1	12	3.05
5 175.205.44.93	↑	GTT Commu...	-	-	3257	GTT Communication...	0%	0/11	0	0	0	2	0.66
6 185.225.242.2	↓	Zscaler	-	-	22816	Zscaler	0%	0/11	0	0	0	0	0
7 185.225.242.195	↓	Zscaler	San Jose, California	United States	22816	Zscaler	-	-	-	-	-	-	-
8 185.225.242.3	↓	Zscaler	-	-	22816	Zscaler	0%	0/11	0	0	0	0	0
9 206.223.117.103	↓	-	-	-	-	-	27.27%	3/11	1	1	0	6	1.94
10 104.44.41.156	↓	Microsoft Corpo...	-	-	8075	Microsoft Azure	0%	0/11	0	1	1	6	1.49
11 104.44.238.238	↓	Microsoft Corpo...	-	-	8075	Microsoft Azure	0%	0/11	0	1	1	2	0.29
12 No Response	↓	-	-	-	-	-	100%	11/11	-	-	-	-	-
13 No Response	↓	-	-	-	-	-	100%	11/11	-	-	-	-	-
14 13.107.136.9	Application	Microsoft Corpo...	Redmond, Washington	United States	8068	Microsoft Azure	0%	0/11	0	1	1	1	0

ZDX further **segments cloud paths into network legs** for a more granular view. For applications accessed via **ZIA**, ZDX identifies three distinct network legs: **client to egress**, **ZIA to egress**, and **ZIA Public Service Edge to application**.

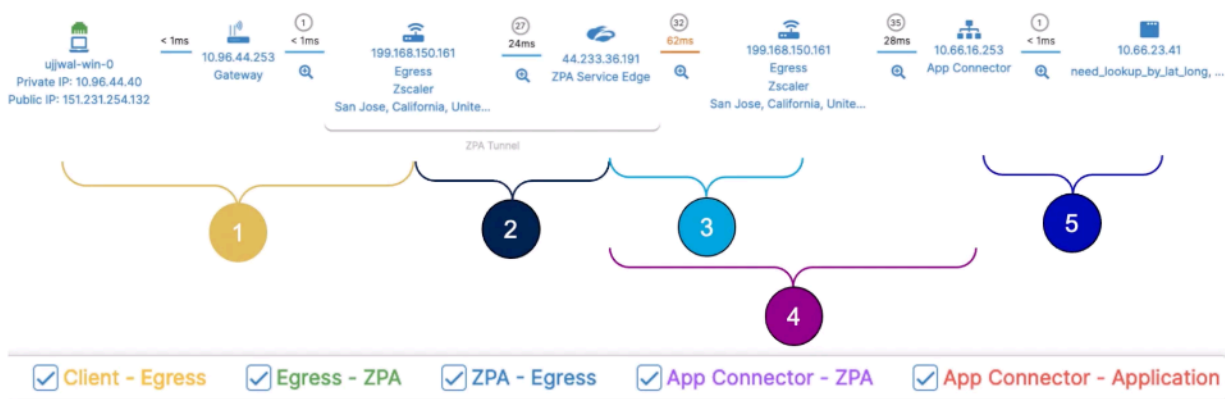
ZIA Leg Abstractions

Multiple Segments in the Path



Similarly, for applications accessed via **ZPA**, ZDX segments the path into **client to egress**, **egress to ZPA**, **ZPA to egress**, **App Connector to ZPA**, and **App Connector to the destination application**. This level of detail allows IT teams to precisely **troubleshoot connectivity and performance issues** across different access methods.

ZPA Leg Abstractions



By leveraging these architectural components, **ZDX ensures full visibility into application, network, and endpoint performance**, enabling organizations to **identify, diagnose, and resolve digital experience issues quickly and effectively**.

Key Concepts:

What are the key components of ZDX Architecture?	How does ZDX monitor applications?	What types of applications can be monitored by ZDX?
The core components of ZDX include the destination applications being monitored, endpoints with ZDX enabled , the Telemetry and Policy Gateway (TPG) for data transmission, and the ZDX Analytics Engine for processing and analyzing performance metrics.	ZDX continuously monitors applications by sending probes every five minutes by default, gathering performance data, and processing it through the Telemetry and Policy Gateway (TPG) and ZDX Analytics Engine for analysis.	ZDX can monitor predefined applications , such as SharePoint Online, with automatic probe creation, while custom applications require the manual creation of at least one web probe for monitoring.

Let's take a moment to summarize what we have learned in this section.

- **ZDX Architecture Overview:** ZDX consists of three main components: destination applications monitored under ZDX (e.g., Box.com or Office.com), endpoints with ZDX enabled, and the ZDX infrastructure, including the Telemetry and Policy Gateway (TPG) and the ZDX Analytics Engine.
- **Application Monitoring Types:** ZDX supports monitoring for two types of applications—**Predefined Applications**, which include built-in templates for common SaaS applications, and **Custom Applications**, which require manual probe configuration.
- **Probing Components:** Application monitoring in ZDX relies on two key components: **Web Probes**, which collect page fetch time and server response metrics, and **Cloud Path Probes**, which analyze network hops, packet loss, and latency.
- **Cloud Path Scenarios and Analysis:** ZDX provides both graphical and command-line visualizations of cloud paths for applications, whether accessed **directly**, through **Zscaler Internet Access (ZIA)**, or via **Zscaler Private Access (ZPA)**, enabling detailed network performance analysis.

ZDX Features and Functionality

ZDX Features and Functionality

ZDX provides a comprehensive set of features designed to enhance digital experience monitoring. Its capabilities enable **early detection of user experience degradation**, **rapid resolution of performance issues**, and **optimized application performance** while offering **deep network visibility** and **detailed device insights**.

In this section, we will explore five key features that make ZDX a powerful solution:

- **Visibility into SaaS & Private Applications** – Gain insights into the performance of both cloud-based and private applications to ensure seamless user experience.
- **UCaaS Monitoring** – Monitor unified communications platforms such as Zoom and Microsoft Teams to proactively detect and address performance issues.
- **Software & Device Inventory** – Maintain a detailed inventory of software and devices, helping IT teams track usage, identify potential issues, and ensure compliance.
- **Automated Root Cause Analysis (Y-Engine)** – Leverage AI-powered analysis to quickly pinpoint the root cause of digital experience problems, minimizing troubleshooting time.
- **ZDX APIs** – Integrate ZDX with existing IT and security tools, allowing for streamlined workflows and extended monitoring capabilities.

Visibility into SaaS & Private Applications

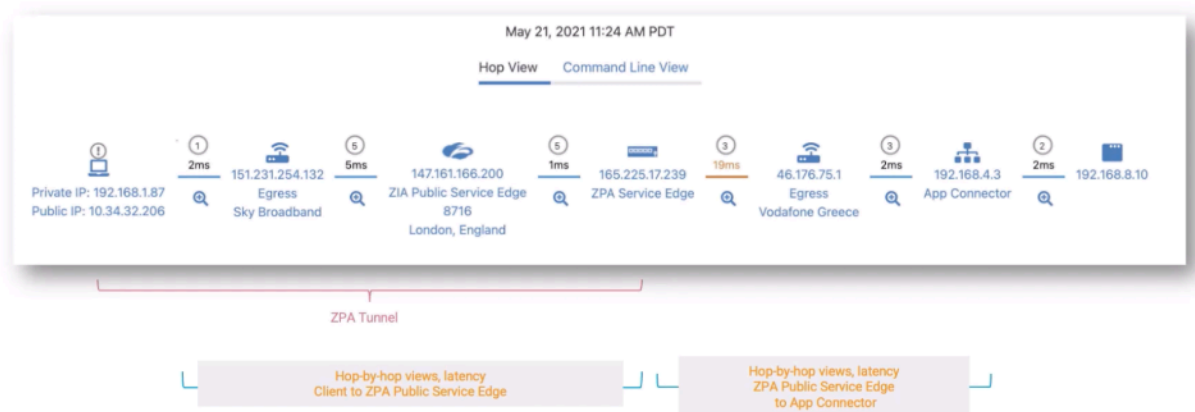
Zscaler Digital Experience (ZDX) delivers comprehensive visibility into an organization's **Zero Trust environments, private applications, and SaaS applications.**

Many traditional monitoring tools struggle in a **Zero Trust environment** due to the way these architectures are designed. The **Zero Trust Exchange** does not allow unauthorized inbound connections, including active monitoring probes. As a result, conventional monitoring solutions often fail to collect meaningful data. However, **ZDX overcomes this challenge** by leveraging Zscaler's infrastructure, allowing it to **monitor traffic across all hops and network paths**, providing unmatched visibility into the environment.

Once ZDX is deployed, it provides a **clear view of the entire application path**, whether the traffic is routed through **ZIA (Zscaler Internet Access), ZPA (Zscaler Private Access), or directly over the internet**. Regardless of the route taken, ZDX captures insights at every network hop, tracking **key performance metrics and user experience indicators**.

For example, in the diagram below, we see the full path of an application request as it **traverses through ZIA, reaches the ZPA Service Edge, continues to the App Connector, and finally connects to the destination application**. This level of **deep visibility** empowers IT teams to **quickly diagnose user experience issues, troubleshoot network problems, and accelerate resolutions**, ensuring seamless application performance.

Network Path Insights for Zero Trust Environments (ZPA)

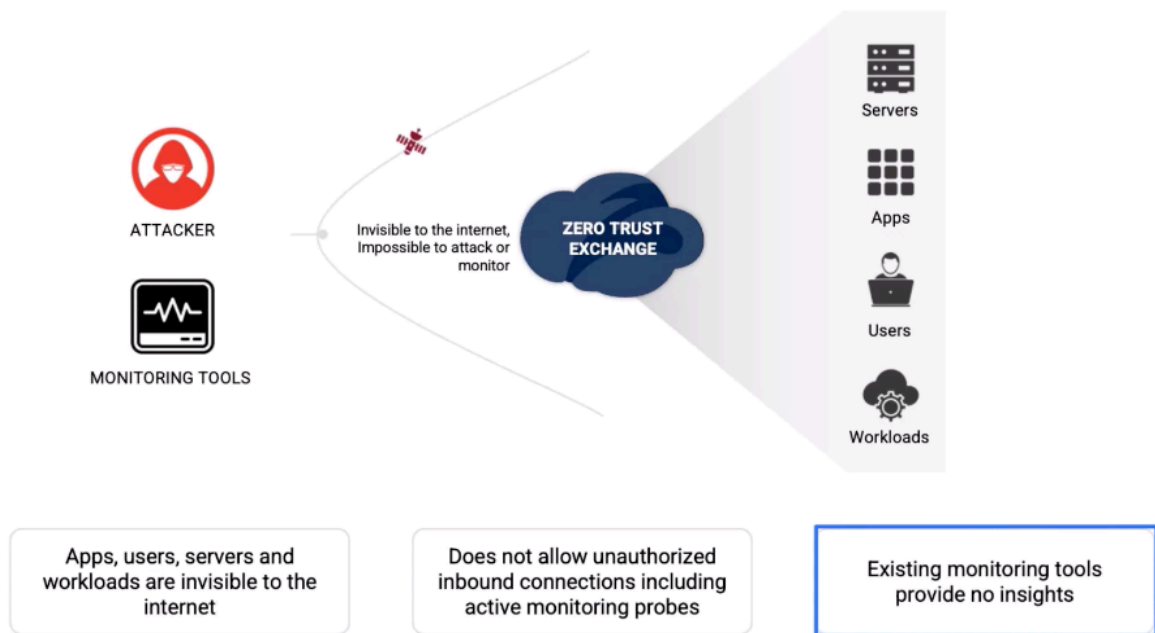


IT teams can identify and resolve network issues faster for ZPA secured apps

Key Concepts:

Why do monitoring tools fail in Zero Trust environments?	How does ZDX achieve visibility in Zero Trust?	What are the IT benefits of ZDX's visibility?
They fail because Zero Trust prevents unauthorized inbound connections, limiting the effectiveness of traditional monitoring tools.	ZDX provides end-to-end visibility across all hops and paths, leveraging its unique infrastructure unlike other monitoring tools.	It enables IT teams to quickly resolve issues by offering comprehensive visibility into network performance and user experience.

Lack of Network Path Insights into Zero Trust Environments



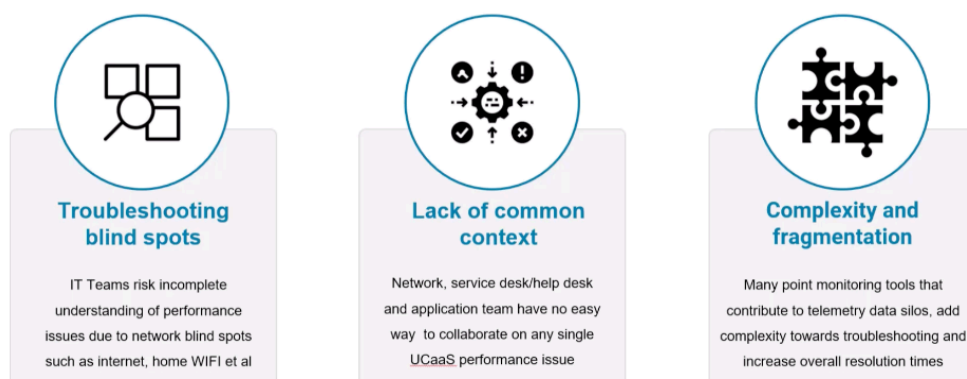
UCaaS Monitoring

ZDX enhances online meetings by consolidating all relevant performance metrics into a single platform, making it easier to identify and resolve issues such as poor audio quality, lagging video, or asymmetric audio problems.

Traditionally, troubleshooting these issues involved using multiple tools and manual investigations. With ZDX, IT teams gain real-time visibility into unified communications applications like Microsoft Teams and Zoom, streamlining the troubleshooting process.

Problems we Address

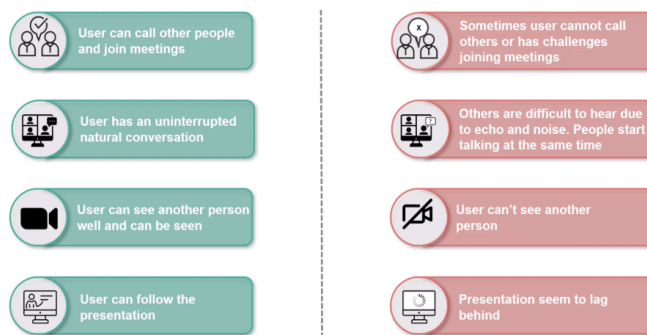
Lack of complete picture to troubleshoot Microsoft Teams and Zoom issues



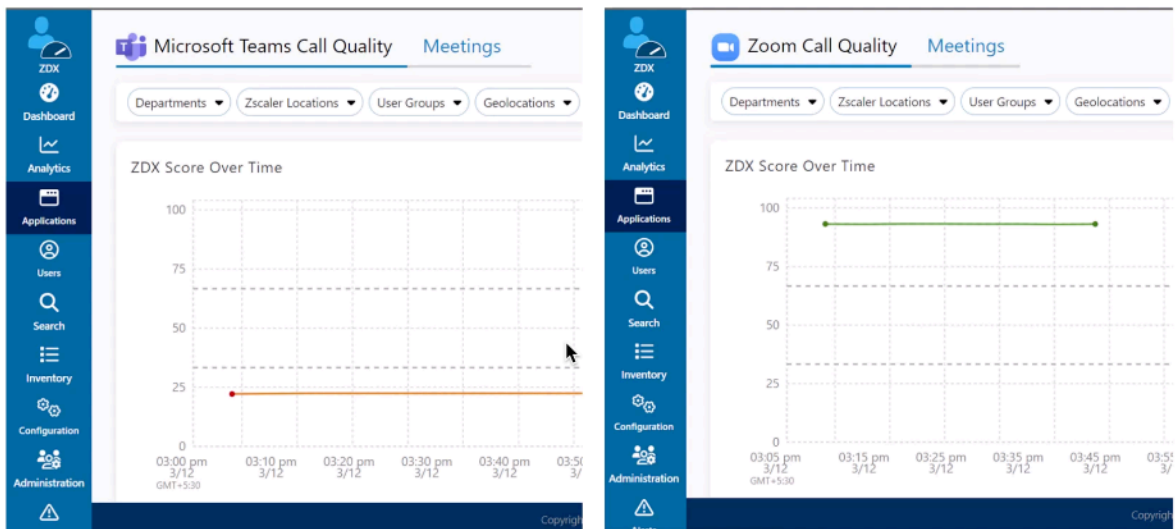
Key aspects of UCaaS Monitoring include:

- **Simplified Troubleshooting** – Instead of using multiple tools to diagnose meeting issues, ZDX consolidates network, application, and device context into a single view.
- **Common Meeting Challenges** – Users often face problems such as poor audio quality, video lag, or one-way audio where one person can hear the other but not vice versa.
- **Manual Troubleshooting Limitations** – The traditional service desk workflow involves collecting OS details, network logs, and sometimes even packet captures, yet still fails to pinpoint the root cause of the issue.
- **API Integration for Enhanced Insights** – ZDX integrates directly with Teams and Zoom APIs to collect and overlay audio, video, screen-sharing, and MOS scores within the user's timeline, providing deeper insight into meeting quality.
- **Organization-Level Call Quality Monitoring** – ZDX provides visibility into call quality trends across the organization, allowing IT teams to drill down into specific meetings, affected users, and contributing factors impacting call performance.

Good vs Bad Meeting Experience



Visibility into Microsoft Teams and Zoom Call Quality



Key Concepts:

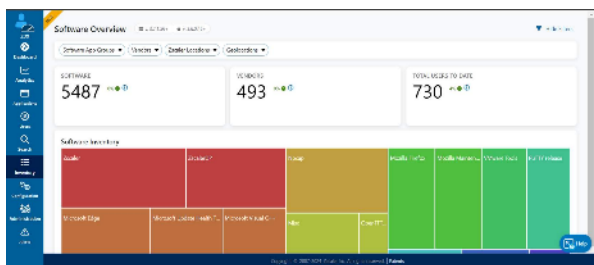
What common issues do users face during meetings?	How does traditional troubleshooting approach these issues?	How does ZDX improve the troubleshooting process?
Users may encounter issues such as poor audio quality, video lag, or one-way audio disruptions during meetings.	Service desks gather detailed information and escalate issues to admins, but pinpointing the exact problem remains challenging, leading to a complex troubleshooting process.	ZDX streamlines troubleshooting by integrating application-level telemetry and providing a unified view of call quality, network performance, and device context, delivering high-fidelity alerts.

Software & Device Inventory

A user's device and its software versions play a crucial role in overall user experience. Ensuring that devices within an organization are running the latest OS, patches, and software versions is essential for optimal performance and security. To address this, ZDX provides **Software and Device Inventory**, offering visibility into device configurations and software versions across the organization.

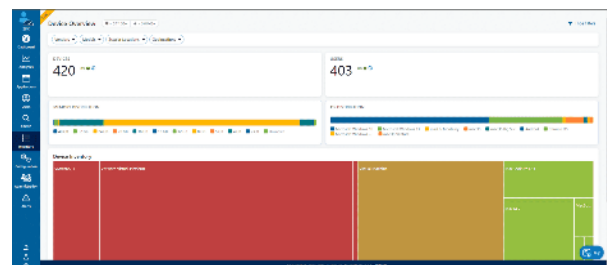
SOFTWARE INVENTORY

Software Inventory allows you to view current and historical information about software versions and updates on your users' devices.

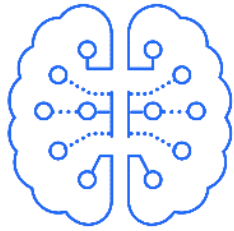


DEVICE INVENTORY

Device Inventory allows you to view current information about your organization's devices and their associated users.



Automated Root Cause Analysis & API Integration

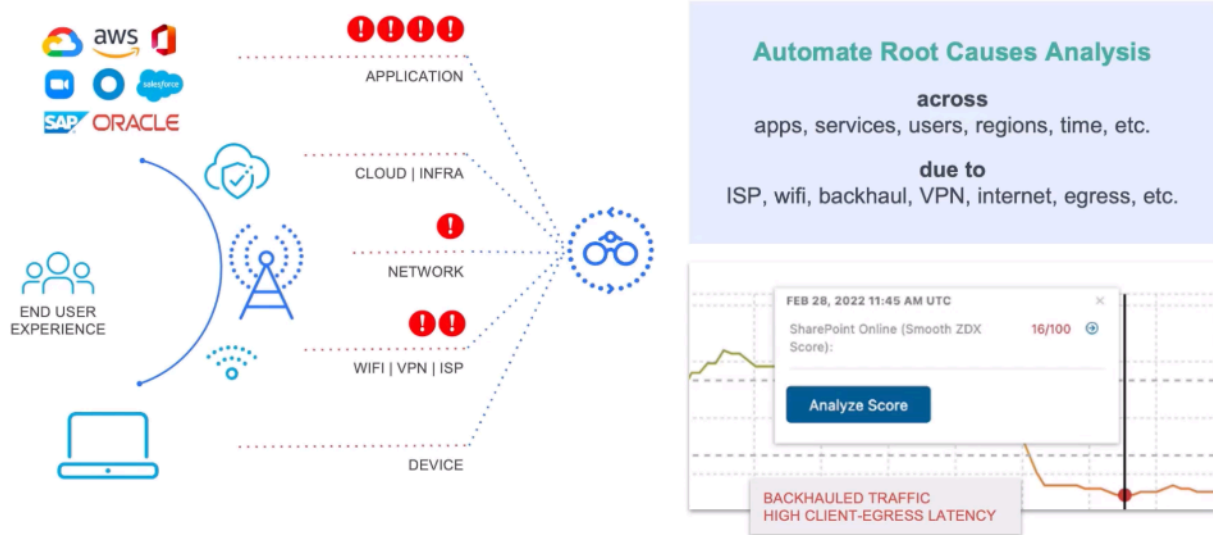


Now, let's explore these final two features, which span across all aspects of the ZDX solution: **Y-Engine** and **APIs**.

ZDX's Y-Engine (Automated Root Cause Analysis) enables organizations to automatically isolate the root causes of performance issues, reducing troubleshooting time, eliminating finger-pointing, and helping users get back to work faster.

Troubleshooting performance issues is often a complex and time-consuming process, requiring expertise across multiple areas such as device health, network metrics, and packet flow analysis. In many cases, identifying the root cause can take days or even weeks. **Y-Engine leverages AI and machine learning** to automate this process by analyzing multiple data points and identifying potential causes of performance degradation.

ZDX Y-Engine Automates Root Cause Analysis



With **Y-Engine**, users can select a poor ZDX score and click the **Analyze Score** button. The system then examines not only the current data but also **historical context**, identifying what happened before and after the issue occurred. This helps IT teams quickly pinpoint the root cause, significantly accelerating issue resolution. This feature is particularly valuable for **Tier 1 and Tier 2 service desk operators**, enabling them to troubleshoot end-user issues more efficiently without requiring deep technical expertise.

ZDX's APIs integrate digital experience insights with popular ITSM tools like ServiceNow, providing additional context and triggering automated remediation workflows.

Key Concepts:

What does the Y-Engine in ZDX aim to automate?	How does Y-Engine facilitate troubleshooting for service desk operators?	What possibilities does ZDX API integration offer?
The Y-Engine leverages machine learning to automate root cause analysis by examining multiple data points, rapidly identifying the factors impacting the ZDX score, and accelerating issue resolution.	By analyzing poor ZDX scores and surrounding data, Y-Engine delivers instant root cause analysis, empowering Tier 1 and Tier 2 service desk operators to troubleshoot and resolve issues more efficiently.	ZDX API enables data extraction into external platforms like Splunk and seamless integration with third-party services like ServiceNow, enhancing troubleshooting sessions and providing valuable data-driven insights.

Summary of Key Learnings

- **Visibility into SaaS & Private Applications:** ZDX provides comprehensive monitoring within Zero Trust environments, offering visibility into network performance and user experience. This helps IT teams quickly identify and resolve issues.
- **UCaaS Monitoring:** By integrating application-level telemetry, ZDX simplifies troubleshooting for meeting-related issues. It provides in-depth insights into factors affecting call quality on platforms like Microsoft Teams and Zoom, helping IT teams diagnose and address performance issues efficiently.
- **Software & Device Inventory:** ZDX improves user experience management by offering detailed insights into software versions, updates, and device configurations across the organization. This feature enables IT teams to track historical and current software usage to maintain system performance and security.
- **Y-Engine & ZDX APIs:** ZDX's Y-Engine leverages machine learning to automate root cause analysis, allowing IT teams to diagnose performance issues faster. Additionally, ZDX APIs facilitate seamless integration with external platforms like ServiceNow and Splunk, enhancing data analysis and streamlining troubleshooting workflows.

ZDX Use Cases

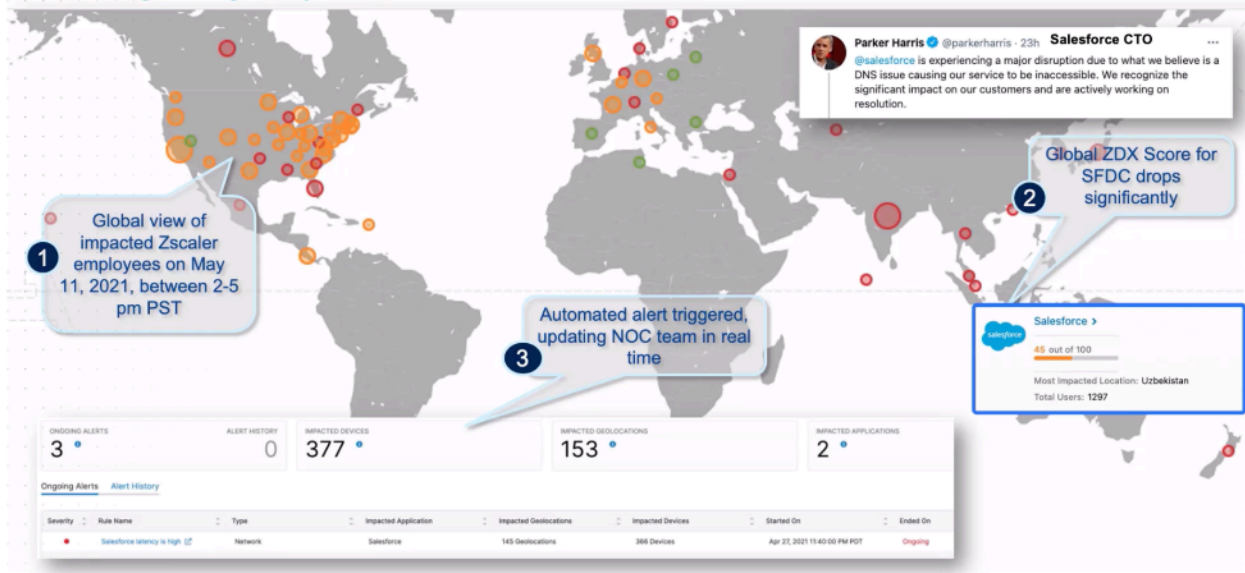
Zscaler ZDX provides powerful end-user monitoring capabilities to address a wide range of performance and troubleshooting challenges. Below are six common use cases where ZDX enhances visibility and improves digital experiences:

- **Real-time Detection of SaaS Outages:** Instantly identify and respond to SaaS application outages, minimizing downtime and user disruptions.
- **Baselining Performance Between Office and Remote Work:** Compare performance metrics across office and remote environments to ensure a seamless user experience.
- **Detecting Employee Home Wi-Fi Issues:** Pinpoint home network issues affecting performance, helping IT teams proactively address connectivity problems.
- **Detecting High CPU Causing Application Degradation:** Identify when high CPU usage on user devices is impacting application performance and take corrective action.
- **Visibility into Private Applications via ZPA:** Gain insights into private application performance and user connectivity issues within the Zscaler Private Access (ZPA) environment.
- **Call Quality Monitoring for Microsoft Teams and Zoom:** Monitor and analyze UCaaS call quality, providing IT teams with the data needed to resolve audio and video issues quickly.

Now, let's explore these key ZDX use cases in more detail.

Use Case #1: Real-time Detection of SaaS outages

Salesforce global outage on May 11, 2021



This is the ZDX map view captured by Zscaler's NOC team just minutes after the Salesforce outage occurred. Each red dot represents a location where Zscaler employees are situated, with their precise locations determined using operating system data, latitude, and longitude. The color coding reflects baseline performance, highlighting significant application issues in real time. At the top of the image, a tweet from Salesforce's CTO confirms the ongoing issues, while in the bottom right, an alert generated by ZDX was automatically forwarded to Slack. This proactive notification ensured that the ZDX NOC team was informed of the outage before anyone else.

Use Case #2: Baselining Performance Between Office and Working from Anywhere



In this use case, we analyze a user experiencing access issues while working from home, which disappear when they are in the office. Using ZDX, we can retrospectively examine network performance during the user's remote work sessions. In this case, the data reveals high latency when connecting to the ISP, indicating that the issue likely originates from the user's home network.

Use Case #3: Detecting Employee Home WIFI Issues

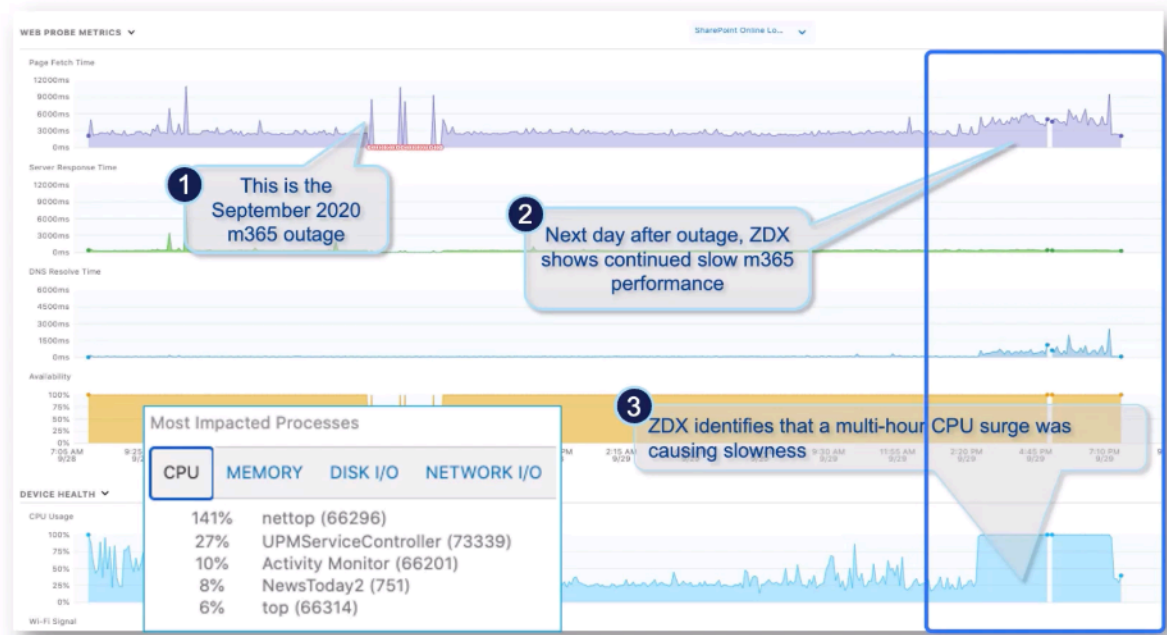
Weak WIFI Signal



The third use case focuses on a common challenge for remote employees—Wi-Fi signal degradation affecting their user experience. Since most employees rely on Wi-Fi networks, any drop in signal strength can lead to performance issues. In this example, ZDX detects that a user is experiencing high page load times, which directly correlates with a weak Wi-Fi signal. By analyzing this data, IT teams can quickly diagnose the issue and suggest solutions, such as switching to a 5 GHz network or moving closer to the access point to improve connectivity.

Use Case #4: Detecting High CPU Causing Application Degradation

End User Device Performance Issues



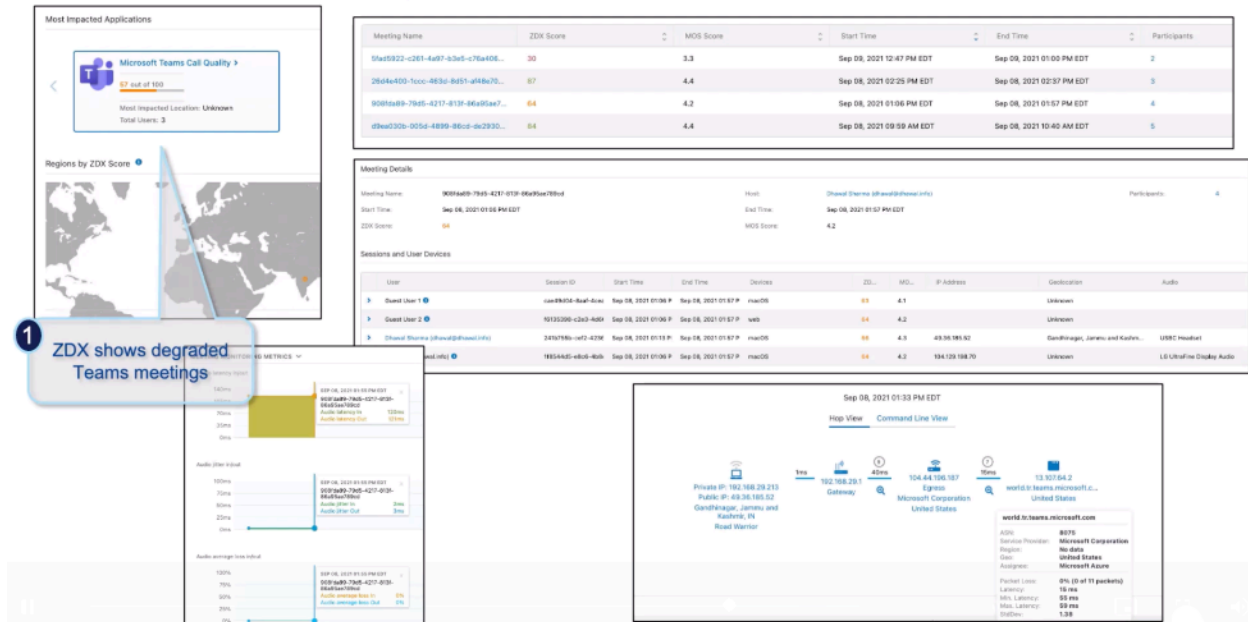
In the fourth use case, a user is experiencing application slowness, and by analyzing ZDX data, we quickly identify that the likely cause is high CPU utilization on the user's device. The data shows that the CPU is consistently running at 100%, which directly impacts page load times and overall system performance. This insight allows IT teams to diagnose the issue efficiently and recommend solutions, such as closing resource-intensive applications or optimizing system performance, to enhance the user experience.

Use Case #5: Visibility into Private Applications via ZPA

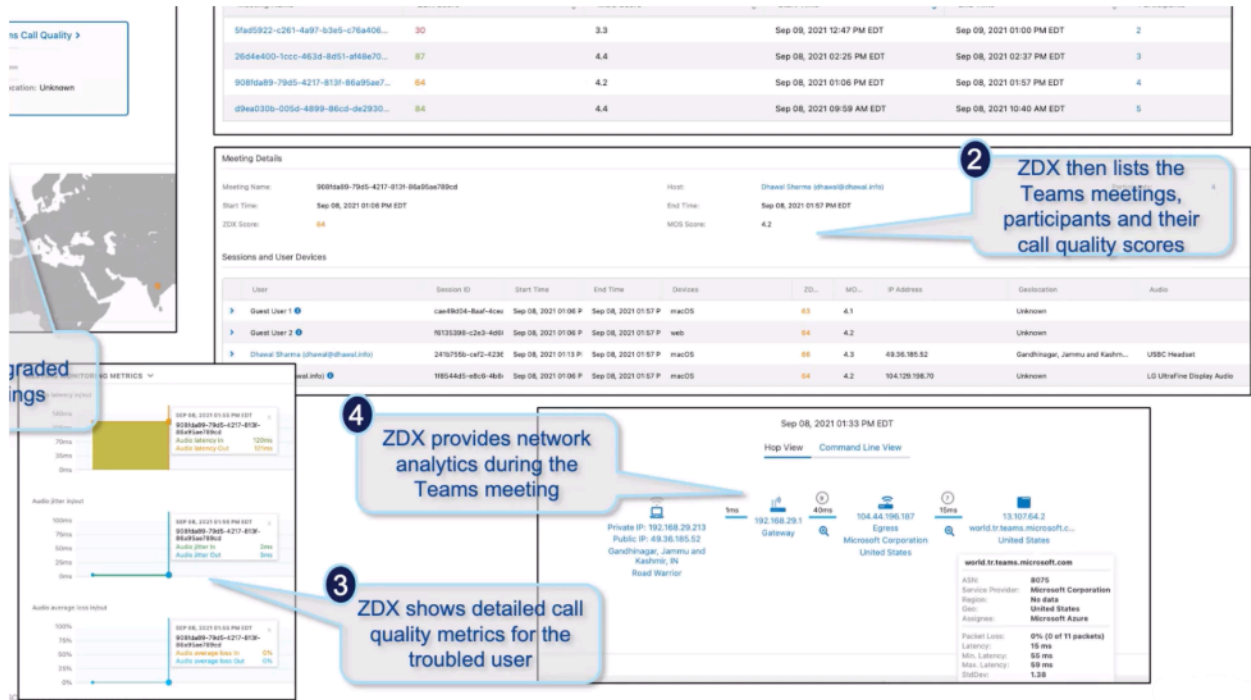


With ZDX, as previously discussed, we can provide visibility into a Zero Trust environment. In this scenario, a user is experiencing slowness while accessing an application through ZPA. By analyzing ZDX data, we quickly identify that the issue is likely caused by latency within the destination network where the application is hosted. This suggests that the problem is not with the user's connection but rather a local network issue within the customer's environment, allowing IT teams to focus their troubleshooting efforts in the right area.

Use Case #6: Call Quality Monitoring for Microsoft Teams and Zoom



Another key use case of ZDX is its ability to diagnose issues in Microsoft Teams or Zoom call quality. In this example, we observe a degradation in the ZDX score for Teams Call Quality, though the same workflow applies to Zoom as well. By drilling down into the data, we can review meetings over a specific period and identify those with poor call quality, highlighted in red.



From there, we can select a specific meeting to analyze the participants, their external IP addresses, their connection locations, and the type of audio devices they used. Further investigation allows us to focus on a user experiencing audio issues and determine the exact nature of the problem—whether it's choppy audio, increased video latency, or poor screen-sharing quality. Additionally, ZDX provides visibility into the network path, helping IT teams quickly pinpoint any latency or connectivity issues affecting the meeting experience.

Key Concepts:

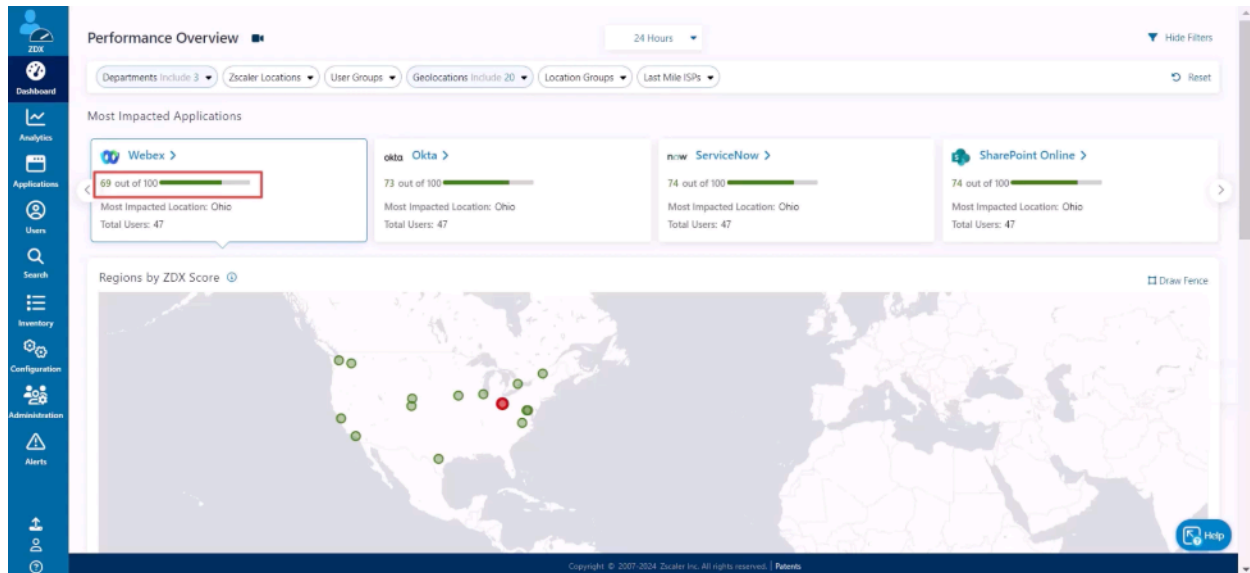
How does ZDX address user access issues from home?	How does ZDX help with WiFi related user experience issues?	How does ZDX address call quality issues in Teams or Zoom?
ZDX enables retrospective analysis, allowing IT teams to identify root causes of access issues from home, such as latency to the ISP.	ZDX can detect degraded Wi-Fi signal strength leading to high page load times and provide remediation suggestions, such as upgrading to a 5 GHz network or moving closer to the access point.	ZDX enables in-depth analysis of call quality scores, identifying meetings with poor performance and providing insights into participant details, network paths, and specific issues such as choppy audio or video latency.

Summary of Key Learnings

- **Real-time Detection of SaaS Outages:** ZDX provides early detection of SaaS outages, reducing pressure on IT teams by proactively identifying and addressing performance issues before they escalate into widespread user complaints.
- **Baselining Performance Between Office and Remote Work:** ZDX helps differentiate performance between office and remote environments, identifying ISP-related latency issues that impact users working from home.
- **Detecting Employee Home Wi-Fi Issues:** ZDX diagnoses Wi-Fi signal strength issues affecting remote employees and provides actionable recommendations, such as upgrading to a 5 GHz network or relocating closer to the access point.
- **Detecting High CPU Causing Application Degradation:** ZDX pinpoints high CPU utilization on user devices, identifying it as a root cause of slow application performance and degraded user experience.
- **Visibility into Private Applications via ZPA:** ZDX enhances troubleshooting within a Zero Trust environment by providing visibility into latency issues affecting access to private applications hosted in customer networks.
- **Call Quality Monitoring for Microsoft Teams and Zoom:** ZDX enables real-time monitoring and analysis of call quality issues in platforms like Microsoft Teams and Zoom, allowing IT teams to drill down into specific meetings, diagnose root causes, and optimize performance.

ZDX Dashboard Overview

The **ZDX Dashboard** provides a comprehensive view of application performance and user experience, enabling quick detection and troubleshooting of performance issues. It includes several key widgets and graphs designed to highlight problem areas, such as **Most Impacted Applications**, **Regions by ZDX Score Map**, **ZDX Score Graph**, and **Page Fetch Time Graph**.



Performance Overview and Filtering Options

The **Performance Overview** page of the ZDX Dashboard offers a **high-level snapshot** of how applications are performing across your organization. At the top of the dashboard, several **filters** allow IT teams to focus on specific issues reported by users.

- The **Time Range Filter** allows performance data to be viewed over a period ranging from **2 to 48 hours** for the advanced ZDX plan and **2 to 24 hours** for the standard plan. A **custom time frame** can also be set, including an option to analyze the previous **30 minutes** of ZDX score data.
- Additional **filters** include **departments, Zscaler locations, user groups, location groups, last mile ISPs, and geolocations**, which represent organizational structures and office locations as configured in the ZIA tenant.
- **Active Geolocations** display the actual cities where users are located, using longitude and latitude data from their devices.

Key Dashboard Metrics

Each monitored application displays critical performance insights, helping IT teams pinpoint and resolve digital experience issues efficiently.

- **ZDX Score:** Represents the overall **digital experience** of all users for an application, based on a **scale from 1 to 100** over the selected time period.
- **Most Impacted Location:** Identifies the location experiencing the **worst digital experience** for that application, allowing IT teams to focus on problem areas.
- **Number of Users:** Displays the **total number of users** interacting with each application during the selected time frame, providing insights into the **scale of the issue**.

Since the **Zscaler Client Connector** uses **synthetic probes**, data collection happens **continuously** as long as user devices are active, eliminating the need for **manual user interaction** to gather insights.

Visualizing Performance Issues

The **Regions by ZDX Score** widget provides a **map-based visualization** of user locations for a selected application. This feature allows IT teams, such as **tech support**, to **quickly identify regional outages** by zooming in on affected areas before users begin submitting support tickets.

- The **ZDX Score Graph** displays how the **ZDX score fluctuates** over the selected time period, helping IT teams **track performance trends**.
- The **Page Fetch Time (PFT) Graph** measures how long it takes for the selected application to **transfer a web page to users**. **Page Fetch Time (PFT)** is one of the **most critical metrics** in assessing digital experience, as a high PFT can lead to **poor user experience**, even when other performance indicators appear normal.

Summary of Key Learnings

- **Time Range Filter:** Allows users to select a performance window between **2 to 48 hours** (Advanced ZDX) or **2 to 24 hours** (Standard ZDX), with an option to **analyze the last 30 minutes**.
- **Filtering Options:** Enables filtering by **departments, locations, user groups, ISPs, and geolocations**, providing granular insights into digital experience.
- **ZDX Score:** Assigns a **performance score from 1 to 100** for each application, reflecting overall user experience.
- **Most Impacted Location:** Identifies the **worst-performing location** for an application, helping prioritize troubleshooting efforts.
- **Number of Users:** Displays **how many users** are using an application during the selected period, helping assess the **scale of potential issues**.

By leveraging these insights, IT teams can **proactively identify, troubleshoot, and resolve performance issues** efficiently, ensuring an optimal user experience across the organization.

Zscaler Zero Trust Automation

Introduction to APIs

An **API (Application Programming Interface)** is a structured set of rules and protocols that enable different software applications to communicate and exchange data seamlessly. APIs consist of multiple **endpoints**, which serve as designated interaction points between systems, each providing access to specific sets of data and functionalities. These endpoints allow applications to request and retrieve information, automate workflows, and integrate with other platforms efficiently.

RESTful API

A **RESTful API** is a web service that facilitates communication between software systems over the internet using standard **HTTP methods** such as **GET, POST, PUT, and DELETE**. It operates in a **stateless** manner, meaning each request is independent and contains all the necessary information for processing. RESTful APIs identify and interact with resources through **unique URLs**, ensuring a consistent and scalable approach to web-based integrations.

How APIs Work

APIs facilitate the exchange of data between applications, systems, and devices through a **request and response** cycle. A request is sent to the API, which then retrieves the necessary data and returns a response. In some cases, API requests can also be triggered by external events, such as notifications from other applications.

API Client

The API client initiates a request to access specific data or perform an action. This request is sent to an API server, which processes it and responds with the requested data or confirmation of the action taken.

API Request Components

The structure and behavior of an API request depend on the type of API being used. However, most API requests typically include the following components:

- **Endpoint:** An API endpoint is a specific URL that provides access to a particular resource. For example, in a blogging application, the `/articles` endpoint would handle requests related to retrieving, creating, or updating articles.

- **Method:** The HTTP method determines the type of action the API should perform on a given resource. RESTful APIs typically use standard **HTTP methods** such as **GET (retrieve data)**, **POST (create data)**, **PUT (update data)**, and **DELETE (remove data)**.
- **Parameters:** Parameters provide additional instructions to the API for processing the request. They can be included in the request **URL, query string, or request body**. For instance, in a blogging API, the /articles endpoint might accept a “**topic**” parameter to return articles related to a specific subject.

Zscaler APIs

Zscaler APIs provide **programmatic access and control** over various Zscaler services, enabling seamless automation, configuration, and monitoring across different environments. These APIs enhance security, streamline management, and integrate with third-party services for improved operational efficiency.

Zscaler Internet Access (ZIA) API

The **ZIA API** enables programmatic access to configure and control the **Zero Trust Exchange**, providing secure access to **cloud service APIs**, **Sandbox Submission APIs**, and **Third-Party App Governance APIs** through different authentication schemes. This allows organizations to automate security policies, manage cloud access, and enhance threat protection.

Zscaler Digital Experience (ZDX) API

The **ZDX API** provides insights into application health, access metrics, and digital experience monitoring. It enables integration with **ServiceNow for help desk ticketing**, monitoring **Zoom call quality**, and analyzing endpoint performance to diagnose issues affecting user experience.

Zscaler Private Access (ZPA) API

The **ZPA API** allows developers and administrators to automate the management of **Zscaler Private Access (ZPA)** features, facilitating **secure remote access** to private applications while ensuring efficient deployment and policy enforcement.

Zscaler Cloud & Branch Connector API

The **Cloud & Branch Connector API** enables the automation and management of Zscaler **Cloud Connector and Branch Connector** features. This API allows organizations to streamline **network security policies**, manage **cloud traffic routing**, and **integrate with third-party services** for enhanced operational control.

Zscaler OneAPI

Zscaler OneAPI delivers **programmatic access** to various Zscaler services while ensuring **consistency in API design, reliability, and high performance** across all products. It provides a **unified and centralized** approach to managing key API components, including authentication, tenant access policies, rate limiting, caching, and API lifecycle management.

By standardizing API interactions across Zscaler's ecosystem, OneAPI simplifies **automation and integration** with external services, enabling seamless interoperability. This streamlined framework ensures a **uniform cross-product API experience**, reducing complexity and enhancing operational efficiency for security teams and developers.

Before OneAPI : Zscaler Automation Framework

Before the introduction of **Zscaler OneAPI**, API clients faced significant challenges when interacting with multiple Zscaler products. Each product had its own **registration, authorization, token request, and token grant** process, requiring users to repeatedly go through complex authentication steps when switching between services.

For automation workflows, this created additional **operational inefficiencies** as users had to manage and remember multiple endpoints, increasing the risk of errors and making integration cumbersome.

The introduction of **OneAPI** addresses these challenges by **unifying API interactions into a single, consistent framework**, simplifying authentication, reducing complexity, and providing a more **streamlined and efficient user experience**.

Zscaler Zero Trust Automation

Zscaler **Zero Trust Automation** is designed to help enterprises and partners rapidly and efficiently adopt a **Zero Trust Architecture** by automating security processes, enhancing control, and reducing manual efforts.

Key Benefits:

- **Enhanced Security Posture** – Zero Trust Automation enforces strict access controls and continuous verification, significantly improving an organization's security resilience.
- **Operational Efficiency** – Automation streamlines security processes, reducing complexity and eliminating the need for time-consuming manual configurations.
- **Maximized ROI** – By automating routine security tasks, organizations can lower operational costs and redirect resources toward more strategic security initiatives.
- **Reduced Human Error** – Automated workflows minimize the risk of misconfigurations and security breaches caused by manual errors.
- **Faster Threat Detection and Response** – Automated systems can detect, analyze, and respond to threats in real time, reducing the impact of security incidents.
- **Comprehensive Visibility and Control** – Leveraging **Zscaler OneAPI**, organizations gain centralized visibility and control across their security environment, ensuring continuous monitoring and proactive risk management.

By automating security tasks, **Zscaler Zero Trust Automation** enables organizations to **accelerate Zero Trust adoption**, improve efficiency, and strengthen their cybersecurity posture.