

Zscaler Zero Trust SD-WAN

Securely connect branches, factories, and data centers without routed overlays or lateral threat movement.

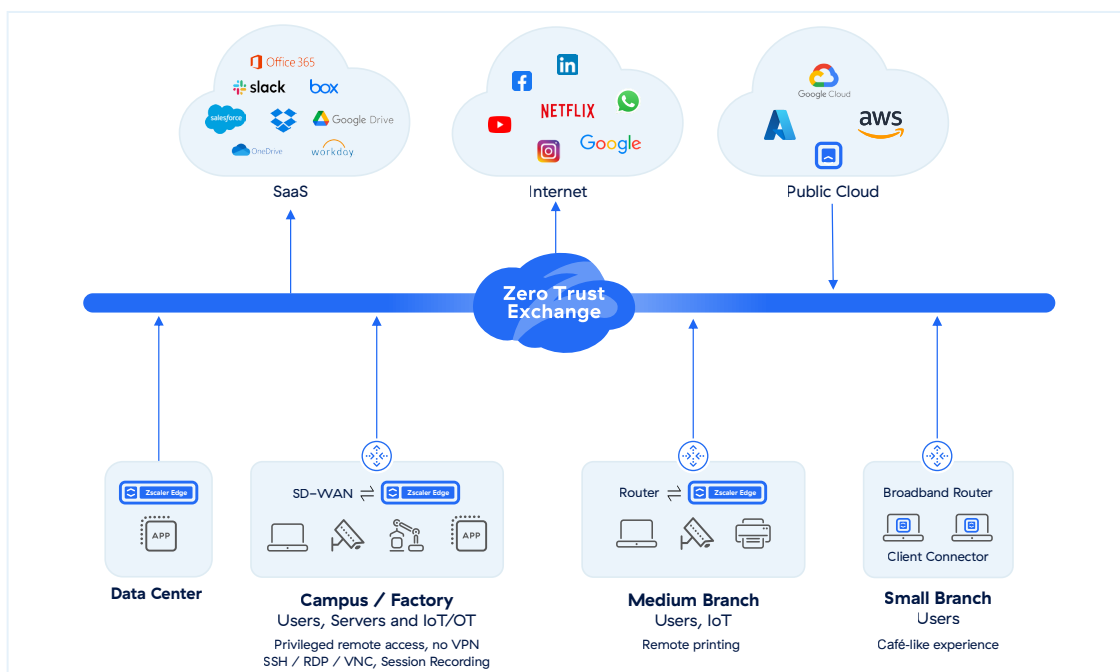
Traditional SD-WANs extend your network into remote branches and the cloud. This expands your attack surface, enables lateral threat movement and facilitates ransomware attacks.

Securing traditional networks requires a complex patchwork of firewalls, proxies, NAC gateways and endpoint agents, leading to runaway increases in cost and complexity. In the end you are still left vulnerable as ransomware attacks continue to increase in scope and frequency.

Zscaler Zero Trust SD-WAN offers a simpler, safer and more cost-effective means for users, devices and workloads to communicate, without the complexity and security challenges of routed overlay networks.

Zscaler Zero Trust SD-WAN:

- Enables cafe-like branches, without extending your network everywhere
- Reduces ransomware risk by eliminating lateral threat movement
- Shrinks the attack surface by eliminating exposed VPN ports and firewalls
- Slashes infrastructure costs by radically simplifying your network architecture
- Improves application performance by eliminating traffic backhaul to data centers
- Ensures cyberthreat and data protection by inspecting all traffic



Traditional SD-WANs Facilitate Ransomware Attacks

Organizations face several challenges when using legacy network and security architectures to connect a branch to the internet or to their other applications in a public cloud or data center environment.

- **Expanded attack surface:** Extending the network to remote branch sites offers more opportunities for attackers to infiltrate your organization. Every firewall or VPN gateway is an entry point, and zero-day vulnerabilities continue to plague the industry.
- **Lateral threat movement:** An infected user or IoT device in a branch office is able to scan the network and move laterally to other sites, data centers, and virtual private clouds. Recent ransomware attacks have taken as little as 45 minutes from initial intrusion to crippling outages, leaving no time for operations teams to react.
- **Cost and complexity:** The patchwork of firewalls, proxies, NAC agents and IP-based policies designed to secure and segment SD-WANs adds tremendous operational complexity and cost, and impairs your organization's agility.
- **Poor performance and user experience:** Traffic backhaul to data centers and through multiple security inspection points often results in poor application performance and an inconsistent experience for users.

Zero Trust SD-WAN Eliminates Lateral Threat Movement

Zero Trust SD-WAN securely connects your branches, factories and data centers without the complexity of VPNs or overlay routing. It ensures zero trust access between users, IoT/OT devices and applications based on organizational policies. Combining the power of Zscaler's industry leading Zero Trust Exchange platform, with seamless connectivity for locations, clouds and users, organizations can embrace a secure access service edge (SASE) framework and enable a cafe-like branch experience.

- Zero Trust SD-WAN provides branches, campuses and factories with fast and reliable access to the internet, SaaS, and private applications with a direct-to-cloud architecture that provides high security and operational simplicity.
- It eliminates lateral threat movement and greatly reduces ransomware risk for your organization.
- It slashes infrastructure and operation costs by eliminating complex routing, VPNs, firewalls, while ensuring full cyberthreat and data protection.

How Zero Trust SD-WAN works

Zero Trust SD-WAN uses a physical or virtual appliance at the branch/campus/factory to manage ISP connections and forward traffic to the Zero Trust Exchange based on organizational policies. Branch traffic is securely forwarded over ephemeral DTLS connections to the Zero Trust Exchange where it can be inspected for cyberthreats and data loss with context-aware security policies.

The Zero Trust Exchange facilitates bi-directional communication between devices and internet apps or private apps running in other locations, data centers or the cloud.

For example, a print server in a data center can send print jobs to a printer in a remote branch through the Zero Trust Exchange, without the need for routed networks, VPNs or exposed ports. Trusted application traffic can be sent directly across the internet with direct internet breakout.

This unique approach provides three key advantages:

- **A more secure organization:** Ransomware cannot moving laterally between sites; infected devices cannot scan anything beyond their local networks
- **A simpler, less expensive branch:** No more routed overlays, firewalls or site-to-site VPNs
- **Improved user experience:** Applications run faster without traffic backhaul and multiple security choke points

Zero Trust SD-WAN Use Cases

- **VPN replacement:** Eliminate the complexity of site-to-site VPNs and routed overlays with a simpler, more secure zero trust solution
- **SD-WAN refresh:** Deliver cafe-like branches and reduce ransomware risk
- **M&A:** Integrate users and apps without the complexity and cost of integrating networks
- **Secure factories:** Eliminate lateral movement between factories and secure IT/OT environments

Branch Connector Hardware and Software Models





FEATURE	ZT 400	ZT 600	ZT 800	ZT VM
				
Type	Small– Medium branches	Small–Medium branch	Medium–Large branch	Branch and Data Center
Encrypted throughput	200 Mbps	500 Mbps	1 Gbps	Varies
Physical ports	4x RJ45 GbE	6x RJ45 GbE	6x RJ45 GbE, 2x SFP	N/A
Zero touch provisioning	✓	✓	✓	N/A
Gateway mode with app-aware path selection	✓	✓	✓	N/A
Granular forwarding policies	✓	✓	✓	✓
Cyber threat and data protection policies for internet traffic	✓	✓	✓	✓
Secure private access for IoT/OT devices	✓	✓	✓	✓

TABLE 1: ZSCALER ZERO TRUST SD-WAN CAPABILITIES

FEATURE	DETAILS
Capabilities	
Zero touch provisioning and automated deployment	<ul style="list-style-type: none"> • Zero touch provisioning with pre-defined templates • Fully automated deployment • Dynamic discovery of branch office geo-location
Granular forwarding policy for internet and private application traffic	<ul style="list-style-type: none"> • Options to send the traffic to ZIA, ZPA, or Direct (bypassing Zscaler services) • Flexible traffic selection criteria location, sublocation, location group, 5 tuple, or FQDN
Unified zero trust policies	<ul style="list-style-type: none"> • Unified policy for user-to-application, IoT device-to-application, and server-to-server through ZPA's enhanced policy to include new client types • Location and geo-based policies • Security policy enablement that includes IPS, SSL proxy, URL filtering and data protection • Full security stack with posture configured for IoT/OT and servers
High availability	<ul style="list-style-type: none"> • Automatic failover with N+2 redundancy ensures service continuity • Two instances of Branch Connector provide additional support for traffic bursts and redundancy in case of a hardware failure • A load balancer is configured for active-passive fault tolerance using a virtual IP address (VIP) using common address redundancy protocol (CARP)
Centralized visibility and granular logging	<ul style="list-style-type: none"> • Centralized dashboard for device health and traffic monitoring • Available filtering for cloud, data center, and branch deployments • Detailed logging of every session and transaction for all ports and protocols—including all public and private DNS transactions • Full integration with NSS infrastructure—existing NSS firewall VM can be used to stream the logs to SIEM
WAN interface termination	<ul style="list-style-type: none"> • Dual ISP connectivity (Ethernet) • Multi-homing with a single appliance
LAN interface management	<ul style="list-style-type: none"> • Multiple L3 LAN networks • 802.1q/VLAN tagging support • DHCP server • DNS gateway
On-device firewall policies	<ul style="list-style-type: none"> • Granular access control for local LAN to LAN (east-west) traffic • L3/L4 Access Control Lists (ACLs)
Application aware path selection	<ul style="list-style-type: none"> • Dynamic path selection for mission-critical SaaS or private applications • Intelligent Zscaler POP connectivity • Built-in SLA monitoring and failover
Routing	<ul style="list-style-type: none"> • Static routing
Zscaler Data Centers/POPs	<ul style="list-style-type: none"> • Zscaler has built its cloud security platform in more than 150 data centers across the world – strategically placed where customers are located • Built-in availability with seamless failover to next available service PoP



About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at [zscaler.com](https://www.zscaler.com) or follow us on Twitter @zscaler.

© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ and other trademarks listed at [zscaler.com/legal/trademarks](https://www.zscaler.com/legal/trademarks) are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.