WHITE PAPER

Leveraging Zscaler Zero Trust Platforms to Meet CMMC

Helping Organizations Meet CMMC Compliance

Contents

Executive Summary

This document reviews the Zscaler architecture and identifies how it helps an organization or a DoD supplier meet and comply with the DoD Cybersecurity Maturity Model Certification (CMMC). This addresses CMMC compliance from an architecture perspective and helping to meet compliance with the controls of NIST 800–171. Zscaler supports organizations seeking compliance by leveraging its security architecture that supports network transformation and zero trust and has been recognized by Gartner as a leader for the past 10 years.

This solution is based on Zscaler's Internet Access–Government (ZIA GOV) and Private Access–Government (ZPA GOV) systems. These platforms are FedRAMP certified (Moderate, High) and meet the 2023 DoD requirements for FedRAMP and FedRAMP equivalency[1]. They enhance the security of an organization and reduce the risk of CUI data loss. The Zscaler platforms support an organization's effort to modernize its security architecture while meeting critical CMMC controls across all levels.

Zscaler provides a modern SSE solution constructed in software–defined perimeter that performs as the bedrock for a Zero Trust Architecture (ZTA). The Zscaler architecture minimizes risk and compromise for an organization by reducing the attack surface and allowing only authenticated endpoints to communicate. The adoption of ZTA improves security and the cybersecurity maturity of an organization. It supports the risk mitigation and cybersecurity principles originally conceived by the DoD when creating CMMC.

[1] "Federal Risk and Authorization Management Program Moderate Equivalency for Cloud Service Providers' Cloud Service Offering," Department of Defense, December 21, 2023.

What is CMMC 2.0?

The Cybersecurity Maturity Model Certification (CMMC) program is aligned to DoD's information security requirements for Defense Industrial Base (DIB) partners. CMMC is designed to enforce protection of sensitive unclassified information that is shared by the DoD with its contractors and subcontractors. The program provides the DoD increased assurance that contractors, subcontractors, and research institutions are meeting the cybersecurity requirements that apply to acquisition programs and systems that process controlled unclassified information.

The CMMC 2.0 program has three key features:

- Tiered Model: CMMC requires that organizations entrusted with national security information implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forward the process for requiring protection of information that is flowed down to subcontractors.
- Assessment Requirement: CMMC assessments allow the Department to verify the implementation of clear cybersecurity standards.
- Implementation through Contracts: Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

CMMC Model encompasses 14 Capability Domains and three levels to measure cybersecurity maturity. CMMC 2.0 standardized the control set to align with NIST 800–171 for Level 2 and incorporate an additional control set from NIST 800–172 for level 3 compliance.

Status of CMMC 2.0

On December 26, 2023 the DoD released the CMMC Proposed Final Rule. The CMMC rule has been four years in the making and will require CMMC compliance to sell services to the DoD. The DoD closed the window for public comment on February 26, 2024. The DoD is in the process of reviewing the public comments and the expected publication of the CMMC Final Rule will occur in early 2025.

DFARS Clause 252.204–7012, NIST 800–171 and 800–172 cybersecurity requirements for prime and subcontractors are no longer voluntary. DoD audits, coupled with the Cybersecurity Maturity Model Certification (CMMC), will require all organizations conducting business with the DoD to self–attest or be certified by a third party, or C3PAO, that they meet specific CMMC level criteria. A C3PAO is a service provider organization that the CMMC Accreditation Body (CMMC–AB) has accredited and authorized to conduct CMMC assessments. The C3PAO also submits findings and recommendations to the Cyber–AB to certify that Organizations Seeking Certifications (OSCs) seeking to bid, win, and perform in a specific Aerospace & Defense contract comply with the CMMC 2.0 levels 1–3.

One of the notable additions identified in the December 2023 CMMC rule is the addition of an attestation from a senior level official that validates an organization's compliance for CMMC. This signals the DoD is shifting to stronger accountability to the DIB which in turn opens the door for penalties for non–compliance. Additionally, on December 21, 2023 the DoD released the "DoD FedRAMP Equivalency" for cloud service providers. This memo requires FedRAMP Moderate or FedRAMP Ready platforms when used to support Covered Defense Information. This identifies the DoD support for cloud platforms contingent upon the proper security and certifications being in place.

The Case for CMMC

The aggregate loss of controlled unclassified information (CUI) from the Defense Industrial Base (DIB) increases the risk to national economic security and, in turn, national security. To reduce this risk, the DIB must enhance its protection of CUI in its networks.

The Center for Strategic and International Studies (CSIS) estimates that malicious cyber activity costs the world $945 billion annually[2]. This trend has been steadily rising over the past 10 years. Statista estimates global cybercrime will increase to $13.8 trillion by 2028[3]. In February 2024 the Wall Street Journal reported the head of the FBI addressed congress and identified that Cyberattacks from China are at an unprecedented scale. He further discussed that China had pre–positioned malware in critical US systems[4].

Zscaler and its CIO office has identified the following five attack trends for 2024 and the evolving cybersecurity landscape and threat vectors which further support the need for CMMC[5].

- Generative AI–Driven Attacks – AI is maturing to support more use cases and applications including Cybersecurity attacks. GenAI tools will become available in 2024 that allow threat actors to automate attack vectors such as exposed firewall assets, VPN or VDI.

[2] "Extremely Destructive' Russian Cyberattacks Could Cost U.S. Billions of Dollars in Economic Damage, Goldman Warns" Forbes, March 7, 2022.
[3] "Estimated Cost of Cybercrime Worldwide 2012 – 2028" Statista 2024.
[4] "FBI Director Says China Cyberattacks on U.S. Infrastructure Now at Unprecedented Scale," Wall Street Journal, February 18, 2024.
[5] "Top 5 Cyber Predictions for 2024: A CISO Perspective" January 02, 2024, Zscaler Blog.

AI has the potential to catapult cyberthreat evolution years into the future in a matter of months. 2024 is an election year in the United States and AI will be used to power misinformation and other elusive attacks.

- Ransomware as a Service – Ransomware will continue to evolve and Ransomware as a Service will spread and increase the volume of successful attacks. The Ransomware as a Service model will elevate cybercrime and empower less skilled crime groups to expand their reach into digital networks and cyberspace.
- Evolution of Man in the Middle (MiTM) Attacks – Failure to implement a zero-trust architecture will result in an increase in man in the middle attacks. There is trending use of Phishing toolkits that leverage sophisticated MiTM attacks which are accessible to a broader range of threat actors. This tactic targets users of a specific server or system and captures data in transit, such as user authentication credentials by mimicking online services through proxy servers.
- Supply Chain Attacks on Generative AI and Ecosystems – Supply Chain attacks will target vulnerable generative AI ecosystems. As supply chains become more interconnected and attacks more sophisticated in 2024, both upstream and downstream components of supply chains will be increasingly at risk. As organizations integrate more AI components to their supply chains, Large Language Mode (LLM) and AI will increasingly be part of supply chain security conversations.
- Government Regulations related to Cybersecurity reporting – Attackers will further hone their already adept stealth methods of cyberattacks and remain undetected. Expect a heightened focus on covert strategies leveraging evasion techniques and encryption to support undetected access.

The above trends demonstrate evolving threats and the use of AI and advanced techniques used for cyberattacks. Nation states have been conducting cyber-attacks against DIB companies and stealing US Intellectual Property with increasing frequency. The CMMC looks to temper the problem and provides cybersecurity protection improvements combined with an assessment framework to ensure the confidentiality of US data supported by the DIB.

Zscaler: A Crossroads of Transformation and CMMC Compliance

The Zscaler ZIA and ZPA platforms enable organizations to securely connect users to the internet and applications, regardless of device, location, or network. The platforms improve security, reduce cost and deliver a better user experience.

As organizations implement IT modernization initiatives, they should be striving to reduce network and security complexities while improving their security posture, incident response times, and user experience. Zscaler transforms organizations with Zscaler Internet Access-Government (ZIA GOV) enabling organizations to route mission-critical traffic securely to the cloud without the latency of hair-pinning through an organizations security gateway or Policy Enforcement Points (PEP).

Additionally, the native operation of Zscaler will address many of CMMC's challenging technical controls.

Zscaler provides support for an organization's strong authentication and integrates with SAML to ensure the extensibility and enforcement of IDP credentials. Zscaler securely forwards traffic to Zscaler enforcement nodes leveraging industry and government tunneling and encryption standards. Zscaler provides policy enforcement for an organization to ensure the protection of CUI and FCI data and allow access to only authorized individuals.

Zscaler's infrastructure supports CMMC leveraging the multiple government accreditations. This includes FedRAMP Moderate (ZIA, 2019) to FedRAMP JAB High (ZPA, 2020) to DoD Impact Level 5 (ZPA, 2021). Zscaler's various accreditations not only illustrate the ability to support federal and defense customers, but also an emphasis on promoting federally approved NIST compliant Secure Service Edge (SSE) technologies. Along with ZIA and ZPA, Zscaler's Digital Experience technology is available in FedRAMP Moderate and ZIA FedRAMP High environments.

From Secure Web Gateways (SWG) to Security Service Edges (SSE), Gartner has consistently recognized Zscaler as a Magic Quadrant Leader for 12 years. This year-after-year performance underscores the Zscaler Zero Trust Exchange and Zscaler Advanced Cloud Sandbox as the industry model for successfully implementing the Cybersecurity and Infrastructure Security Agency's (CISA's) Trusted Internet Connection (TIC) 3.0 guidelines. Zscaler is committed to helping keep civilian organizations and employees safe, productive, and focused on their mission.

Lastly, receiving FedRAMP-High and DoD IL5-High Impact levels has positioned Zscaler uniquely to support more customers within the Department of Defense (DoD) and Intelligence Community (IC) organizations. As an accredited DoD IL5 Zero Trust solution, Zscaler is fit to protect the government's most sensitive, unclassified data against the catastrophic effect on operations, assets, or warfighters wherever they are operating within the DoD or IC's multi-hybrid cloud strategy.

ZS-CMMC 2.0 Security Control Mapping

The Zscaler ZIA and ZPA were mapped against NIST 800-171 (Rev 2) to determine how the products align with the CMMC requirements. Zscaler's CMMC 2.0 controls directly and indirectly map to the CMMC controls and allow an organization using Zscaler a path towards CMMC compliance. The Zscaler Zero Trust Architecture also supports CMMC Level III controls and NIST 800-172 and the prevention of advanced threats like APTs via the inherent elements of the ZTA architecture.

An overview of the Zscaler mapping to CMMC controls are summarized in the table below:

Meets CMMC 2.0 Control | Supports CMMC 2.0 Control | N/A: Customer Process | N/A

Access Control (AC)	Awareness & Training (AT)	Audit & Accountability (AU)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Risk Assessment (RA)	Security Assessment (CA)	System & Communication Protection (SC)	System & Information Integrity (SI)
AC.L1-3.1.1	AT.L2-3.2.1	AU.L2-3.3.1	CM.L2-3.4.1	IA.L1-3.5.1	IR.L2-3.6.1	MA.L2-3.7.1	MP.L1-3.8.3	PS.L2-3.9.1	PE.L1-3.10.1	RA.L2-3.11.1	CA.L2-3.12.1	SC.L1-3.13.1	SI.L1-3.14.1
AC.L1-3.1.2	AT.L2-3.2.2	AU.L2-3.3.2	CM.L2-3.4.2	IA.L1-3.5.2	IR.L2-3.6.2	MA.L2-3.7.2	MP.L2-3.8.1	PS.L2-3.9.2	PE.L1-3.10.3	RA.L2-3.11.2	CA.L2-3.12.2	SC.L1-3.13.5	SI.L1-3.14.2
AC.L1-3.1.3	AT.L2-3.2.3	AU.L2-3.3.3	CM.L2-3.4.3	IA.L2-3.5.3	IR.L2-3.6.3	MA.L2-3.7.3	MP.L2-3.8.2		PE.L1-3.10.4	RA.L2-3.11.3	CA.L2-3.12.3	SC.L2-3.13.2	SI.L1-3.14.4
AC.L2-3.1.4		AU.L2-3.3.4	CM.L2-3.4.4	IA.L2-3.5.4		MA.L2-3.7.4	MP.L2-3.8.4		PE.L1-3.10.5		CA.L2-3.12.4	SC.L2-3.13.3	SI.L1-3.14.5
AC.L2-3.1.5		AU.L2-3.3.5	CM.L2-3.4.5	IA.L2-3.5.5		MA.L2-3.7.5	MP.L2-3.8.5		PE.L2-3.10.2			SC.L2-3.13.4	SI.L2-3.14.3
AC.L2-3.1.6		AU.L2-3.3.6	CM.L2-3.4.6	IA.L2-3.5.6		MA.L2-3.7.6	MP.L2-3.8.6		PE.L2-3.10.6			SC.L2-3.13.6	SI.L2-3.14.6
AC.L2-3.1.7		AU.L2-3.3.7	CM.L2-3.4.7	IA.L2-3.5.7			MP.L2-3.8.7					SC.L2-3.13.7	SI.L2-3.14.7
AC.L2-3.1.8		AU.L2-3.3.8	CM.L2-3.4.8	IA.L2-3.5.8			MP.L2-3.8.8					SC.L2-3.13.8	
AC.L2-3.1.9		AU.L2-3.3.9	CM.L2-3.4.9	IA.L2-3.5.9			MP.L2-3.8.9					SC.L2-3.13.9	
AC.L2-3.1.10				IA.L2-3.5.10								SC.L2-3.13.10	
AC.L2-3.1.11				IA.L2-3.5.11								SC.L2-3.13.11	
AC.L2-3.1.12												SC.L2-3.13.12	
AC.L2-3.1.13												SC.L2-3.13.13	
AC.L2-3.1.14												SC.L2-3.13.14	
AC.L2-3.1.15												SC.L2-3.13.15	
AC.L2-3.1.16												SC.L2-3.13.16	
AC.L2-3.1.17													
AC.L2-3.1.18													
AC.L2-3.1.19													
AC.L2-3.1.21													
AC.L1-3.1.20													
AC.L1-3.1.22													

Figure 1 — CMMC Control Graph Mapped

As outlined in the above graph, Zscaler organized its CMMC capabilities into one of four categories:

- **Meets CMMC 2.0 Controls:** Zscaler GovCloud provides a direct means to support the practice requirement presuming proper configuration and enrollment.
- **Supports CMMC 2.0 Controls:** Performing as a force multiplier, Zscaler's GovCloud suite of capabilities, customers facilitate additional activities and requirements, which support compliance with CMMC's practice requirements.
- **Not Applicable/Customer Process:** Part of CMMC's focus centers on an organization's internal policies and procedures. It is process-driven and inherently a customer responsibility and may not support the respective CMMC controls in such cases; Zscaler can leverage its FedRAMP-High and DoD experience to guide customers to achieve industry best practices.
- **Not Applicable:** Identified CMMC 2.0 controls are the customer's full responsibility.

Of the three CMMC levels Zscaler provides an organization substantial leverage in meeting each of the controls. The bar chart below identifies the CMMC requirements and the controls and procedures and processes that can be addressed through the Zscaler solution.

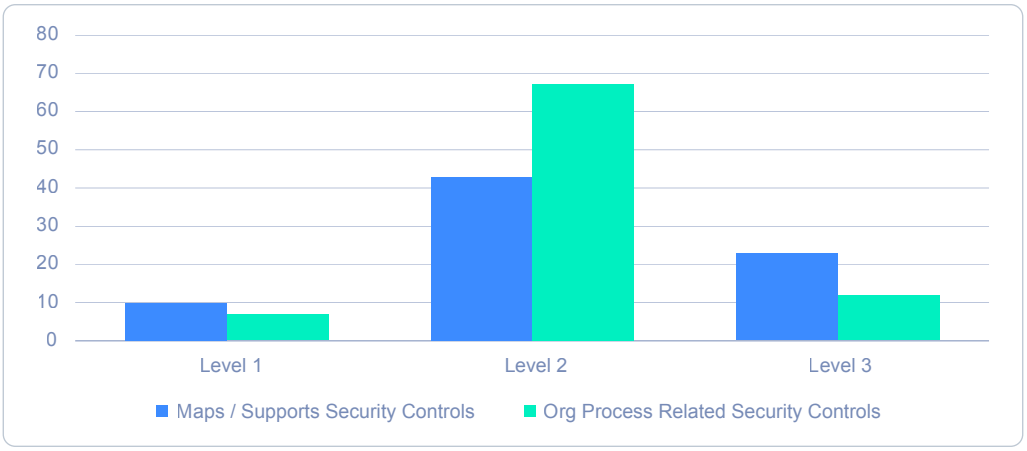


Figure 2 — CMMC 2.0 Level 1, 2, and 3* Levels and Zscaler Applicability | *CMMC 2.0 Level 3 coverage is notional

Conclusion

Zscaler can assist an organization in transforming its IT security environment to be highly adaptive to the new threat landscape and provide a modernized approach to meet US federally regulated accreditations, like CMMC. Zscaler provides a path towards cybersecurity maturity, network transformation, zero trust which results in a more secure environment with a better user experience

Appendices

Appendix A — ZS CMMC 2.0 Technical Mapping

The below sections highlight Zscaler's GovCloud technical abilities that either map or support CMMC's security controls and practices.

ZS-GovCloud: Access Control

ZIA GOV

- Manages access by authorized users through a SaaS service.
- Controls what activities a user can perform on cloud apps via CASB.
- Leverages IDP context when building access policies.
- Encrypts all data to the Zero Trust Exchange, assuming the lowest level of security.
- Monitors and controls all connections as a full proxy.
- Routes all on-prem and remote traffic.
- Creates deny rules based on location.
- Fully controls any outbound connections to external systems.
- Ensures controlled information is not accessed by unauthorized users on cloud applications.

ZPA GOV

- Encrypts all data to the Zero Trust Exchange, assuming the lowest level of security.
- Monitors and controls all connections as a full proxy.
- Zero Trust for all on-prem and remote traffic.
- Allows for posture checks for remote admins before access.
- Limits internal user access to external systems.
- Fully controls who can access applications that contain CUI data.
- Shows application and server locations as users request them.

ZS-GovCloud: Audit & Accountability

ZIA GOV

- Logs all transactional data from user to service.
- Maintains and provides access to audit logs for a year.
- Provides in-depth logging and analytics for multiple security tools to one log feed and automated dashboard and report generation.
- Reduces the number of logs and the amount of log data.

ZPA GOV

- Logs all connections at a trans-actional level, including user/device/app/location.
- Maintains and provides access to audit logs for a year.
- Provides in-depth logging and analytics for multiple security tools to one log feed and automated dashboard and report generation.
- Shows application and server locations as users request them.
- Reduces the number of logs and the amount of log data.

ZS-GovCloud: Configuration Management

ZIA GOV

- Blocks applications by default.

ZPA GOV

- Blocks applications by default.
- Ensures Zero Trust Access (443) for every port opened outbound to the network.
- Shows application and server locations as users request them.

ZS-GovCloud: Identification & Authentication

ZIA GOV

- Limits access of identified users to specified resources stored in the cloud.
- Validates the identity before granting access to the application, data, and resources.
- Supports the IdP's enforcement of passwords
- Supports the enforcement of multifactor authentication capability before granting access to any user.

ZPA GOV

- Controls access by identified users to specified private applications.
- Validates identity before granting access to the resource.
- Supports the IdP's enforcement of passwords.
- Supports the enforcement of multifactor authentication capability before granting access to any user.
- Configures device posture profiles.

ZS-GovCloud: Incident Response

ZIA GOV

- Supports detection and reporting of events as part of CISCP and DIB-CS.
- Supports tracking, documenting, and reporting incidents to designated officials.
- Supports a Security Operations Center (SOC) capability that facilitates a 24/7 response.
- Supports the use of manual and automated, real-time responses to anomalous activities.
- Reduces false positives.
- Use of AI to correlate incident data.
- Uses Zscaler's constantly updated threat database to provide automatic mitigations for IOCs.

ZPA GOV

- Supports detection and reporting of events as part of CISCP and DIB-CS.
- Supports tracking, documenting, and reporting of incidents to designated officials.
- Supports a Security Operations Center (SOC) capability that facilitates a 24/7 response.
- Supports the use of manual and automated, real-time responses to anomalous activities.

ZS-GovCloud: Risk Management

ZIA GOV

- Catalogs and periodically updates threat profiles and adversary Tactics, Techniques & Procedures (TTPs).
- Employs AI-backed threat intelligence to develop system architecture, selection of security solutions, monitoring, threat hunting, and response and recovery activities.

ZPA GOV

- Catalogs and periodically updates threat profiles and adversary Tactics, Techniques & Procedures (TTPs).
- Employs AI-backed threat intelligence for developing system architecture, selecting security solutions, monitoring, threat hunting, and response and recovery activities.

ZS-GovCloud: System & Information Integrity

ZIA GOV

- Uses AI-backed threat indicator information to inform intrusion detection and threat hunting as a part of CISCP and DIB-CS.
- Immediately update malicious code protection mechanisms when new releases are available.
- Provides AV scans on every external transaction, including SSL B/I encrypted traffic.
- Logs all outbound and inbound activity from ZIA assets.

ZPA GOV

- Logs all outbound and inbound activity all from ZPA assets.
- Configures device posture profiles.

ZS-GovCloud: System & Communications Protection

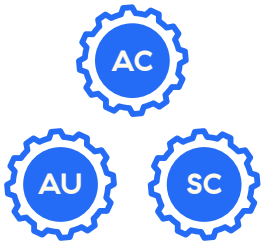
ZIA GOV

- Forwards traffic to the ZIA cloud using IPsec or TLS with FIPS-validated cryptography.
- Scans for the exfiltration of sensitive traffic through DLP & CASB.
- Denies network communications traffic by default and allows network communications traffic by exception.
- Prevents unintended data exfiltration through intelligent traffic routing.
- Implements cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission.
- Terminates network connections at the end of the sessions or after a defined period of inactivity.
- Protects the authenticity of communications sessions.
- Logically isolates all network traffic.
- Completely isolates access to a CUI environment for approved SaaS.
- Enforces port and protocol compliance.
- Fully monitors and controls the system from the internal to the external boundaries.

ZPA GOV

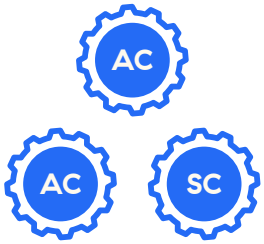
- Enforces port and protocol compliance.
- Fully monitors and controls the system from the internal to the external boundaries as a full security stack.
- Redefines organizational boundaries based on the user's need and threat landscape with their Zero Trust Exchange approach.

Appendix B – ZS-CMMC 2.0 Capability Mapping



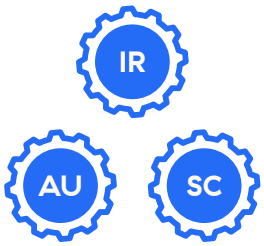
Advanced Firewall

Protects users connecting to the Internet with application visibility and user access-level controls for all ports and protocols.



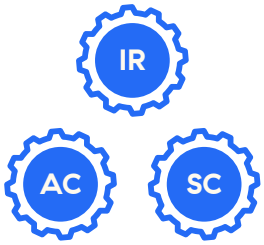
Full DNS Security (including DNSSEC and DNS tunneling)

DNS Tunneling can be used to circumvent traditional security measures and has the potential to introduce a variety of hazards into networks. Zscaler has introduced the ability to detect, control, and analyze tunneling traffic to counteract this threat.



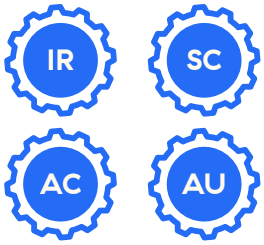
Advanced Cloud Sandbox

Complete Behavioral Analysis (BA) engines that implement non-signature-based protection against zero-day exploits. Patient "Zero" protection with your Sandbox policy is configured to allow and scan files for the first-time action. This Zscaler service blocks users from downloading unknown files until the file is sent to the Sandbox for behavioral analysis. If a file is found to be malicious, this becomes a patient O event.



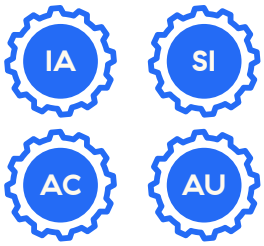
URL Filtering

Protect your organization from harmful URLs using granular policies that specify who can access what, when, where, and how.



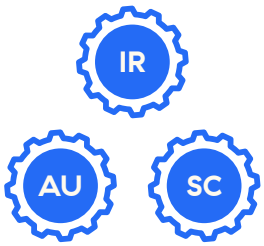
Cloud Application Control (CASB)

Manage access to cloud applications like webmail, streaming media, social networking, and instant messaging with granular policies that specify who can access what, when, where, and how.



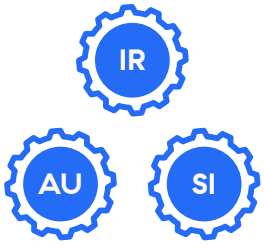
Data Loss Prevention (DLP)

Protects data across devices and networks to ensure data locality, data privacy, and regulatory requirements are met through granular controls—ensuring that data does exfiltrate the CMMC-defined boundary for the organization.



Nanolog & Log Streaming Service (NSS & LSS)

Seamlessly transmits web and firewall logs from the Zscaler Cloud to the enterprise security information and event management (SIEM) in real-time, like Sentinel, Splunk, IBM QRadar, and more. Tight integration with best-of-breed SIEM providers with the Zscaler Splunk App provides detailed dashboards and reporting for all Zscaler products, including the ingest DLP incident information, bringing full context for DLP incidents directly into Splunk.



Private Service Edge (PSE)

Deploy to extend Zscaler's cloud architecture to the Organization premises using virtual machines (recommended only for Organizations with specific regulatory or connectivity requirements).

zscaler™ | Experience your world, secured.™

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** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com