zscaler™ | U.S. Government Solutions

Secure and Scalable Zero Trust Solutions for the Department of Defense (DoD)

Zscaler US Government Solutions, LLC

Address: 7900 Westpark Drive McLean, VA 22102

WHITEPAPER

Table of Contents

1. Introduction

As the Department of Defense (DoD) advances its Zero Trust transformation, Zscaler has emerged as a key solution for modernizing security, streamlining user access, and strengthening mission readiness. Traditional hardware and IP address–centric approaches relied on implicit trust within perimeter–based networks, which are often costly to maintain and prone to exploitation by adversaries. To meet the demands of an increasingly interconnected environment—spanning cloud, mobile, and on–premises systems—the DoD requires a scalable and resilient solution that enforces continuous verification rooted in Zero–Trust principles.

Zscaler meets these requirements through its certified Federal (FedRAMP Moderate and High) and Defense (Impact Level 2 and 5) authorizations, ensuring the secure handling of unclassified data at the appropriate information Impact Levels. Furthermore, through our continued commitment to the Department, Zscaler has proven its ability to provide a IL6 capable solution that enables a robust security framework for classified environments. Our solution is seamlessly deployable without the need for operator retraining as the IL6 administration will be nearly identical to Zscaler's IL5 solution.

Zscaler's hybrid on–premises and cloud–based solution provides consistent security enforcement and seamless connectivity, regardless of where operations take place. This hybrid approach aligns with the DoD's shift to a zero–trust paradigm by eliminating assumptions of trust, applying granular policies, and enforcing least–privileged access on a continuous basis. By leveraging Zscaler's various authorized clouds and extending that cloud to an on–premises environment (where applicable) with Private Service Edge, the DoD can transition away from the legacy mindset of "trust but verify once" to a state–of–the–art architecture of "verify, limit lateral movement, and authenticate continuously." The end result provides enhanced security and mission agility while reducing cost and infrastructure complexity. This will allow DoD Enterprise to adopt modern zero–trust principles that are resilient, secure, and scalable.

This document further outlines how Zscaler's overarching offerings address the critical challenges faced by the DoD, including secure and scalable access in contested and degraded environments (DDIL/CDO–L). By taking advantage of advanced cloud native technologies with flexible on–premises solutions the DoD, using Zscaler, ensures resilient, secure, and mission ready solutions tailored to meet the DoD's operational current and future goals.

Accelerating DoD's Zero Trust Mission

Zscaler Delivers Resilient, Secure, and Scalable Access Across Cloud and On–Prem Environments.

2. The Defense Departments Program Overview

The DoD Zero Trust (ZT) Strategy outlines a forward-looking vision for zero trust security as a critical enabler of the DoD's mission. Central to this strategy is the recognition that *"a Zero Trust culture lays the rock-solid digital foundation that connects all DoD members across a trusted digital force."* This culture will advance through the integration of people, processes, and technologies, all strategically aligned to deliver operational advantages in a rapidly evolving national security environment. Furthermore, the DoD's ZT strategy emphasizes *"delivering a future cybersecurity posture that simplifies access for DoD members while imposing higher costs on competitors and adversaries."*

The shift from network-centric to data-centric security demands a concentrated effort to safeguard the DoD's most critical mission-essential data, applications, assets, and services (DAAS). This approach aims to prevent, detect, respond to, and recover from malicious cyber activity across diverse operational environments. The DoD's current trust and access model relies heavily on IP addresses supporting USG, applications, servers, and externally managed endpoints. This dependency requires the use of IP addressed-based access control lists (ACLs) and firewalls, enforcing simple go/no-go policies without accounting for contextual "need-to-know." nor true user identity. Decisions based solely on IP addresses provide access to applications and data without regard to intent, device posture, identity nor extended attributes. Zscaler addresses these limitations by implementing attribute-based access controls, which consider both the hygiene status of externally managed endpoints and the user's identity. Unlike traditional one-time authentication methods such as SSO, Zscaler continuously evaluates user and device attributes to ensure secure access. Zscaler Private Access also eliminates lateral movement within the network, a critical measure to halt malware reconnaissance. By preventing lateral movement, Zscaler mitigates the first steps of the MITRE ATT&CK® Framework—reconnaissance and phishing attacks—severely restricting adversaries' ability to identify vulnerabilities or bypass policy enforcement points.

This approach has proven effective against advanced cyber threats, such as those seen in the recent MGM Resorts cyberattack. By eliminating opportunities for adversaries to reconnoiter or exploit weak access controls, Zscaler significantly reduces the risk of breaches. In summary, the integration of endpoint detection, identity providers, and Zero Trust Network Access (ZTNA) enables granular access control on a per-user, per-transaction, and per-application basis at scale. This comprehensive strategy aligns with the DoD's Zero Trust vision, ensuring a resilient and secure operational environment for the future.

Modernizing DoD Access Models

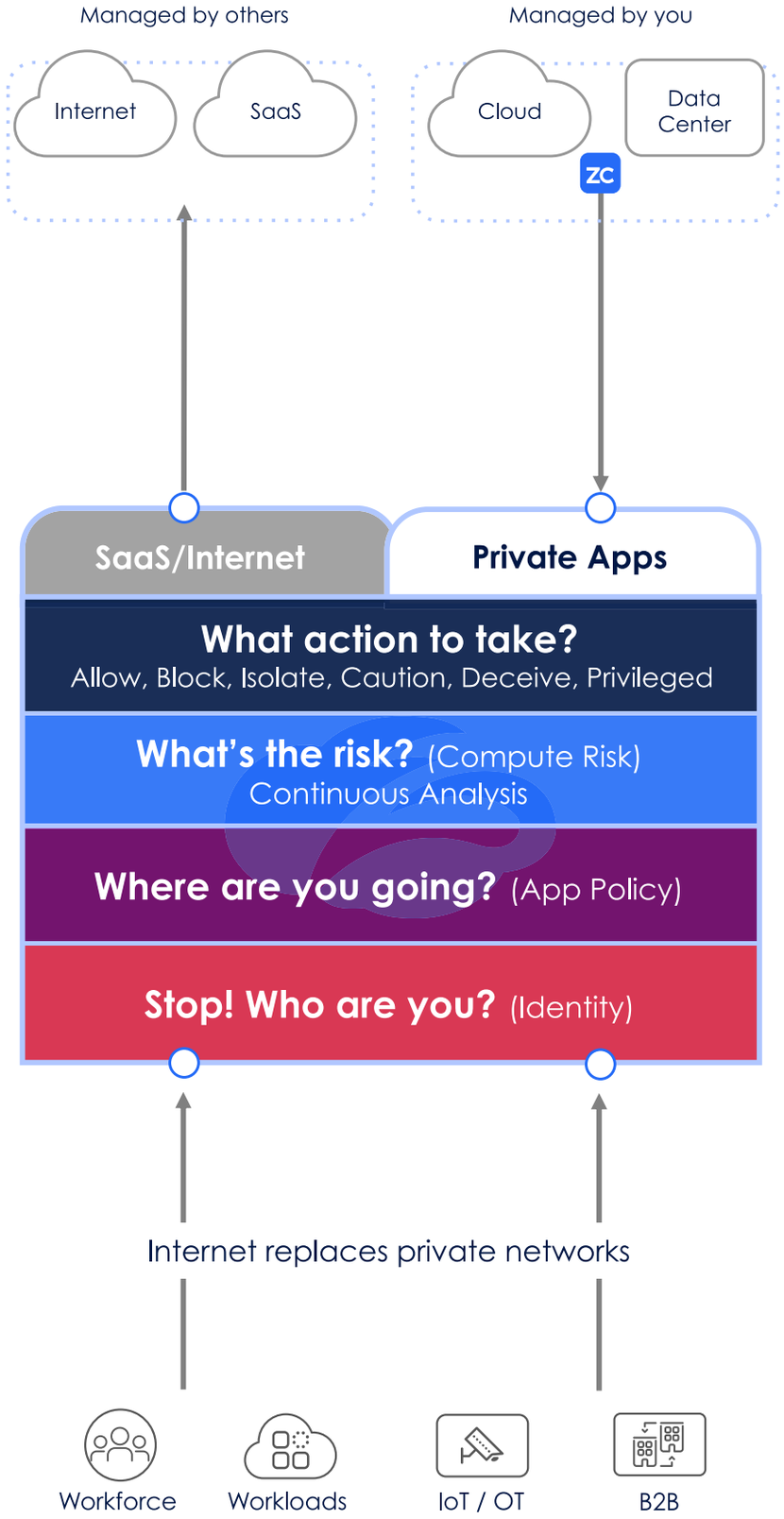
From IP Lists to Per-User, Per-Transaction Zero Trust Controls.

3. Zscaler Solutions Overview

Zscaler's solution delivers unparalleled capabilities for securing applications and users across on-premises, remote, and mission-critical environments. Key differentiators include seamless integration with Identity Providers (IdP) via SAML, open APIs for custom integrations, and certifications tailored to Federal and Defense requirements. Zscaler supports these transformative initiatives through its Zero Trust Exchange platform, which integrates Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), and Zscaler Digital Experience (ZDX). The image below demonstrates the five tenants of Zero Trust.

4 No pass through connections allowed

Forward Proxy for full content & SSL inspection (Saas/internet Reverse Forward Proxy combined for internal apps access. Eliminates the egress attack surface – no source IPs exposed.



5 No inbound connections (internal apps)

Outbound-only connections between a user and app

Apps are invisible, not exposed to the internet Eliminates attacks on apps and services *(can't attack what you can't see)*.

3 Connect to an app, not a network

App segmentation without network segmentation. The network is just transport.

2 Verity user identity and context

Single and multi-factor user authentication. Conditional access with device, location, app context.

1 Distributed multitenant architecture (100+ locations)

Policy and security enforced near the user (no backhaul)
Thin branch for routing, security in the cloud.

As demonstrated in the image above, Zscaler's comprehensive suite enables secure, policy-driven access to mission-critical applications by creating micro-tunnels over existing network infrastructure. As a cloud-native platform, Zscaler reduces latency, enhances operational efficiency, and improves user experiences for DoD personnel through its globally distributed infrastructure. Once Zscaler is configured and applications are transitioned from the existing infrastructure to Zscaler's logical Zero Trust Exchange, all direct client-to-server network access is eliminated. Importantly, no user or refactoring of the application is required to implement Zscaler's Zero Trust Solution. This eliminates unfettered lateral movement by users and grants access to mission-critical applications on need. It also eliminates the ability of non-authorized users to enumerate or connect to the application without being vetted and connected through the Zero Trust Exchange. Finally, the user traffic is securely routed through Zscaler's TLS based micro-tunnel overlay, enforcing a Zero Trust Network Access (ZTNA) posture and ensuring a resilient, secure operational environment.

3.1. DoD Potential Use Cases

Zscaler's cloud-native approach to zero trust, driven by policy-based access, seamlessly aligns with a wide range of use cases within the Defense Department. Among the many use cases, we have identified four that demonstrate the highest potential for immediate impact. These use cases directly address critical challenges faced by network and security administrators, offering pragmatic solutions to essential operational requirements.

The Zscaler security model prioritizes secure connections by ensuring that access is granted only to authenticated and authorized users, in alignment with organizational defined policies. These brokered connections enable seamless access to applications and services, irrespective of the user's location or the application's hosting environment, making them highly adaptable to diverse operational scenarios

3.1.1. Use Case #1: Internet Access Point Modernization

Zscaler Internet Access (ZIA) can serve as a modern replacement for the DoD Internet Access Points by consolidating critical security and traffic inspection capabilities into a cloud-native or hybrid Zero Trust platform. ZIA operates as a secure web gateway, seamlessly integrating advanced features such as Full Content Inspection (FCI), Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), advanced threat protection, and data loss prevention. These capabilities are inherently built into Zscaler's globally distributed cloud architecture, delivering best-in-class protection inline with traffic flow for both users and applications.

By routing all user traffic through its distributed cloud, ZIA eliminates the need for traditional, hardware-based access points, providing unparalleled scalability, enhanced visibility, and uniform policy enforcement across all locations. For deployments requiring on-premise control of the data plane, Zscaler can extend its architecture through Private Service Edges, enabling localized traffic processing while maintaining the full benefits of centralized cloud management and security. This flexible, scalable approach simplifies operations, improves performance, and ensures compliance with DoD's stringent security requirements, empowering secure and efficient internet access for users globally.

3.1.2. Use Case #2: Cloud Browser Isolation

Today the DoD does not have a fully integrated Cloud Browser Isolation (CBI) with its IAP by integrating Cloud Browser Isolation (CBI) into Zscaler Internet Access (ZIA) this provides the DoD with a streamlined and highly secure solution for mitigating browser-based threats.

As a cloud-native secure web gateway, ZIA inspects traffic inline using a Zero Trust framework, and CBI enhances this by isolating active web content—such as JavaScript and HTML—in a disposable cloud-based environment. This prevents malicious code from reaching endpoints, safeguarding against threats like drive-by downloads, zero-day exploits, and phishing.

By consolidating CBI into ZIA's distributed architecture, the DoD benefits from efficiency of consistent policy enforcement, simplified management, and seamless scalability, eliminating the need for standalone solutions. This integration supports the DoD's modernization goals by reducing complexity while maintaining compliance with stringent security standards, enabling secure and efficient web access for users anywhere.

3.1.3. Use Case #3: Identity Attribution and Multi-cloud access

To access applications, users must first be authenticated through a SAML 2.0-compliant Identity Provider (IdP). User attributes configured within the IdP can be seamlessly integrated into Zscaler's policy engines, enabling highly granular control over which users are permitted to access specific applications. Applications secured by the Zscaler platform are hosted in known, trusted locations with defined reachability from the Zscaler cloud. Importantly, users are not required to have any knowledge of these applications from a network perspective, such as their IP addresses, physical or cloud-based locations, or architecture.

In a multi-tenant environment, this approach enhances the security posture of all applications. The Zscaler platform protects communication and data transfer across multiple Cloud Service Providers (CSPs) , including but not limited to AWS, Azure, and Google. Zscaler's zero-trust security architecture inspects all traffic in real-time and enforces security policies consistently, independent of the data's origin or destination. This ensures secure and seamless connectivity between cloud services within multi-cloud ecosystems while maintaining robust security controls.

3.1.4. Use Case #4: Application Migration

The Zscaler Zero Trust Exchange ensures no user, workload, or device is inherently trusted. It verifies identity, uses AI to assess risk, and enforces policies before securely connecting users to applications—regardless of network or location—through integration with the organization's Identity Provider (IdP). ZPA streamlines early cloud migration efforts by replacing traditional infrastructure with policy-based access control. This approach provides secure and controlled user access during workload migrations between on-premises and cloud environments, all without altering existing network infrastructure.

Applications, whether hosted on-premises or within a multi-tenant cloud architecture, can be seamlessly migrated between environments while ensuring uninterrupted user access. A cornerstone of the Zscaler solution is its ability to actively manage and secure user access to and interact with workloads throughout the migration lifecycle—before, during, and after the transition—while simultaneously enhancing the overall end-user experience.

While Identity and Access Management (IAM) forms the foundation of secure cloud-based access (IaaS), ZPA further strengthens this approach by rendering applications completely invisible to unauthorized users and devices. This ensures that only pre-authorized users and devices can interact with protected applications, effectively mitigating modern security threats such as Distributed Denial-of-Service (DDoS) attacks, unauthorized access from third-party sources, and the lateral movement of malware

within internal networks. This approach ensures a resilient, secure, and agile migration process while upholding zero-trust security principles.

3.2. Zscaler Internet Access (ZIA)

Organizations have invested heavily in traditional firewall-based security, but modern threats demand a cloud-native secure web gateway (SWG). By inspecting 100% of TLS/SSL-encrypted traffic without backhauling or performance impacts, this approach secures every transaction, while reducing cost and complexity. A zero trust proxy architecture enables direct, identity-based user-to-app connections, enforcing policies at scale for comprehensive protection.

Zscaler Internet Access (ZIA) provides a secure, scalable, and cloud-native solution for Internet and Software as a Service (SaaS) application access, and on-premises web applications tailored to meet the unique needs of the Department. As the DoD transitions to cloud-based solutions for greater agility, scalability, and cost savings, this shift also expands the attack surface, increasing exposure to sophisticated threats that evade traditional security measures. Built on Zero Trust principles, ZIA delivers advanced threat protection, seamless integration with existing IT infrastructure, and dynamic scalability to support the DoD's global user base.

When deployed, ZIA acts as a Policy Decision Point/Policy Enforcement Point (PDP/PEP), blocking malicious traffic and inspecting encrypted data in real time leveraging the DoD Public Key Infrastructure (PKI). It mitigates zero-day threats with AI-driven detection – collected from 500 trillion signals per day that Zscaler processes – and sandboxing. In addition, the Data Loss Prevention (DLP) capabilities safeguard sensitive information and ensure compliance with DoD security standards. The DLP function is available for data at rest, data in motion, and data at GFE. Additionally, ZIA's layer-7 application-aware next-generation cloud firewall simplifies management and reduces complexity, providing the DoD with a robust, comprehensive security solution for evolving cloud environments.

Zcaler Internet Access delivers the world's most deployed Security Service Edge (SSE), built on over a decade of Secure Web Gateway (SWG) leadership. This allows replacement of legacy network security solutions with zero trust for secure connectivity, a great user experience, and administrative visibility and control. Furthermore Zscaler can extend its data plane on-premises with Zscaler Internet Access (ZIA) Private Service Edges, delivering the same advanced capabilities as its cloud infrastructure—such as SWG, CASB, DLP, and threat protection—while addressing requirements for data localization, low latency, and compliance. Fully integrated with the Zero Trust Exchange, these service edges ensure consistent policies, seamless scalability, and hybrid cloud support, enabling secure, flexible, and high-performance solutions for organizations bridging cloud and private environments. The capabilities of the ZIA solution are summarized on the next page:

ZIA Capability	DoD ZIA Solution Description
Threat Protection	Blocks malicious traffic and defends against advanced cyberattacks. Zscaler's commercial cloud feeds all its threat data into the IL2 Cloud, which in turn feeds into the IL5 Cloud. Zscaler is also collaborating with the Intelligence Community to integrate their threat data into the IL5 Cloud for enhanced protection.
Real-Time Inspection TLS/SSL	Inspects encrypted traffic to prevent data breaches without degrading performance using DoD PKI.
Data Loss Prevention (DLP)	Secures sensitive data remains during transmission and ensures compliance with standards.
Scalability	Dynamically scales to meet the needs of a growing user base, while maintaining consistent performance.
Integration	Integrates with DoD's existing and future IT infrastructure for centralized policy enforcement and analytics.
NextGen Cloud Firewall	Provides application aware (Layer-7) firewall capabilities to protect against malicious activities.
Advanced Threat Protection	Features sandboxing, machine learning, and AI-driven detection to neutralize zero-day threats.
Content Filtering	Enforces acceptable use policies and blocks access to harmful websites.
User and Application Behavior Analytics	Monitors and reports unusual activity to preempt security incidents and integrates into ZPA for automated risk scoring and policy application.
Identity Proxy	Facilitates secure access with SSO and MFA, controlling access to SaaS applications and preventing zero day attacks in DoD SaaS Tenant.
Cloud Browser Isolation	Isolates harmful web content in a secure, cloud-based environment, including advanced features like Turbo Mode for audio and video.
DNS Security	Filter risky and malicious domains and stop the use of DNS tunneling to transfer malicious payloads and sensitive data.
AI Powered Cloud Sandbox	Stop unknown malware inline with protections sourced from more than 400 billion daily transactions, including zero day threat quarantine.
AI Powered Phishing Detection	Know when patient zero phishing attacks are attempting to infiltrate your agency with advanced AI-based inline detection.
Dynamic Risk-Based Policies	Stop active attacks and future-proof your defenses with continuous user, device, app, and content risk analysis fueling dynamic access controls.

3.3. Zscaler Private Access (ZPA)

Zscaler transforms network security by eliminating the inefficiencies and complexities of traditional firewall-centric architectures. Legacy systems rely on static IP-based enforcement, intricate firewall rules, and segmentation, which create technical bloat, administrative overhead, and vulnerabilities such as lateral movement. Zscaler's modern zero trust approach removes these shortcomings, streamlining operations without requiring major architectural changes.

With Zscaler Private Access (ZPA), the network becomes irrelevant to enforcing security. ZPA securely directs on-demand user traffic through encrypted tunnels, connecting authenticated and authorized users solely to approved applications—without granting access to the broader network. By leveraging all available network paths, including commercial and government, ZPA eliminates insider threats from lateral traffic movement. Its Zero Trust Network Access (ZTNA) model enforces least-privilege access while ensuring resilient connectivity, end-to-end encryption, and the invisibility of applications to unauthorized users.

ZPA also enhances security with continuous monitoring, device posture verification, and seamless integration with tools like SAML 2.0 identity providers, SIEM systems, and endpoint detection solutions. This enables real-time telemetry, context-aware policy enforcement, and dynamic adjustments. Additionally, Zscaler's Cloud Browser Isolation (CBI) can extend the zero trust posture to on-premises web applications. CBI can provide secure access to applications whether managed or unmanaged, on-premises or in private cloud, BYOD or GFE devices. CBI is another tool that the DoD community can employ to reduce the threat while maintaining access for users. The result is a secure, native-like user experience for accessing mission-critical applications without traditional vulnerabilities.

ZPA's capabilities are extended further with ZPA Private Service Edges, which bring Zscaler's zero trust architecture to on-premises environments. Deployed within data centers or private clouds, these edges process traffic locally to reduce latency while enforcing granular, identity-based access controls. They fully integrate with Zscaler's Zero Trust Exchange, simplifying architecture, eliminating lateral movement, and providing secure, scalable, and efficient application access. This ensures compliance with data privacy requirements while modernizing private application access for both remote and on-premises users. Designed for resilience, ZPA solutions can ensure uninterrupted connectivity through multiple pathways in contested or degraded conditions. Private Service Edges (PSE) can be deployed in locations such as airplanes or data centers, enabling continuous operations even when disconnected when enabled by Private Cloud Controllers (PCC). Furthermore, Zscaler PCC functionalities have enhanced the ZPA PSE capabilities to support disconnected operations, allowing it to function independently for up to 90 days under prescribed conditions.

In summary, ZPA delivers zero trust connectivity by securely connecting users to private applications without exposing them to the internet or the network. It eliminates the need for legacy VPNs, reduces the attack surface, and enforces least-privilege access through identity-based policies. With advanced features like continuous monitoring, end-to-end encryption, application invisibility, and integration with enterprise tools, ZPA enhances security while streamlining operations. The result is fast, secure, and reliable access to mission-critical applications for users anywhere, on any device. Capabilities of the DoD ZPA solution are outlined in the table on the next page:

ZPA Capability	DoD ZPA Solution Description
DoD Zero Trust Network Access (ZTNA)	Enforces least-privilege access by granting users access only to authorized applications, not the DoD networks.
Application-Layer Segmentation	Prevent lateral movement of threats within the network by only creating microtunnels from the user to the application only if the user is authorized.
Seamless User Experience	Reduces latency by connecting users directly to applications through tunnels running over the network provided underlay.
Resilience in Adverse Conditions	Optimized to maintain connectivity in DDIL/CDO-L environments with a Private Cloud Controller in each necessary location caching the Zscaler Control Plane on-prem.
Device Posture Verification	Ensure devices meet compliance policies before granting access and create a tunnel to the application or data. Continuously monitor devices for policy changes.
Continuous Monitoring	Monitors behavior and connections to detect anomalies, leveraging data from ZIA and User Risk to make informed security decisions.
End-to-End Encryption	Encrypts all traffic to safeguard data in transit.
No IP Address Exposure	Keeps applications invisible to unauthorized users, reducing the threat surface and ensuring a Zero Trust zone for all applications and data.
Cloud-Native Scalability	Dynamically scale to accommodate global users without requiring additional hardware appliances.
Granular Policy Enforcement	Dynamically adjusts security policies based on user context, such as location, device posture, and risk, ensuring security follows users wherever they are.
Integration with Security Ecosystem	Supports seamless integration with IdPs SIEM systems, and endpoint detection tools for comprehensive security management.
Cloud Browser Isolation for Non-Internet and Private Applications	Secures sensitive data by isolating access to mission-critical private applications, preventing data loss on government-furnished equipment (GFE) and unmanaged devices.

3.4. Zscaler Digital Experience (ZDX)

DoD users rely on 24/7 access to apps, data, and services, so it's essential to secure these assets from cyberattacks as well as ensure optimal performance. Slowdowns and outages can greatly diminish productivity, employee morale, and the customer experience and worse, could lead to mission failure. Legacy digital experience monitoring solutions leave IT teams unable to see the full picture across devices, networks, and apps. Beyond that, zero trust architectures break traditional network monitoring tools.

Zscaler Digital Experience (ZDX) provides end-to-end visibility into user, application, and network performance, ensuring seamless access to cloud, SaaS, and private applications. By collecting real-time telemetry and using synthetic monitoring, ZDX proactively identifies and resolves performance issues, pinpointing root causes across devices, networks, or applications. Integrated with the Zscaler Zero Trust Exchange, it offers centralized dashboards for actionable insights, improves application performance, and enables proactive troubleshooting. Designed for distributed and hybrid workforces, ZDX enhances productivity, streamlines IT operations, and optimizes the digital experience for users anywhere, on any device. Capabilities of the DoD ZDX solution are outlined in the table below:

ZDX Capability	DoD ZDX Solution Description
Application Monitoring	Active monitoring of application availability and uptime from the end user device. Track critical performance metrics, including page fetch time (PFT) and server response time.
Network Monitoring	Gain granular proxy-aware insights about each network hop between the user device and the application, including Zscaler services such as ZIA and ZPA.
Endpoint Monitoring	Track device health metrics, including Wi-Fi signal strength, CPU, memory usage, and network bandwidth usage for each user.
Incident Dashboard	Detects problems in applications, Wi-Fi, Zscaler data centers, last mile and intermediate ISP, and the endpoint, with automated AI-powered correlation.
ZDX Copilot	Instantly troubleshoot and resolve digital performance problems across applications, networks, and devices, and get insights by asking questions.
AI-powered Root Cause Analysis	Automatically isolate root causes of performance issues. One-click comparison highlights the difference between good versus poor user experience.
Software and Hardware Inventory	Fully understand your software and hardware portfolio and versions deployed across your organization and on each device.
Zscaler Hosted Monitoring	Continuously monitor availability and performance of applications and services from globally distributed locations.
Dynamic Alerting	Set up dynamic alerts and customize them to meet your performance needs, allowing for automatic detection of anomalies. Integrate easily with your service management tools such as ServiceNow and push notifications through webhook or email.

4. Zscaler Classified Clouds

As the Department of Defense (DoD) and its partners increasingly rely on secure cloud solutions to meet mission-critical needs, Zscaler is leading the charge in delivering accredited Classified SaaS cloud offerings. These multi-tenant platforms are designed to support the unique requirements of the Defense and Intelligence Communities, ensuring secure, scalable, and efficient access to sensitive information. Through strategic investments, partnerships, and a phased development approach, Zscaler is setting a new standard in secure cloud innovation. By leveraging its proven Zero Trust architecture, Zscaler is addressing the evolving cybersecurity demands of the DoD and DoD while delivering operational advantages to its customers. This section outlines Zscaler's commitment, capabilities, and roadmap for delivering robust IL6 and TS cloud solutions to meet the most stringent requirements.

4.1. Zscaler IL6 Cloud

Zscaler's primary means of delivering an IL6-capable solution falls under a Cooperative Research and Development Agreement (CRADA) with the U.S. SOCOM. Zscaler is building a multi-tenant, fully accredited ZPA IL6 SaaS cloud platform, which is expected to be operational and available within 18—24 months. Additionally, we are actively delivering capabilities for the U.S. Air Force, scheduled for delivery during the 1st half of calendar year 2026 in support of the Next Generation Gateway (NGG) contract.

The initial focus of the Zscaler IL6 SaaS cloud will be to deliver a fully functional ZPA Secret Cloud. Following the successful deployment of ZPA, additional components of ZIA will be integrated into the Secret Cloud environment, including Cloud Browser Isolation (CBI) and Data Loss Prevention (DLP) capabilities. Additionally, as requirements progress with the Air Force or other Defense customers, we will explore the development of our ZDX capabilities. This phased approach ensures a secure, scalable, and operationally efficient solution to meet the evolving needs of the Department of Defense. Key partnerships include AWS for their accredited and authorized infrastructure, Sequoia for CI/CD pipeline development, and Nooks for secure space solutions. Critical investments include achieving a Facility Clearance License (FCL) and expanding Zscaler's engineering, cloud operations, and compliance teams.

In summary, our objective for calendar year 2025 is to implement a SECRET-capable ZPA control and data plane within the Air Force Cloud One environment, hosted in the AWS Secret Region, by December. Concurrently, we are developing our multi-tenant IL6 ZPA solution to meet the requirements outlined in our CRADA, supporting both testing and IL6 accreditation efforts. As part of this initiative, we are in the process of securing AWS Secret Region accounts through our CRADA partnership and collaborating with industry-leading partners to establish a secure workspace and CI/CD pipeline. Additionally, we plan to issue a Request for Proposal (RFP) for Tier 1 help desk support to ensure seamless operational readiness.

4.2. Zscaler Top Secret (TS) Cloud

Our strategy for developing a TS Cloud will build upon the roadmap established for our Secret Cloud initiative. The partnerships and investments made in the Secret Cloud framework will serve as a strong foundation for the creation of a TS Cloud. This environment will leverage AWS-authorized and accredited infrastructure

to ensure compliance and security standards. Sequoia provides TS emulation environments to support our CI/CD development pipeline, while Nooks offers ICD 705-2 accredited and authorized spaces that Zscaler can utilize as part of this effort.

Zscaler employees will operate and maintain the Top Secret Cloud from authorized locations, including AWS data centers and Nooks office spaces. Zscaler will leverage a partner (e.g., FSI) for delivery and support. Leveraging authorized partners is the most advantageous route due to the complexity of delivering and supporting the Top Secret customer base. FSIs have years of experience and easier access to the requisite talent needed for end-user delivery and support.

Finally, it is important to highlight that the AWS TS Region offers a more feature-rich environment compared to the AWS Secret Region. As a result, the code migration and accreditation process from Secret to TS is anticipated to be significantly less complex than the initial Secret Cloud build. Coupled with our proven expertise in delivering IL6 environments, this positions us to accelerate the development and deployment of a robust TS Cloud solution.

4.2.1. How Zscaler will proceed with a TS Cloud

Our approach for the IL6 cloud was based on finding a sponsor within the Defense Department. Upon securing a sponsor, we were able to initiate the required actions to move forward, including applying for a Facility Clearance (FCL), requesting AWS Secret Region accounts, hiring cleared talent, and acquiring authorized facilities.

The TS cloud will follow a similar approach to the IL6 cloud. The lack of an Intelligence Community (DoD) sponsor serves as the single biggest barrier to entry for Zscaler. Once a sponsor is identified, we can execute the necessary investments. These include modifying our FCL, leveraging ICD 703 accredited facilities with Nooks, uplifting our IL6 code in Sequoia, and applying for AWS TS Region accounts. Sponsorship is especially important for hiring talent, as the DoD currently requires personnel to possess a full-scope polygraph investigation. Without a sponsor, we are unable to hire the necessary staff to operate, maintain, and deliver the cloud.

5. “One Team – One Fight”

The Department of Defense must operate as a unified force to safeguard national security and maintain superiority in an evolving information battlespace. Zscaler embodies the “One Team, One Fight” philosophy by delivering advanced zero trust cloud security solutions that enable mission success. As a FedRAMP–authorized Cloud Security Service Provider (CSP) with certifications from IL2 to IL5 and IL6 (In Process) and trusted by 14 of 15 cabinet–level federal agencies, Zscaler provides scalable, cloud–native architectures that align with the DoD’s priorities of agility, cybersecurity, and cost efficiency.

5.1. Cybersecurity Maturity Model Certification (CMMC) 2.0

Zscaler achieved CMMC Level 2 certification May 2025, reaffirming its role as a trusted partner in securing mission–critical operations for government agencies and contractors. With FedRAMP Moderate, FedRAMP High, and DoD Impact Level 5 accreditations, Zscaler sets the benchmark for meeting government security standards. Its innovative platforms, Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA), simplify legacy network complexity by delivering secure, Zero Trust connectivity for the DoD and Defense Industrial Base (DIB) partners. By mapping its solutions to CMMC 2.0 Level 2 controls, Zscaler streamlines compliance while leveraging its leadership in Secure Web Gateways (SWG) and Security Service Edge (SSE) to guard against evolving threats.

Zscaler CMMC Level 3 Alignment

Zscaler CMMC Level 3 Alignment

Access Control (AC)	Audit & Accountability (AU)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Risk Assesment (RA)	System & Communications Protection (SC)	System & Information Integrity (SI)
AC.L1-3.1.1	AU.L2-3.3.1	AT.L2-3.2.1	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	CA.L2-3.12.1	SC.L1-3.13.1	SI.L1-3.14.1
AC.L1-3.1.2	AU.L2-3.3.2	AT.L2-3.2.2	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	CA.L2-3.12.2	SC.L1-3.13.5	SI.L1-3.14.2
AC.L1-3.1.20	AU.L2-3.3.3	AT.L2-3.2.3	CM.L2-3.4.3	IA. L2-3.5.10	IR.L2-3.6.3	MA.L2-3.7.3	MP.L2-3.8.2	PS.L3-3.9.1e**	PE.L1-3.10.4	CA.L2-3.12.3	SC.L2-3.13.10	SI.L1-3.14.4
AC.L1-3.1.22	AU.L2-3.3.4	AT.L3-3.2.1e**	CM.L2-3.4.4	IA. L2-3.5.11	IR.L3-3.6.1e**	MA.L2-3.7.4	MP.L2-3.8.4	PS.L3-3.9.2e**	PE.L1-3.10.5	CA.L2-3.12.4	SC.L2-3.13.11	SI.L1-3.14.5
AC.L2-3.1.10	AU.L2-3.3.5	AT.L3-3.2.2e**	CM.L2-3.4.5	IA. L2-3.5.3	IR.L3-3.6.2e**	MA. L2-3.7.5	MP.L2-3.8.5		PE.L2-3.10.2	RA.L2-3.11.1	SC.L2-3.13.12	SI.L2-3.14.3
AC.L2-3.1.11	AU.L2-3.3.6		CM.L2-3.4.6	IA. L2-3.5.4		MA.L2-3.7.6	MP.L2-3.8.6		PE.L2-3.10.6	RA.L2-3.11.2	SC.L2-3.13.13	SI.L2-3.14.6
AC.L2-3.1.12	AU.L2-3.3.7		CM.L2-3.4.7	IA. L2-3.5.5			MP.L2-3.8.7			RA.L2-3.11.3	SC.L2-3.13.14	SI.L2-3.14.7
AC.L2-3.1.13	AU.L2-3.3.8		CM.L2-3.4.8	IA.L2-3.5.6			MP.L2-3.8.8			RA.L3-3.11.1e**	SC.L2-3.13.15	SI.L3-3.14.1e**
AC.L2-3.1.14	AU.L2-3.3.9		CM.L2-3.4.9	IA. L2-3.5.7			MP.L2-3.8.9			RA.L3-3.11.2e**	SC.L2-3.13.16	SI.L3-3.14.2e**
AC.L2-3.1.15			CM.L3-3.4.1e**	IA. L2-3.5.8						RA.L3-3.11.3e**	SC.L2-3.13.2	SI.L3-3.14.3e**
AC.L2-3.1.16			CM.L3-3.4.2e**	IA.L2-3.5.9						RA.L3-3.11.4e**	SC.L2-3.13.3	SI.L3-3.14.4e**
AC.L2-3.1.17			CM.L3-3.4.3e**	IA.L3-3.5.1e**						RA.L3-3.11.5e**	SC.L2-3.13.4	SI.L3-3.14.5e**
AC.L2-3.1.18				IA. L3-3.5.2e**						RA.L3-3.11.6e**	SC.L2-3.13.6	SI.L3-3.14.6e**
AC.L2-3.1.19										RA.L3-3.11.7e**	SC.L2-3.13.7	SI.L3-3.14.7e**
AC.L2-3.1.21										RA.L3-3.12.1e**	SC.L2-3.13.8	
AC.L2-3.1.3											SC.L2-3.13.9	
AC.L2-3.1.4											SC.L3-3.13.1e**	
AC.L2-3.1.5											SC.L3-3.13.2e**	
AC.L2-3.1.6											SC.L3-3.13.3e**	
AC.L2-3.1.7											SC.L3-3.13.4e**	
AC.L2-3.1.8											SC.L3-3.13.5e**	
AC.L2-3.1.9												
AC.L3-3.1.1e**												
AC.L3-3.1.2e**												
AC.L3-3.1.3e**												

CMMC 2.0
Level 3

1. 52% Coverage of 145 controls
2. Meets Control: 35
3. Supports Control: 42

ZIA
Level 3 Coverage

1. Meets Control: 9
2. Supports Control: 13

ZPA
Level 3 Coverage

Meets Control: 8

1. Supports Control: 15

Legend:

Meets | Supports | Process | N/A

5.2. Government Efficiency

5.2.1. Transforming DoD Operations for Efficiency and Mission Success

Zscaler can deliver measurable outcomes across the Department of Defenses mission imperatives through its proven zero trust solutions, optimizing cost efficiency, improving cybersecurity resilience, and enhancing workforce readiness. By addressing legacy infrastructure challenges and enabling modern, scalable connectivity, Zscaler empowers the DoD to focus resources on critical mission priorities while achieving significant financial and operational returns. Demonstrable ROI and Operational Impact:

- 85% reduction in cyber exposure: Advanced threat detection, encrypted traffic inspection, and secure access controls.
- 50% faster contractor onboarding: Secure remote access to mission-critical systems.
- 50% lower IT labor costs: Simplified legacy system operations and maintenance.
- Multimillion-dollar annual savings: Transition from costly MPLS circuits to efficient ISP-based connectivity.

5.2.2. Driving Efficiency Through Modernization

Traditional network architectures, such as MPLS and telco-managed solutions, have become a liability for the DoD, undermining operational tempo, cyber resilience, and budget efficiency. These legacy systems slow warfighter effectiveness with inflexible data pathways, expose networks to advanced cyber threats due to limited traffic inspection and outdated controls, and drain resources, costing $90 million annually on MPLS circuits and $50 billion over 15 years on obsolete connectivity frameworks. Zscaler's zero trust approach directly addresses these inefficiencies:

- Legacy system replacement: Eliminate MPLS dependencies and shift to agile, high-speed Internet-based connectivity.
- Enhanced cybersecurity: Inspect encrypted traffic in real time, defend against advanced persistent threats (APTs), and prevent lateral movement.
- Cloud-based scalability: Leverage flexible, software-defined networking that adapts dynamically to evolving operational demands.

Zscaler, in partnership with leading providers like CrowdStrike, Okta, or other Cloud Service Providers, equips the DoD with an integrated security ecosystem that drives mission success. By retiring legacy systems, the DoD achieves immediate cost savings, enhanced cyber resilience, and long-term operational efficiency—positioning itself to navigate an increasingly complex cyber and geopolitical landscape while maximizing return on investment.

6. Glossary Zscaler Terminology

Term	Definition
Zero Trust Architecture (ZTA)	A security model that eliminates implicit trust and continuously verifies every user and device trying to access applications or data, regardless of location.
Zscaler Internet Access (ZIA)	A cloud-delivered security service that protects users from threats while accessing the internet by providing secure web gateway, cloud firewall, data loss prevention, and other integrated services.
Zscaler Private Access (ZPA)	A cloud-delivered Zero Trust solution enabling secure, seamless remote access to internal applications without exposing them to the internet or using a traditional VPN.
Zscaler Digital Experience (ZDX)	A monitoring tool that provides end-to-end visibility into application performance and user experience across Zscaler's Zero Trust platform.
Cloud Security Posture Management (CSPM)	Automated tools and processes designed to identify and remediate configuration vulnerabilities and compliance issues in cloud environments.
Cloud Access Security Broker (CASB)	A service integrated within ZIA that protects data and controls access to SaaS applications, preventing shadow IT and enforcing compliance policies.
Policy Enforcement Node (PEN)	Zscaler's distributed data centers where security policies are enforced in real-time.
Secure Access Service Edge (SASE)	A security framework combining network and security services, such as Zero Trust, SD-WAN, and cloud-delivered security, into a single architecture.
Data Loss Prevention (DLP)	A feature of ZIA that prevents the accidental or intentional leakage of sensitive data by monitoring and controlling data transfers.
Advanced Threat Protection (ATP)	A suite of Zscaler's capabilities, including sandboxing and machine learning, to detect and block sophisticated cyber threats.
Inline Inspection	The process of examining traffic in real-time to identify and block threats or data leakage without impacting performance.
Secure Web Gateway (SWG)	A security solution included in ZIA that inspects all web traffic to enforce compliance policies and block threats.
User-to-Application Segmentation	A core component of ZPA, allowing granular, user-specific access to applications without exposing the entire network.
Machine Learning (ML)	Algorithms within Zscaler's platform that analyze vast amounts of data to detect patterns and identify potential threats in real time.
Cloud Firewall	A service in ZIA that inspects all outbound traffic, providing Layer 7 firewall capabilities to enforce security policies for internet-bound traffic.

Term	Definition
SSL/TLS Inspection	Zscaler's capability to decrypt, inspect, and re-encrypt secure traffic to identify threats hidden within encrypted sessions.
Microsegmentation	A security practice integrated into ZPA that limits access at the application level, ensuring users can only access authorized resources.
Threat Intelligence	A data-driven approach used by Zscaler to analyze and block emerging threats based on real-time global telemetry.
Zscaler App Connector	A lightweight virtual appliance deployed in customer environments that connects user traffic securely to applications via ZPA.
Zscaler Client Connector	A software agent installed on user devices to ensure seamless and secure connectivity to Zscaler services, enforcing Zero Trust policies.
Cloud Sandbox	A Zscaler tool used to analyze and detonate suspicious files in a controlled environment to identify malicious behavior.
Identity Proxy	Zscaler's integration with identity providers (IdPs) to authenticate and authorize users in alignment with Zero Trust policies.
Cloud-Delivered Security	Zscaler's approach to delivering security services entirely from the cloud, eliminating the need for on-premises hardware.
Security Service Edge (SSE)	A subset of SASE, focused specifically on security services such as SWG, CASB, and ZTNA.
Zero Trust Network Access (ZTNA)	A key feature of ZPA, providing secure remote access to applications based on user identity, device posture, and policy compliance.
Private Cloud Controller	Deployed as a software feature, the PCC primary functions are Authentication Redirection of Users, User to PSE Redirection, Log Steaming to SIEM, Policy and Config Sync.

zscaler™

Experience your world, secured.™