



ACCELERATE ZERO TRUST COMPLIANCE

Strengthen federal data security

AWS Zero Trust for Government

In collaboration with



KOVERSE®

okta splunk>





Accelerate Zero Trust compliance with AWS Zero Trust for Government

Federal agencies face pressure to meet the growing challenges of cybersecurity. Alignment to Zero Trust security principles is mandated by [Presidential Executive Order \(EO\) 14028](#): Improving the Nation's Cybersecurity and Office of Management and Budget [Memorandum M-22-09](#). Security modernization requires extensive collaboration, expertise, and investment. Many agencies will rely on partnerships with industry leaders to bolster their security posture and implement proven, modern approaches.

822

U.S. government entities suffered data breaches between 2014 and 2022¹

¹Verizon, [Public Sector Cybersecurity and Threats: What to Watch Out For](#), 2023.

Bolster security with AWS Zero Trust for Government

Secure every user and every access point for maximum threat protection

Strengthen your cyber security defenses to protect against persistent threat actors today and tomorrow. The AWS Zero Trust for Government collaboration helps the US federal government adapt to a changing threat environment, protect sensitive data, optimize resources, and protect the security and privacy of the American people. Experienced industry leaders—AWS, CrowdStrike, Koverse, Okta, Splunk, XQ, and Zscaler—help federal agencies mature Zero Trust capabilities from target to advanced in alignment with the [Department of Defense \(DoD\) Zero Trust strategy guide](#).

Secure your environment and comply with federal mandates using interoperable capabilities

- Integrated cloud services and monitoring—Access a robust, secure, and scalable cloud infrastructure that ensures reliable performance and flexibility.
- Endpoint protection—Enhance your overall system security posture by ensuring only managed, secured, and compliant endpoints can interact with sensitive government data and applications, while safeguarding access based on predefined conditions.
- Identity management and protection—Minimize the risk of unauthorized access, protect against adversary lateral movement, and maintain regulatory compliance by ensuring only authenticated users can access sensitive government data.
- Threat detection—Decrease data loss and damage caused by cyber threats through effective management of security incidents and rapid deployment of incident response measures.
- Security information and event management (SIEM)—Minimize the risk of data breaches while ensuring only authorized users have access to specific resources with granular access controls and traffic routing.

Reduce your compliance burden

Accelerate to Zero Trust maturity goals and deadlines

The AWS Zero Trust for Government collaboration delivers advanced Zero Trust capabilities that are greater than the sum of their parts, speeding up adoption and simplifying implementation to reduce time to value. It provides security solutions aligned to the pillars and cross-cutting capabilities outlined in the DoD Zero Trust Reference Architecture:

Find partners for every stage of your Zero Trust implementation

Users Devices		Network and environments	Applications and workloads	Data
Ensure the right people connect to the right resources at the right time by analyzing and remediating risky or suspicious behavior.	Collect device risk context for continuous trust verification that logs all access activity, analyzing and remediating risky or suspicious behavior.	Enforce authentication and leverage identity as a critical component for policy before granting fast, secure, and reliable access to the internet, SaaS, and private applications—from anywhere.	Enable additional protections to include Zero Trust decision and enforcement points with application delivery methods like proxy technologies and robust cloud infrastructure. These are essential for agencies demanding scalable and secure cloud services.	Meet high federal standards while proactively monitoring and alerting with predictive analytics by deploying capabilities for real-time threat detection and rapid incident response.
				

Visibility and analytics | Automation and orchestration

Enhance visibility, enabling dynamic security policy changes and real-time access decisions. Capture and inspect traffic beyond network telemetry to accurately detect threats, calculate risk scores, and inform authentication policy decisions.	Automate security responses with defined processes and consistent security policy enforcement across all environments that provide proactive command and control.
	





Meet the partners

Experienced industry leaders contribute core strengths

Each partner brings a history of working together and contributes core strengths for seamless, integrated cloud services, endpoint protection, identity management, incident management, and cloud monitoring for end-to-end Zero Trust protection.

Protect against modern threat actors with interoperable solutions



AWS anchors the Zero Trust framework with its robust cloud infrastructure. It provides consistency and sanitization via AWS Snowball, where S3 replicates local storage to a configured region, consistency of command line interface (CLI), and works with familiar images on the device (AMI—Amazon Machine Image). AWS meets federal compliance and data sovereignty requirements.

➤ Visit the [AWS page](#)



CrowdStrike provides visibility for actionable user and device intelligence to evaluate risk and automate access decisions. An agent is installed on AWS Snowball, allowing local threat detection, a Zero Trust assessment score, and monitoring for machine-to-machine activity. CrowdStrike calculates risk scores based on threat status, user behavior, and device context, sharing them with Okta and Zscaler to consider in policy engine and authentication decisions.

➤ Visit the [CrowdStrike page](#)



Okta delivers the modern, cloud-native identity platform that is essential for optimal Zero Trust maturity. Okta's FedRAMP-authorized (and DOD IL4-authorized) solutions ensure the least privilege access with seamless integrations into any application or security technology. It synchronizes with IdP when there is general connectivity and allows users to be provisioned locally on AWS Snowball before leaving for the field. Okta interfaces with CrowdStrike, Splunk, and Zscaler to enable interoperable protection.

➤ Visit the [Okta page](#)



XQ Zero Trust data platform delivers distributed file and structured data encryption across all trusted and untrusted environments. The patented technology suite provides decentralized data rights management and data loss prevention to separate environment and data access. XQ seamlessly interfaces with any technology including CrowdStrike, Splunk, Okta, Snowflake, and Zscaler to enable interoperable protection. With XQ, customers can define roles and permissions to govern data access (RBAC) and add Attribute Based Access Controls (ABAC) including geofencing.

➤ Visit the [XQ page](#)



Splunk SIEM and SOAR capabilities provide real-time threat detection and rapid incident response, meeting high standards for monitoring and incident management. Use Splunk to proactively monitor and alert and use predictive analytics from data captured from Okta's contextual-based authentication and threat/health insights.

➤ Visit the [Splunk page](#)



Securely connect users and devices directly to apps with Zscaler Zero Trust Exchange. The cloud-native solution minimizes the attack surface and eliminates lateral threat movement. It provides inline protection against threats and data loss, while reducing cost and complexity. Reduce risk through shared telemetry and threat intelligence from deep integrations with Okta, CrowdStrike, and AWS.

➤ Visit the [Zscaler page](#)



Koverse Data Platform (KDP) 4.0 introduces attribute-based access controls (ABAC) that allow customers to safely work with complex, sensitive information to power the most demanding analytics, data science, and AI use cases. KDP 4.0 creates a flexible, unified security model across data at the dataset and record level, increasing the value and utilization of all data within an organization.

➤ Visit the [Koverse page](#)



Address the challenges that matter for your mission

Leverage the collaboration tailored for federal agencies

AWS Zero Trust for Government partners help agencies rapidly replace outdated perimeter defenses with continuous protection and advanced authentication.

Mature your architecture with AWS Zero Trust for Government

[Visit the page](#)

