Integrated Security for Zero Trust in the Public Sector

Bring simplicity, speed, and advanced protection to your government cloud environments with a unified solution from AWS, Okta, and Palo Alto Networks

Navigating the complexity of Zero Trust adoption in government agencies

Federal and state agencies are under increasing pressure to strengthen their cybersecurity postures by adopting a modern, Zero Trust approach. But many are still relying on legacy, perimeter-based systems that leave them exposed to sophisticated and state-sponsored cyber threats. Agencies must follow guidance from organizations such as CISA and NIST, while the Department of Defense (DoD), for example, must complete more than 150 security activities while ensuring their vendors meet compliance standards such as FedRAMP and GovRAMP. To succeed, they need integrated, cloud-ready solutions that go beyond siloed tools and deliver automated, end-to-end protection across their environments.

Only 3 out of 23

US federal agencies met their tier three requirements for EO 14028 in 2023.*

A scalable, holistic security and compliance solution from 3 trusted leaders in government IT

US Federal and state agencies can simplify Zero Trust implementation by combining the cloud scalability of Amazon Web Services (AWS), the power of identity from Okta, and the advanced threat protection of Palo Alto Networks. This unified approach delivers robust integrations to help agencies secure cloud infrastructure, manage user identities, and protect networks—while also enhancing operational agility and maintaining mission continuity.

All three providers hold key government compliance requirements, including FedRAMP, GovRAMP, and DoD Cloud Computing Security Requirements Guide (CC SRG) accreditations, making them trusted partners for agencies interested in commercially available technologies. With proven past performance supporting US federal, state, and local governments, AWS, Okta, and Palo Alto Networks offer a reliable path forward for Zero Trust adoption.

* "Federal Agencies Made Progress, but Need to Fully Implement Incident Response Requirements," United States Government Accountability Office, December 2023.

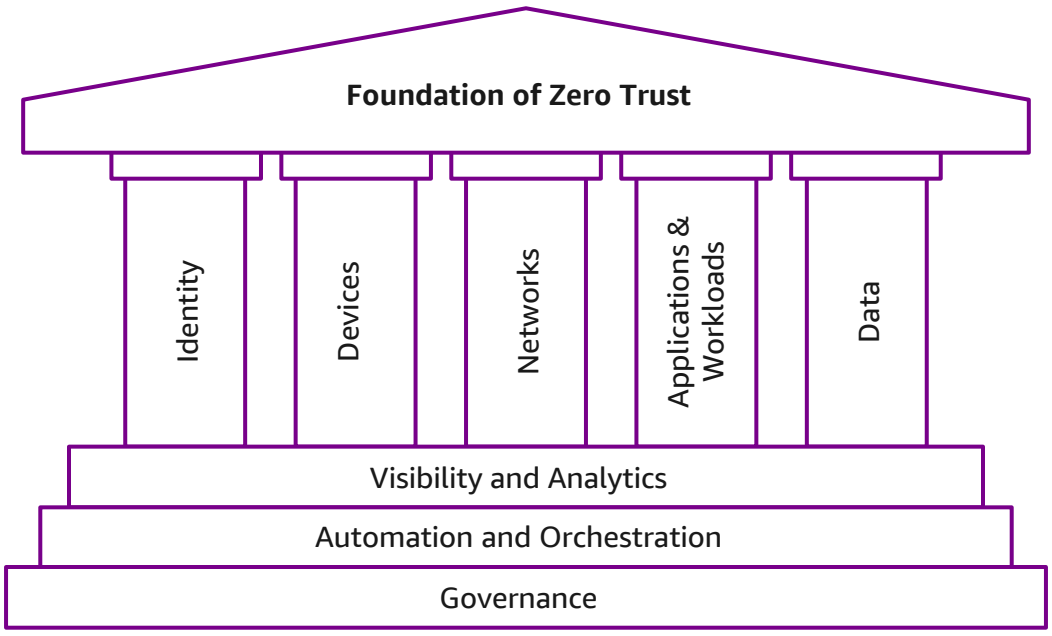
- Gain **cost efficiency**, eliminate tool sprawl, and reduce manual effort by consolidating tools and automating workflows.
- **Maximize staff** without requiring specialized skills thanks to built-in automation, AI-driven insights, and policy-based controls across the AWS, Okta, and Palo Alto Networks platforms.
- **Secure access** and **support mobility** for users everywhere—from managed and unmanaged devices to workloads across hybrid and multi-cloud environments for both employees and contractors.
- **Facilitate compliance** with flexible configuration, data retention, and vulnerability alerts using providers that meet the highest standards for US public sector security and governance.

Comprehensive protection for your mission-critical data

Secure. Simple. Scalable.

Align with the Zero Trust pillars and unify protection across **identity**, **devices**, **networks**, **data**, **applications**, and **workloads** with cloud-native security that leverages automation, AI-driven insights, and user-friendly tools.

- **Applications and workloads security:** Deploy quickly, scale seamlessly, and centralize data across environments with **AWS**.
- **Identity security:** Implement an identity-first, context-aware approach using fine-grained access controls to protect your applications and mission-critical data with **Okta**.
- **Network and device security:** Segment networks, monitor continuously, and prevent breaches with **Palo Alto Networks**.
- **Data security:** Manage the privacy controls of your data, control how your data is used, and encrypt your data with **AWS**.



- FedRAMP and GovRAMP authorization
- Continuous monitoring
- Multi-factor authentication (MFA)
- Real-time threat detection
- Least-privilege access
- Micro-segmentation

Enforce Zero Trust to safeguard government data with AWS GovCloud (US) as the secure cloud for private applications, Okta Adaptive MFA for identity verification, and Palo Alto Networks Prisma Access and Prisma Access Browser to protect access, identities, and all device types. Together, these solutions eliminate implicit trust, enforce least-privilege access, and continuously monitor data to meet US public sector security and compliance needs.

Centralize logs and run real-time analytics by integrating signals from Okta and Palo Alto Networks, as well as data aggregated in Amazon Security Lake. Okta captures identity signals before, during, and after authentication, while Palo Alto Networks Cortex detects device posture changes and triggers policy updates. Together, they facilitate continuous monitoring and automated enforcement.

Unify visibility to detect threats and correlate identity events with cloud activity across environments by aggregating security logs from AWS services, identity data from Okta, and security insights from Palo Alto Networks Prisma Cloud into FedRAMP-authorized Amazon Security Lake for centralized analysis.

Secure government software factories and CI/CD pipelines on AWS by enforcing strong identity verification and least-privilege access controls. Okta manages developer authentication with single sign-on (SSO) and MFA while Palo Alto Networks delivers Container- and Infrastructure-as-Code scanning—ensuring access to AWS resources remains compliant and authorized throughout the software supply chain.

Take the easiest path to Zero Trust with AWS, Okta, and Palo Alto Networks

Ready to adopt Zero Trust and meet mandates by deadline? Get started by visiting Okta and Palo Alto Networks in AWS Marketplace.