Protect public sector workloads through identity-driven security

Public sector security is entering a new era

AI-powered threats can exploit compromised credentials or devices in seconds. AI can also be used to scale phishing and evade traditional security systems. Public sector organizations need integrated identity, endpoint, and access security to continuously assess risk and protect mission-critical workloads on Amazon Web Services (AWS).

Move from siloed detection to coordinated response with AWS, CrowdStrike, Okta, and Zscaler

Anchor access decisions in identity with **Okta**

Evaluate and control access at the identity layer—the most common starting point for modern attacks—by continuously assessing risk and acting on real-time signals from endpoint and network layers.

Surface endpoint and workload risk with **CrowdStrike**

Detect and confirm suspicious activity across cloud, virtual and physical endpoints in order to provide critical context to downstream security controls.

Apply Zero Trust access enforcement with **Zscaler**

Enforce security policies with real-time context, enabling fast, secure connections between users, devices, and applications while applying Zero Trust access principles to prevent threats and data loss.

The Shared Signals Framework (SSF) powers coordinated security

SSF is an OpenID Foundation standard that enables CrowdStrike, Okta, and Zscaler to securely exchange real-time threat and risk signals. This shared context drives automated, adaptive responses and strengthens protection for applications and workloads running on AWS, including AI-powered and agentic workloads.

Coordinate protection for public sector cloud environments

Modernize hybrid environments without increasing cost or fragility

As public sector organizations modernize hybrid environments spanning on-prem, cloud, and SaaS, they must protect mission-critical services without adding cost or complexity. That includes emerging AI-powered services and workloads running alongside traditional systems. By anchoring access in identity, continuously validating endpoint posture, and replacing legacy VPNs with Zero Trust connectivity, agencies can strengthen security while maintaining operational continuity. AWS, CrowdStrike, Okta, and Zscaler integrate to deliver cloud infrastructure, real-time device intelligence, and identity-driven access controls that reduce tool sprawl, simplify operations, and enable secure, resilient modernization.

Respond to AI-driven threats through shared signals and automated control

AI-assisted attacks increasingly target public sector organizations by exploiting compromised identities and trusted access paths rather than perimeter gaps. As agencies introduce AI into mission workflows, security teams need coordinated, automated controls that move as fast as emerging threats. The integrated solution unifies cloud analytics, real-time endpoint intelligence, continuous identity risk assessment, and application-layer enforcement to share signals and trigger rapid containment. The result is faster detection of identity-based threats, reduced manual triage, and stronger protection for sensitive data and GenAI-enabled applications without slowing mission delivery.

Meet Zero Trust mandates and compliance deadlines

With fixed deadlines tied to federal Zero Trust mandates and evolving requirements such as DoW Target Level and CMMC, public sector organizations must demonstrate measurable progress across identity, device posture, network access, and continuous monitoring. Siloed controls make it difficult to validate enforcement, produce audit-ready evidence, and sustain compliance as systems evolve, especially as AI systems introduce new data access patterns. The integrated solution aligns identity, endpoint telemetry, network inspection, and cloud governance through coordinated controls and shared signals, enabling consistent enforcement across hybrid infrastructure. This approach shifts agencies from point-in-time assessments to continuous compliance, reduces manual audit preparation, and strengthens visibility and control over access to sensitive and AI-enabled applications.

Okta secures AI with trusted partners

When it comes to AI, identity matters. Together with AWS, CrowdStrike, and Zscaler, Okta secures AI by governing agents, workloads, and users through identity-driven policies and shared real-time risk intelligence.
For public sector organizations, that means maintaining trust as AI adoption accelerates. The result is scalable AI innovation with security built in.

Learn more about unified security for cloud and AI-powered environments with best-of-breed providers.

About Okta

Okta, Inc. is The World's Identity Company™. We secure AI, machine, and human identity so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to protect their AI agents, users, employees, and partners while driving security, efficiencies, and innovation. Learn why the world's leading brands trust Okta for authentication, authorization, and more at **okta.com.**