Solution Brief March 2026

Protect public sector workloads through identity-driven and endpoint security

Public sector security is entering a new AI era

AI-powered threats can exploit compromised credentials or devices in seconds. At the same time, agencies are adopting AI-enabled services and digital modernization initiatives that introduce new identities and access patterns. Public sector organizations need integrated identity and endpoint security to continuously assess risk and protect mission-critical workloads on Amazon Web Services (AWS).

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

Anchor access decisions in identity with Okta

Continuously assess identity risk using Okta Identity Threat Protection, informed by real-time endpoint signals from CrowdStrike. Access adapts dynamically as risk changes, helping public sector organizations prevent compromised users from reaching sensitive systems and AWS-hosted mission workloads while advancing Zero Trust maturity goals.

Surface endpoint and workload risk with CrowdStrike

Detect and confirm suspicious activity across cloud, virtual, and physical endpoints supporting public sector operations. CrowdStrike Falcon shares device posture and threat intelligence with Okta to provide critical context for adaptive access decisions and stronger protection of AWS environments.

Protect mission systems with coordinated enforcement

By combining identity-driven access controls with endpoint risk insights, public sector organizations strengthen protection for applications and data running on AWS. Detection in one layer immediately informs enforcement in another, reducing lateral movement, limiting blast radius, and supporting continuous verification across hybrid, multi-cloud, and AI-enabled environments.

The Shared Signals Framework (SSF) powers coordinated security

SSF is an OpenID Foundation standard that enables Okta and CrowdStrike 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 mission-critical services.

Coordinate protection for public sector cloud environments

Secure cloud modernization initiatives

As public sector organizations migrate legacy systems and citizen-facing services to AWS, modernization efforts must align with Zero Trust mandates and compliance frameworks. By anchoring access decisions in identity and continuously validating endpoint posture, public sector organizations can protect users and regulated workloads during cloud transitions. CrowdStrike and Okta integrate to deliver adaptive access controls and real-time endpoint intelligence that strengthen protection for AWS-hosted systems and AI-enabled services without disrupting service delivery.

Enforce continuous Zero Trust verification for high-impact systems

Public sector organizations operate critical systems subject to evolving cybersecurity mandates and data protection requirements. Zero Trust requires continuous verification across identity and device layers rather than implicit trust.
CrowdStrike shares real-time endpoint risk signals with Okta Identity Threat Protection, enabling public sector organizations to dynamically adjust access to sensitive AWS workloads as risk changes. This identity-driven enforcement model helps prevent compromised credentials or unmanaged devices from reaching high-impact systems and regulated data. It also strengthens governance over emerging AI-enabled applications that process sensitive public sector data.

Strengthen cyber resilience and mission continuity

Government and public service organizations must contain threats quickly to maintain essential services and public trust. By integrating identity and endpoint intelligence, suspicious endpoint activity can trigger adaptive access controls, session revocation, or automated containment across AWS environments. This coordinated response reduces dwell time, limits lateral movement, and accelerates investigation — strengthening resilience against sophisticated and AI-driven attacks targeting mission systems.

Okta secures AI with trusted partners

When it comes to AI, identity matters. Together with AWS and CrowdStrike, Okta secures AI by governing agents, workloads, and users through identity-driven policies and shared real-time risk intelligence.
The result is scalable AI innovation with security built in.

Learn more on how to protect cloud and AI-powered environments with identity and endpoint security.