Solution Brief

Unify identity and application access across public sector cloud environments

Public sector security is entering a new AI era

AI-assisted threats operate at machine speed, increasingly exploiting compromised identities and trusted access paths rather than traditional perimeters. At the same time, public sector organizations operate highly hybrid environments where on-prem systems, cloud services, and SaaS platforms coexist.

Public sector organizations need unified, identity-centered security that continuously evaluates risk and securely connects users directly to applications running on Amazon Web Services (AWS), including emerging AI-powered services and data environments.

Move from siloed access controls to coordinated enforcement

Establish identity as the control plane with Okta

Evaluate and control access at the identity layer—the most common starting point for modern attacks—by continuously assessing risk and enforcing context-aware authentication and authorization.

Okta centralizes workforce identity and applies consistent Zero Trust access policies across SaaS, cloud, and on-prem applications running on AWS.

The Shared Signals Framework (SSF) powers coordinated security

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

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.

Connect users directly to applications with Zscaler

Securely connect users and devices directly to applications rather than networks through the Zscaler Zero Trust Exchange. Applications sit behind the exchange, making them invisible to threats and reducing the attack surface. Inline inspection and data protection policies are applied as access is granted, preventing lateral movement and limiting exposure of sensitive data across distributed public sector environments.

Protect workloads on a secure AWS foundation

Run applications and data on a secure, scalable cloud foundation that supports unified Zero Trust architectures. AWS provides encryption in transit and at rest, centralized governance, and continuous visibility across cloud workloads. Public sector organizations modernize infrastructure while maintaining resilience and policy control.

Support public sector modernization, AI threat response, and compliance requirements

Modernize hybrid environments without increasing cost or fragility

Public sector organizations operate highly hybrid environments where on-prem systems, cloud services, and SaaS platforms coexist. As public sector organizations modernize workloads on AWS, legacy VPN-based access increases complexity and expands the attack surface. Okta establishes identity as the control plane, while Zscaler connects users directly to applications instead of networks. Running on a secure, scalable AWS cloud foundation, this model reduces infrastructure sprawl and preserves operational resilience as agencies expand digital and AI-powered services.

Respond to AI-driven identity abuse with application-level control

AI-assisted threats increasingly exploit compromised identities and trusted access paths. Security must continuously evaluate risk and constrain access as conditions change. Okta assesses identity risk in real time and enforces context-aware authentication. Zscaler applies inline inspection and connects users directly to applications, reducing lateral movement and limiting data exposure. AWS provides centralized visibility across cloud workloads, strengthening control as AI-powered services expand.

Meet Zero Trust mandates with enforceable, measurable controls

Federal Zero Trust requirements demand demonstrable enforcement across identity, access, and cloud environments. When controls operate independently, validation becomes difficult to sustain. Okta centralizes workforce identity and applies consistent access policies. Zscaler enforces application-level connectivity and inspection. AWS delivers encryption, governance, and workload visibility. Together, these coordinated controls support continuous verification and measurable Zero Trust progress across cloud and AI-powered environments without increasing operational burden.

Okta secures AI with trusted partners

When it comes to AI, identity matters. Together with AWS and Zscaler, 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 advance Zero Trust with unified identity and application security on AWS.