Solution Brief March 2026

Combine identity and endpoint security across cloud and AI-powered environments

AI is reshaping the threat landscape

AI-powered attacks can move across identities, endpoints, and cloud workloads quickly. To keep pace with risk, organizations running on Amazon Web Services (AWS) need coordinated security that connects identity and endpoint intelligence in real time.This is especially true as AI-powered applications and automated workflows expand across cloud environments.

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 prevent compromised users from accessing AWS resources.

Surface endpoint and workload risk with CrowdStrike

Detect and confirm suspicious activity across cloud, virtual, and physical endpoints. CrowdStrike Falcon shares device posture and threat intelligence with Okta to provide critical context for adaptive access decisions and workload protection on AWS.

Protect AWS workloads with coordinated enforcement

By combining identity-driven access controls with endpoint risk insights, organizations strengthen protection for applications and workloads running on AWS. Detection in one layer immediately influences enforcement in another, reducing lateral movement and limiting blast radius across environments across 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.

okta aws CROWDSTRIKE

Modernize security with an integrated ecosystem

Migrate and innovate securely

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.

Prevent threats with an identity-driven Zero Trust approach

Zero Trust works when identity and endpoint risk are evaluated together. CrowdStrike shares real-time endpoint risk insights with Okta Identity Threat Protection, enabling continuous identity risk assessment and context-aware access enforcement. As risk changes, access adapts dynamically—helping prevent compromised credentials or devices from reaching sensitive AWS workloads and limiting lateral movement across environments. This approach also strengthens identity governance as AI-enabled applications introduce new users, services, and machine identities into the environment.

Accelerate detection and response across AWS

Security teams often struggle to correlate identity and endpoint alerts across tools. By integrating Okta and CrowdStrike, detection in one layer immediately informs enforcement in another. High-risk activity can trigger step-up authentication, session revocation, or automated containment actions, improving response times and reducing the blast radius of attacks targeting AWS and AI-powered workloads.

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.