Solution Brief

Unify cloud-native security across identity, applications, and cloud

Identity-based attacks operate at machine speed

Modern attacks increasingly exploit compromised identities and trusted access paths rather than traditional perimeter defenses—and AI amplifies the scale and precision of these tactics.

Organizations running on Amazon Web Services (AWS) need unified, cloud-native security that connects identity and application access in real time. Coordinated controls across identity, connectivity, and cloud environments reduce attack surface and protect modern workloads, human and AI alike, without adding complexity.

Coordinate identity and application controls to reduce attack surface with Okta, Zscaler, and AWS

Anchor access decisions in identity with Okta

Identity is the most common starting point for modern attacks. Okta evaluates and controls access at the identity layer by continuously assessing risk and enforcing context-aware authentication and authorization.

By establishing identity as the control plane, Okta applies consistent 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 agentic workloads.

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

Trusted access paths are increasingly exploited. Zscaler securely connects users and devices directly to applications rather than networks, eliminating implicit trust. Applications sit behind the Zero Trust Exchange, making them invisible to threats and reducing the attack surface. Inline inspection and data protection apply as access is granted, limiting lateral movement and protecting sensitive data.

Run workloads on a secure AWS cloud foundation

Applications and data run on a secure, scalable cloud foundation that supports unified security architectures. AWS provides encryption in transit and at rest, centralized governance, and continuous visibility across workloads. These controls preserve resilience and policy enforcement as environments modernize and expand.

Modernize with unified security and coordinated control

Migrate and innovate securely

Modernization accelerates cloud adoption, but legacy network-based access expands complexity and exposure. As applications move to AWS, security must follow the workload, including AI-powered applications and services. By anchoring access decisions in identity and connecting users directly to applications instead of networks, organizations modernize without expanding implicit trust. Coordinated controls across identity, application access, and cloud infrastructure reduce attack surface while preserving visibility and operational agility.

Prevent identity-based threats with coordinated access controls

Modern attacks exploit compromised identities and trusted access paths. Security must evaluate risk continuously and adapt access as conditions change. Context-aware authentication from Okta, combined with application-level enforcement and inline inspection from Zscaler, constrains access before misuse spreads, protecting both users and AI-driven workloads. Running on AWS, this coordinated model shrinks attack surface, limits lateral movement, and strengthens protection across hybrid and cloud environments.

Act on risk faster with coordinated enforcement

Fragmented tools slow response when identity risk changes. When identity and application controls operate together, shifts in risk immediately influence access decisions. High-risk behavior can trigger step-up authentication or restricted application access, reducing exposure in real time. Centralized visibility across AWS workloads and AI-powered services supports faster containment while simplifying security operations.

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.
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.