okta aws CROWDSTRIKE zscaler

Unify your cloud-native security

AI is reshaping the threat landscape

AI amplifies the scale and speed of modern attacks across environments. At the same time, organizations are deploying AI-powered applications that introduce new identities and permissions. But most security stacks continue to operate in silos that limit cross-platform visibility and slow security responses.

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.

Modernize security with an integrated ecosystem

Migrate and innovate securely

As organizations migrate on-premises apps to AWS, security must move with the workload. By anchoring access decisions in identity, validating device and workload trust continuously, and connecting users directly to applications, organizations can form a unified security fabric across hybrid and cloud environments. AWS, CrowdStrike, Okta, and Zscaler allow teams to modernize faster without expanding risk, while maintaining visibility and control over how users interact with AI-powered applications and sensitive data.

Prevent threats with a unified Zero Trust architecture

Zero Trust works when identity, device, network, and cloud signals are evaluated together rather than in isolation. CrowdStrike and Zscaler share real-time risk signals with Okta Identity Threat Protection, enabling continuous identity risk assessment and context-aware access enforcement. Access adapts dynamically as risk changes, strengthening protection for applications and workloads running on AWS—including AI agents—while limiting lateral movement and reducing blast radius.

React faster with coordinated security operations

Security operations break down when teams are flooded with alerts from multiple sources (leading to alert fatigue), but lack the ability to quickly prioritize and act decisively. By operating from a shared security context, our integrated solution turns detection into direct action. Risk signals immediately influence access, connectivity, and workload behavior without manual handoffs between tools. The result is shared intelligence and automated enforcement without operational drag.

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.**