**Solution Brief** April 2026

# Unify cloud-native security for financial services

## With AWS, CrowdStrike, Okta, and Zscaler

### AI is reshaping the threat landscape for financial institutions

AI amplifies the scale and speed of modern attacks across environments. Financial institutions face increasing threats, such as credential misuse and fraud targeting digital platforms and internal systems. 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 and financial fraud—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 supporting financial operations 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 help prevent threats, help protect sensitive financial data, and help reduce lateral movement.

### 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.

okta CROWDSTRIKE zscaler™ aws

# Strengthen financial security with an integrated ecosystem

## Modernize securely

As financial institutions modernize legacy systems and migrate workloads to AWS, security must move with the platform. 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 clear visibility into access across financial systems and applications.

## Protect against fraud and ransomware

Financial institutions operate in an environment where fraud and ransomware increasingly exploit legitimate credentials and excessive privileges. Continuous identity verification and adaptive access controls help reduce credential misuse and prevent attackers from moving laterally across financial systems. By sharing real-time signals across identity, endpoint, and network layers, AWS, CrowdStrike, Okta, and Zscaler allow access to adapt dynamically as risk changes—strengthening protection for critical financial applications and workloads running on AWS.

## Secure sensitive financial data across environments

Financial institutions manage highly sensitive data across applications, environments, and devices. By unifying identity, endpoints, telemetry, connectivity controls, and cloud visibility, AWS, CrowdStrike, Okta, and Zscaler help organizations maintain consistent visibility into who accessed sensitive financial data, how it was used, and where it moved. The result is stronger protection for regulated data, improved compliance readiness, and reduced risk of data exposure.

## 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 for financial services with security built in.

**Learn more about unified security for financial institutions with best-of-breed providers**