Modernize your security with Zero Trust

Integrated solutions from industry leaders deliver end-to-end security and an exceptional user experience

In collaboration with

CROWDSTRIKE

okta

zscaler

As people work from anywhere, on any device, and applications move from on-premises to the cloud, maintaining the user experience has never been more important. Legacy security products do not support modern businesses and the challenges they face, including:

Increased business and security risks

Increased cost and complexity

Poor user experience

The Zero Trust framework

Zero Trust is more than the sum of user identity, segmentation, and secure access. It's a security strategy upon which to build a complete security ecosystem. Zero Trust is founded on the principle of least-privilege and the idea that no user, device, workload, or app is inherently trustworthy. It is distinct from a "castle and moat" architecture, which trusts anything inside by default.

Security is a shared responsibility between Amazon Web Services (AWS) and the customer. AWS is responsible for "Security OF the Cloud" while the customer is responsible for "Security IN the Cloud."

Learn more

Deploy Zero Trust with AWS, CrowdStrike, Okta, and Zscaler

Cloud-native Zero Trust built on industry-leading solutions from AWS, CrowdStrike, Okta, and Zscaler delivers a superior user experience and faster deployment. Through an integrated solution architecture, you gain end-to-end visibility for faster cross-platform threat detection, protection, and remediation, along with enhanced productivity. You can work with a team of partners committed to helping you successfully implement end-to-end Zero Trust and maximize your return on investment.

Integrated solutions from industry leaders provide:

- Reduced risk, lower costs/complexity, and an exceptional user experience
- Integrated user authentication and provisioning for faster access
- Continual assessment of device posture using Falcon Zero Trust Assessment (ZTA) score
- Automated workflows with extended detection and response (XDR)-enabled sharing
- Shared zero-day threat intelligence for faster detection and remediation

In collaboration with: CROWDSTRIKE okta zscaler

Achieve integrated Zero Trust with recognized leaders

Identity access and management with Okta

A Leader in the 2022 Gartner® Magic Quadrant™ for Access Management, Okta centralizes identity management with a context-based policy engine to authenticate users and manage identities that prevent unauthorized access.

Secure connectivity to applications with Zscaler

A Leader in the 2023 Gartner® Magic Quadrant™ for Security Service Edge (SSE), Zscaler prevents cyber threats and data loss while providing users with fast, reliable Zero Trust connectivity to applications, along with workload security using any network.

Endpoint protection with CrowdStrike

A Leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms, CrowdStrike is relentlessly focused on building technologies to help organizations where they need it most: Detecting and responding to security threats while also protecting the most critical areas of risk – endpoints, cloud workloads, identity, and data.

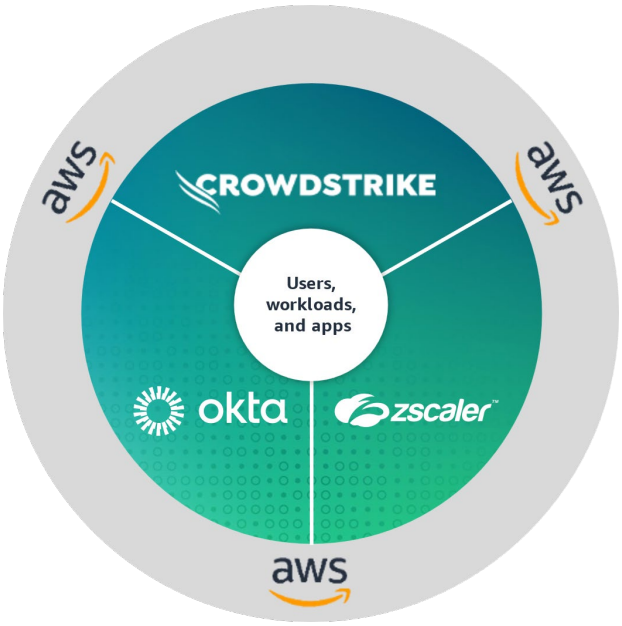
Cloud infrastructure with AWS

A Leader in the 2022 Gartner® Magic Quadrant™ Cloud Infrastructure & Platform Services (CIPS), AWS has a global network of availability zones and robust management tools to enable businesses to easily deploy, manage, and scale application services with high security.

okta

Identity

- User/policy mgmt
- Authentication/MFA
- Authorization
- Device context



zscaler

Connectivity

- Security policy enforcement
- Attack surface reduction
- Threat prevention/SSE
- Data protection

CROWDSTRIKE

Endpoint

- EDR/XDR
- Threat prevention
- Risk-based access
- Device & user context

aws

Secure cloud

- Scalability
- Resilience
- Apps & workloads

In collaboration with: CROWDSTRIKE okta zscaler

Integrated solution use cases

Accelerate application migration to AWS

Legacy security products were not built for the cloud, making the migration of on-premises applications slow, complex, and costly. Accelerate your migration by quickly discovering the applications to protect, applying consistent security throughout the migration process, and directly connecting users to applications for faster performance and a positive experience.

Provide Zero Trust application access

The modern workforce requires access to business applications in AWS services like Amazon S3 from any location, using any device, at any time. Legacy security products (VPNs and firewalls) expand the attack surface, enable threats to move laterally, and provide a poor user experience. Modernize your security and reduce the attack surface by connecting users directly to applications without VPNs for faster access and consistent security.

Secure AWS workloads

As workloads and applications move to the cloud, the risks from misconfigurations, inconsistent security, and threats moving laterally are a major concern. Implement modern security, built for the cloud that proactively identifies and resolves vulnerabilities, eliminates lateral threat movement, and applies the principle of least privilege to protect critical workloads on AWS.

Protect your data

As users access data across a variety of devices from anywhere, any time, the risk of a security breach and data loss increases. Implement a holistic approach to data protection that includes fast, complete inspection of traffic inline and at rest–even if it's encrypted–to keep sensitive data safe and prevent data loss.

Delivering value to our joint customers

"Mercury Financial is benefiting from Zscaler integrations with AWS as well as leveraging benefits from integrations with other leading AWS partner solutions, such as CrowdStrike, Okta…"

Read case study

Jason Smola
Enterprise Security and Infrastructure Architect, Mercury Financial

Learn more about our solutions.

Visit provenzerotrust.com