Achieve an integrated end-to-end Zero Trust architecture with recognized leaders

In collaboration with

CROWDSTRIKE

okta

zscaler™

Table of contents

aws

Stay ahead of evolving risks

Don't let security threats – or siloed solutions – slow you down

With applications migrating to Amazon Web Services (AWS) and employees working from anywhere, using any device, maintaining the right level of security and performance is critical; but it can present multiple challenges. The need for Zero Trust is rapidly increasing with the worldwide Zero Trust Network Access market set to grow at a CAGR of 30.3% through 2026.[1]

Key security challenges

- **Expanding attack surface:** Applications and workloads are moving to the cloud, and workers need access from any device and location.
- **Complex access management:** Lack of real-time threat assessment slows down access decisions.
- **Evolving threat landscapes:** Threat actors are sophisticated and constantly devising new attack strategies, malware, and zero-day threats.

Threat actors exploit multiple attack vectors:

- Identity and access
- Endpoint devices
- Networks
- Applications and workloads
- Data

of adversaries use one or multiple forms of evasion to bypass detection.[2]

[1]IDC, Worldwide Zero Trust Network Access Forecast, 2022–2026: Transforming Network Security, Traversing Convergence - US49100522, June 2022.
[2] CrowdStrike, Modern Adversaries and Evasion Techniques, 2023.

Zero Trust architecture competitive advantages

In modern, distributed, connect-from-anywhere organizations, enhanced security controls are crucial. As enterprises face the challenges of a rapidly evolving threat landscape, supporting work-from-anywhere, and migrating workloads to the cloud, a Zero Trust framework is required.

Zero Trust is not a single solution; it is more than the sum of user identity, segmentation, and secure access. It's a strategy upon which to build a complete security ecosystem. Zero Trust is founded on the principle of least privilege access and the idea that no user, workload, application, or device is inherently trustworthy. It is distinct from a "castle and moat" architecture, which trusts anything inside by default.

To implement a Zero Trust architecture, multiple solutions need to work together to enforce fine-grained rules and policies. Amazon Web Services (AWS) and AWS partners – CrowdStrike, Okta, and Zscaler – offer an integrated, cloud-native, holistic security solution. It is a best-of-breed collaboration to enable your organization's successful transition to Zero Trust and stay ahead of evolving, known and unknown threats.

Securing every user, every device, and every connection

okta

Identity

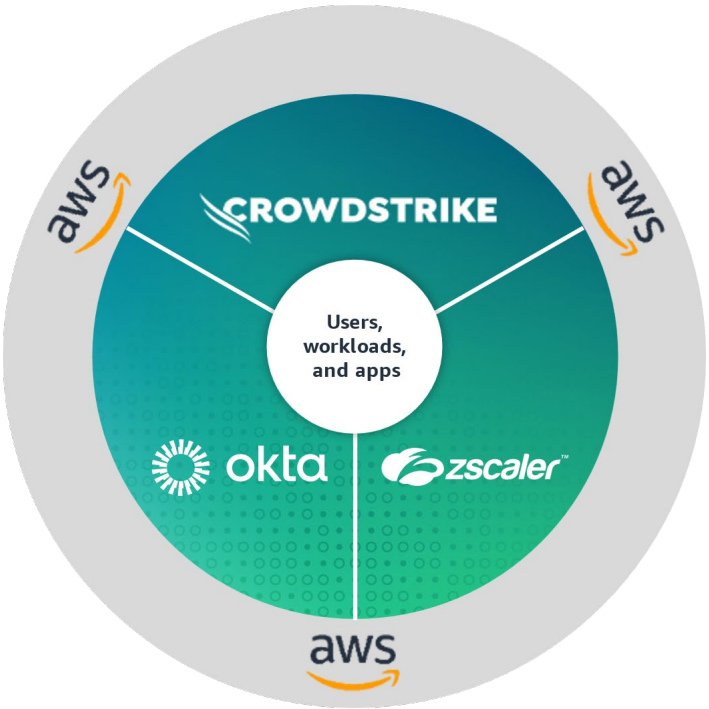
- User/policy mgmt
- Authentication/MFA
- Authorization
- Device context

CROWDSTRIKE

Endpoint

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

aws



zscaler

Connectivity

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

aws

Secure cloud

- Scalability
- Resilience
- Apps & workloads

Key components of Zero Trust

Identity and access management

okta

Authenticate users and manage identities to prevent unauthorized resource access

- Assess the risk of users and authorize fast, context-aware access with Okta and CrowdStrike Falcon
- Automate access and authenticate users with Okta's context-based policy engine linked to AWS IAM Identity Center
- Ingest and view Okta identity and authentication log data within CrowdStrike Falcon Insight XDR, then trigger response actions automatically
- Synchronize users and security groups between Okta and Zscaler in near-real time to automatically update, manage, and remove access to company resources based on role changes

Secure connectivity to applications

zscaler™

Prevent cyber threats and data loss while providing users with fast, reliable Zero Trust connectivity to apps, along with workload security

- Securely connect users and devices directly to apps with Zscaler Zero Trust Exchange, which acts as an intelligent switchboard
- Cloud-native solution minimizes the attack surface and eliminates lateral threat movement
- Provides inline protection against threats and data loss, while reducing the cost and complexity of legacy products
- 150+ points of presence globally, optimizing traffic flow to ensure the best user experience
- Reduce risk through shared telemetry and threat intelligence from deep integrations with Okta, CrowdStrike, and AWS

Endpoint protection

CROWDSTRIKE

Protect against security threats in virtual and physical assets across endpoints, cloud workloads, identity, and data

- Verify endpoint status before allowing access with CrowdStrike and Okta
- Assess and protect virtual and physical assets with automatic cross-platform workflow between CrowdStrike Falcon and Zscaler ZTE
- Enable run-time protection with CrowdStrike sensors on Amazon EC2, Amazon EKS, AWS Fargate, and AWS Lambda
- Respond and remediate incidents within DevOps toolsets using CrowdStrike Falcon Cloud Security
- Eliminate modern threats with deep integrations between Okta, Zscaler, and AWS

Cloud infrastructure

aws

The most secure cloud infrastructure

- Build, run, and scale your applications on infrastructure architected to be the most secure cloud computing environment available today
- Move fast and stay secure by confidently integrating and automating security into every part of your organization
- Innovate with a wide portfolio of security services and partner solutions to help achieve end-to-end security for your organization

aws

Security is a shared responsibility

Security is a shared responsibility between AWS and the customer. AWS is responsible for "Security OF the Cloud" while the customer is responsible for "Security IN the Cloud." AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. Customer organizations are responsible for securing their workloads and applications in the cloud. You can work with a team of partners committed to helping you successfully implement end-to-end Zero Trust:

Accelerate application migration to AWS

Legacy security products were not built for the cloud, making the migration of on-prem 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 is a major concern. Implement modern security, built for the cloud that proactively identifies and resolves vulnerabilities, eliminates lateral threat movement, and applies the principles of least privileged access 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.

"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

aws

Trusted, industry-leading solutions for end-to-end Zero Trust

- **AWS named a Leader in the 2022 Gartner® Cloud Infrastructure & Platform Services (CIPS) Magic Quadrant™** for the 12th consecutive year. Read more
- **CrowdStrike named a Leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms** for third consecutive year. Read more
- **Okta named a Leader in 2022 Gartner® Magic Quadrant™ for Access Management** for sixth consecutive year. Read more
- **Zscaler named a Leader in the 2023 Gartner® Magic Quadrant™ for Security Service Edge** (SSE). Read more

Reduce risk, cost, and complexity by deploying integrated Zero Trust.

Learn more

Amazon Web Services has been the world's most comprehensive and broadly adopted cloud. AWS has been continually expanding its services to support virtually any workload, and it now has more than 240 fully featured services for compute, storage, databases, networking, analytics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 102 Availability Zones within 32 geographic regions, with announced plans for 15 more Availability Zones and five more AWS Regions in Canada, Germany, Malaysia, New Zealand, and Thailand. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs. Learn more

CrowdStrike is a global cybersecurity leader that has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity, and data. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value. Learn more

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more

An AWS Advanced Tier Software Partner, Zscaler has been a leader in Zero Trust security for over a decade. Zscaler accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 points of presence (PoPs) globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more