okta CROWDSTRIKE zscaler™

Zero Trust in Action: Customer Stories from Okta, CrowdStrike, and Zscaler

Rate

Mortgage and lending fintech leader with 850+ branches across 50 states

Infrastructure consolidation around zero trust

>2 million
homeowners and their financial data

500+
applications under single sign-on, passwordless authentication

2–3x
faster user access to apps

Automated provisioning and deprovisioning of users and groups

> Having one Identity platform to rule them all helps keep our costs low while still providing that great experience.
>
> **Darin Hurd, EVP & CISO, Rate Companies**

Security gaps and remote work expand the attack surface and increase complexity.

Rate Companies saw that its IT architecture of three on-premises data centers, legacy VPNs and firewalls, and three cloud platforms expanded the attack surface, made it more vulnerable to cyber risk, and increased complexity. Furthermore, the organization transitioned from on-site work to a hybrid environment, with loan officers constantly on the go, working from one of 850+ branch offices, customer sites, or real estate firms.

Legacy tools created high operational costs and integration challenges.

Rate Companies made a strategic decision to adopt a zero trust architecture. Three considerations drove vendor selection: partnering with an innovative industry leader, implementing a unified platform instead of point products, and rapid time-to-value. The integrations between AWS, CrowdStrike, Okta and Zscaler met all stated criteria.

Secure internet and SaaS access from the cloud, giving users least-privileged access.

To consolidate Rate's infrastructure around zero trust, the company integrated Zscaler with AWS and Okta. With Okta platform integrations, Zscaler securely connects users directly to applications and workloads on AWS—without having to pass through a data center or route users to the corporate network. This minimizes the attack surface, eliminates the risk of lateral threat movement, protects data, and provides a low-latency user experience.

Seamless integrations reduce security risk and boost user satisfaction.

The Okta-Zscaler integration provides automated provisioning and deprovisioning of users and groups via the system for cross-domain identity management (SCIM) integration, to ensure real-time enforcement of zero trust policies. Security Assertion Markup Language (SAML) integration has improved the user login experience, providing seamless authentication. Users log in once a week with passwordless authentication, leading to less friction when users need to access the 500+ applications.

With the CrowdStrike-Zscaler integration, threat intelligence enrichment flows in both directions, bringing increased awareness to device activity. It monitors indicators of compromise, blocks lateral movement of threats, and enforces secure access policies more effectively based on changing risk context of the device. Zscaler also shares network telemetry, including logs from ZIA and ZPA with CrowdStrike, enabling security teams to view and analyze log data, detect anomalies, identify issues, and accelerate investigations using a pre-built dashboard.

ciena

Global leader in high-speed connectivity

Double protected with an improved user experience

>10,000
employee, contractor, and 3rd party identities and their devices accessing over 500 applications

~70
locations in over 35 countries

50%
reduction in costs and support tickets

> “The integrations enable us to react more quickly and effectively to any type of disruption or threat, and the sharing of these signals is a critical success factor for us.

Ed DeGrange, Sr. Director, Security Architecture and Engineering

Digital transformation and need to support hybrid work models.

With over 70 company locations across 35 countries, plus an expanded hybrid work approach, Ciena was concerned about their growing attack surface. The company adopted a zero trust model as part of network upgrades and moving to the cloud, providing the ability to identify, authenticate, and authorize users as well as devices, and continually monitor activity.

High operational complexity and slowed responses with siloed tools.

Ciena needed to simplify their approach and wanted integrated solutions. Strategically embracing the cloud and mobility to prepare for the future, the company decided to layer their security solutions to get full end-to-end coverage across the environment with both speed and scale.

Secure work-from-anywhere access to internet, SaaS, and internal applications.

Ciena worked with CrowdStrike, Okta and Zscaler to develop an integrated zero trust architecture. The company now sees IT as a competitive advantage for improving employee engagement, enhancing their experiences, and allowing them to work from anywhere, while also driving innovation and reducing cost. The new solutions effectively reduced support tickets by over 50%.

AI-driven, cloud-native security from CrowdStrike, Okta & Zscaler.

Deep integrations across the solution include Okta and Zscaler ZPA, SSO+MFA, and Zero Trust Exchange as well as CrowdStrike and Zscaler adaptive security policy enforcement using Falcon ZPA scores for ZIA and ZPA. The net result is that the user experience is the same while working from anywhere, and threat intel sharing allows for dynamic policy enforcement that adapts to fluctuations in risk levels.

SUNBELT RENTALS

Leader in the equipment rental industry

Moving forward with AI enhanced security, automation and zero trust

$19 billion
asset base, managed across ~1,400 locations and 22,000 employees

50-60
billion events handled per month

Response times dropped from days to hours or minutes

> Zero trust provides seamless user experience and friction for bad actors.
>
> **Ken Collins, Head of Information Security, Sunbelt Rentals**

Insufficient baseline security enabled email attacks, phishing and malware.

Fragmented toolsets, manual processes, and slow detection and response times made it hard to proactively address incoming threats. Security operations were heavily reliant on manual processes and there was a clear lack of visibility across the environment.

Threat landscape is rapidly evolving with generative AI.

Gen AI is creating a new level of sophistication for the types of attacks or type of activities from many bad actors. Deepfakes and AI are being used to impersonate people in every way, such as whaling attempts. Traditional awareness and training campaigns are no longer sufficient to address these sophisticated threats. The speed of the types of attacks we see are more crafted and more specific than in the past. Even attacks from the same actor can change very rapidly.

Integrated platform delivers reliability and consistency in robust security posture.

Most solutions were initially selected based on specific needs, not with strategic foresight. The combination of partners naturally evolved into a powerful integrated ecosystem. Unified signals from all three platforms enable high-confidence access control and posture checks, improving both security outcomes and operational efficiency.

Okta, CrowdStrike and Zscaler create a trifecta of confidence in zero trust.

Sunbelt started with CrowdStrike and Okta to address identity, SSO and endpoint security. Adding Zscaler for the internet and network security edge. The integrated stack enabled moving towards a zero trust approach with microsegmentation built around identity with a lot more confidence in the endpoint that was trying to access an application. The volume of incidents and resolution time dropped overnight, going from hours to minutes or seconds, allowing the team to focus on more meaningful work.