CrowdStrike, Okta and Zscaler: Unifying Security with Cross-Domain Protection to Enhance Cyber Resiliency in the AI Era

Challenges

Adversaries are moving faster than ever, with the average observed eCrime breakout time dropping to an all-time low of 48 minutes in 2024, and the fastest occurring in just 51 seconds[1]. At the same time, 79% of attacks were malware-free, leveraging identity exploitation, social engineering, and cloud misconfigurations to evade detection[1]. Traditional, reactive security strategies can no longer counter the evolving tactics of modern adversaries. Threat actors leverage increasingly sophisticated methods, including AI-driven automation and stealth tactics, to infiltrate and move undetected across environments. To overcome these challenges, organizations must move beyond fragmented, point security solutions—an approach that increases complexity, delays response, and ultimately weakens overall security.

What you need

It is time to reimagine how we approach security and use the power of AI to provide speed and scale. Organizations need advanced security platforms that seamlessly work together to deliver layered protection, reducing complexity and driving operational efficiency.

Solution

To address evolving threats intensified by AI, CrowdStrike, Okta, and Zscaler provide a fully integrated, cross-domain security solution designed to eliminate blind spots, enhance visibility, and accelerate response times for robust threat mitigation. This combined approach secures and authenticates identities, enables dynamic context-aware Zero Trust access controls, and protects distributed endpoints while leveraging next-gen SIEM for real-time threat detection and response.

By correlating risk signals across identity, endpoint, cloud, network layers, and beyond, security teams gain a unified view of adversary movement, enabling them to detect, contain, and neutralize threats before they cause damage. With AI-driven automation, bidirectional threat intelligence sharing, and coordinated response actions, the joint solution doesn't just detect threats—it stops them before they escalate.

Security teams can anticipate adversary tactics, automate response actions, and move at machine speed to contain attacks before adversaries break out.

As cyber threats become faster and more sophisticated, organizations must embrace a proactive, AI-powered defense that operates at the speed of the adversary, ensuring threats are neutralized before they impact the business.

Security that Works as One: Unified Protection for a New Era

For organizations embarking on a Zero Trust journey or architecting a Zero Trust solution that maximizes current investments, the strong partnerships and proven

1. CrowdStrike 2025 Global Threat Report, https://www.crowdstrike.com/en-us/global-threat-report/

integrations from market leaders CrowdStrike, Okta, and Zscaler provide a blueprint for an end-to-end Zero Trust solution—from users to endpoints and applications.

These integrations provide administrators with real-time visibility into the threat landscape and the security posture of endpoints and applications. Access to critical applications can be changed based on user, endpoint, and access policies. If an attack occurs, cross-platform remediation is triggered quickly. Defenses are further strengthened with prevention policies applied across integrations to help thwart similar attacks in the future.

The net result is a best-of-breed, cloud-native, dynamic context-driven Zero Trust solution that helps teams stay ahead of modern AI-powered threats with reduced risk and simplified deployment—eliminating the complexity of do-it-yourself approaches.

Solution Highlights

Zero Trust Adaptive Access:

Zscaler enforces least-privileged access based on user identity, device posture, and risk context, with Zscaler Zero Trust Exchange (ZTE) integrating Identity Threat Protection with Okta AI (ITP) and CrowdStrike Falcon® ZTA scores to deploy real-time, risk-based access policies.

Automated Identity Lifecycle Management:

Okta streamlines user provisioning and de-provisioning through Okta SCIM integration, enabling real-time role-based updates and reducing manual workload.

Identity & Endpoint Threat Detection:

CrowdStrike detects and mitigates threats targeting users and endpoints by sharing Zscaler Deception signals with Okta ITP for adaptive responses, while CrowdStrike telemetry provides enriched context to boost threat detection.

Continuous Authentication and Risk-Based Access:

Zscaler enforces dynamic access policies with Okta triggering step-up authentication based on anomalous behavior detected by Zscaler or CrowdStrike.

Unified Risk Visibility:

Zscaler Risk360 and Data Fabric ingest identity logs from Okta and endpoint signals from CrowdStrike.

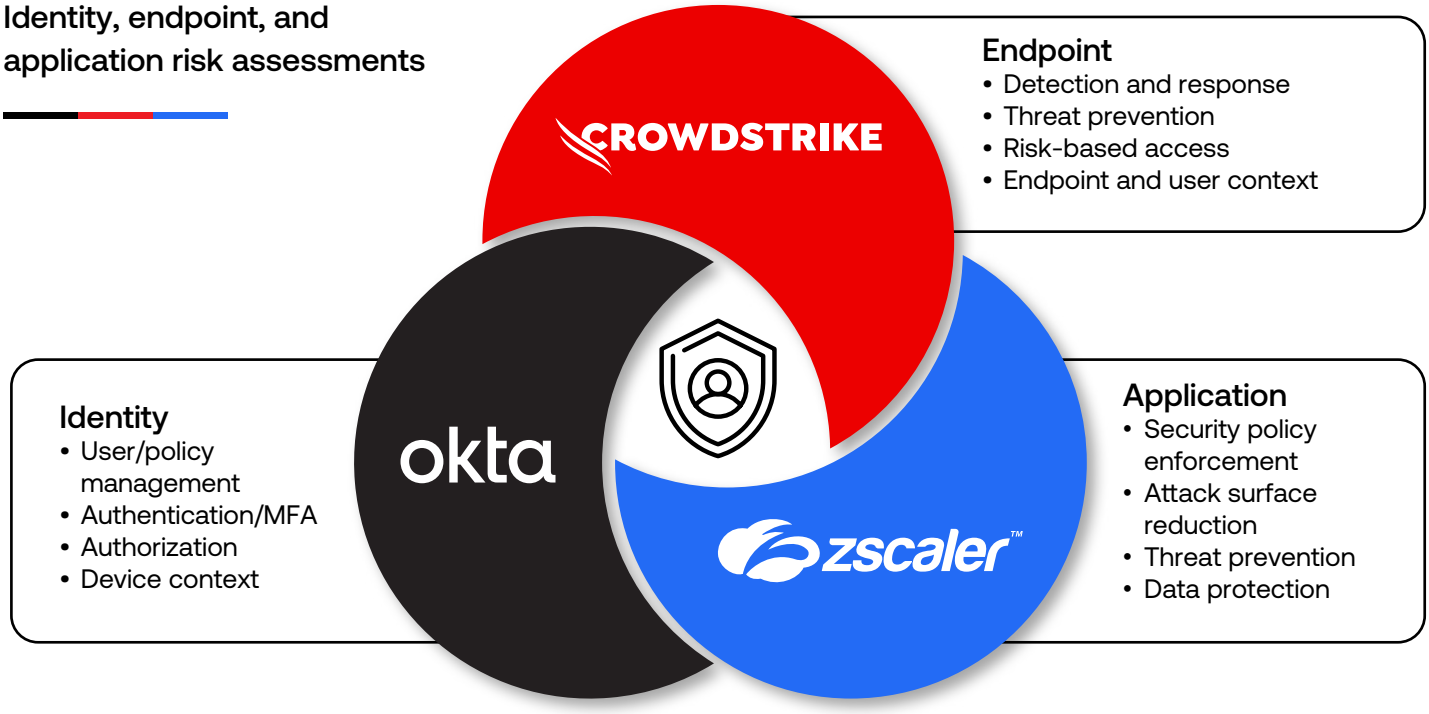
Cross-Platform Threat Intelligence Sharing:

Zscaler shares unified telemetry to accelerate detection and response, with CrowdStrike enhancing Zscaler's custom block lists for proactive protection.

Unified, Cross-Domain Threat Detection and Response:

CrowdStrike delivers comprehensive visibility and coordinated, automated responses across endpoints, identities, and applications via CrowdStrike Falcon® Next-Gen SIEM and CrowdStrike Falcon® Fusion SOAR integrations with Okta and Zscaler to quickly see and stop cross-domain threats, preventing lateral movement.

Identity, endpoint, and application risk assessments



Shared telemetry and threat intelligence

The Benefits of Combined Synergies for Next-Level Cyber Resilience

1. Augmented Zero Trust Access:
Zero Trust access prevents lateral movement of threats with adaptive access policy enforcement based on user identity, device posture, and real-time threat context.

2. Automated Threat Detection and Remediation:
Real-time detection and threat intelligence trigger immediate, coordinated responses, including policy enforcement and Universal Logout.

3. Unified Risk Visibility:
Zscaler Risk360 integrates with logs from CrowdStrike and Okta to provide contextualized telemetry and comprehensive risk insights, accelerating investigation and remediation.

4. Fast Investigation and Response:
Accelerated investigation and response through integration with CrowdStrike Falcon Next-Gen SIEM provides unified visibility, AI-powered detection, and automated workflows to quickly contain cross-domain threats.

5. Efficient Identity Management:
SCIM-based provisioning from Okta ensures secure, automated user provisioning and de-provisioning, allowing only authorized access.

6. Improved User Experience:
Seamless access enabled by Okta SSO, MFA, and Zscaler's adaptive policies enhances productivity without compromising security.

Conclusion

CrowdStrike, Okta, and Zscaler deliver integrated and simplified security solutions that enhance protection, reduce complexity, and ensure scalability for today's evolving digital ecosystems.

Together, they empower organizations with a Zero Trust defense that simplifies identity-based access and strengthens cross-domain threat detection.This powerful partnership helps organizations proactively strengthen their cybersecurity posture and build resilience for the AI era.

About CrowdStrike

CrowdStrike (NASDAQ: CRWD), a global cybersecurity leader, 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 light-weight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

About Okta

Okta, Inc. is The World's Identity Company™. We secure Identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of Identity to drive security, efficiencies, and success—all while protecting their users, employees, and partners. Learn why the world's leading brands trust Okta for authentication, authorization, and more at okta.com.

About Zscaler

Zscaler (NASDAQ: ZS) 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 data centers globally, the SASE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform.

Learn more about our solutions at okta.com, crowdstrike.com , and zscaler.com |