Unified Zero Trust in Action: How Zscaler and CrowdStrike Deliver Cross-Domain Threat Protection

AT-A-GLANCE

Key Benefits:

Unified Zero Trust in Action: Zscaler and CrowdStrike amplify Zero Trust security by enforcing dynamic access controls that reduce attack surface exposure. Legitimate users get secure access to critical systems, while potential attacks are restricted. Through shared threat intelligence, security teams gain greater operational efficiency and improved visibility across network layers.

Proactive Zero-Day Defense: Early insights into risky behaviors and unknown vulnerabilities allow organizations to quickly identify and mitigate zero-day threats. Together, Zscaler and CrowdStrike empower businesses to strengthen defenses and protect sensitive data and workloads against emerging attacks.

Rapid Threat Detection and AI Defense: By centralizing network and endpoint telemetry along with AI-driven event logs, the integration accelerates threat detection, investigation, and response. Customers benefit from faster correlation of threats and streamlined security workflows, reducing attacker dwell time and minimizing risk.

Automated Threat Containment: Integrated response workflows across Zscaler and CrowdStrike platforms enable security teams to rapidly contain and remediate threats without disrupting legitimate business activity. Automated orchestration ensures efficient incident handling while limiting operational impact, saving time and resources.

Unified cross domain Zero Trust security for fast, adaptive, and automated protections that outpace advanced threats.

The Challenge

Addressing today's dynamic threats requires an ecosystem of advanced, integrated solutions. Zscaler and CrowdStrike exemplify this collaborative approach, joining forces to deliver complementary strengths that redefine what holistic enterprise security can achieve. Both organizations are built on cloud-native platforms, engineered for modern security needs rather than retrofitted to legacy models.

Together, they leverage a shared Zero Trust philosophy, setting the industry standard for inline security, secure access, endpoint protection, and advanced threat detection and response. This partnership aligns with customers' key priorities, focusing on stronger security, cost efficiency, and simplified effort in tackling the ever-evolving threat landscape.

By combining the strengths of their cloud-native platforms, the Zscaler and CrowdStrike alliance helps enterprises shift from cyber risk to proactive cyber resilience. Through

intelligent access controls, adaptive policies, and shared threat intelligence, our double digit seamless integrations effectively minimize threats across endpoints, networks, and applications.

The Solution

Zscaler and CrowdStrike have created a seamless defense-in-depth framework that fuses Zero Trust security principles with cross-domain threat protection to deliver layered defenses against today's advanced attacks. This framework minimizes attack surfaces, detects emerging threats, and accelerates response times, providing enterprises with robust and actionable security. By sharing intelligence, Zscaler and CrowdStrike enforce zero trust in every interaction, ensuring access only for safe, trusted devices. Zscaler dynamically adjusts user access using real-time risk assessments and device security alerts from CrowdStrike, while CrowdStrike's threat intelligence helps Zscaler block harmful websites and threats. This adaptive Zero Trust approach continuously responds to changing risks, making it significantly more difficult for attackers to exploit vulnerabilities.

Zscaler and CrowdStrike excel in advanced zero-day threat detection by combining Zscaler's advanced sandbox technology and CrowdStrike's real-time device insights to swiftly identify and isolate unknown malware. Zscaler's use of decoys proactively catches attackers early and feeds reliable intelligence back to CrowdStrike, keeping organizations one step ahead of emerging threats. Their integrated cross-domain protection ensures enterprises can rapidly detect, correlate, and remediate threats across networks and endpoints—thanks to Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) sharing threat telemetry with CrowdStrike Falcon Insight XDR. This allows for unified threat detection, deeper AI-powered threat correlation, and automated response workflows, enabling fast containment, reduced triage times, and minimized operational impact.

How It Works

Zscaler and CrowdStrike integrations support the following use cases:

- **Posture-Driven Conditional Access Control to Applications**
  Zscaler ensures access is granted only to compliant and trusted devices by integrating Zero Trust Assessment (ZTA) scores from CrowdStrike Falcon. Threat detection signals are used to block non-compliant endpoints and secure sensitive applications. Browser isolation adds another layer of security, safeguarding restricted groups without impacting user productivity.

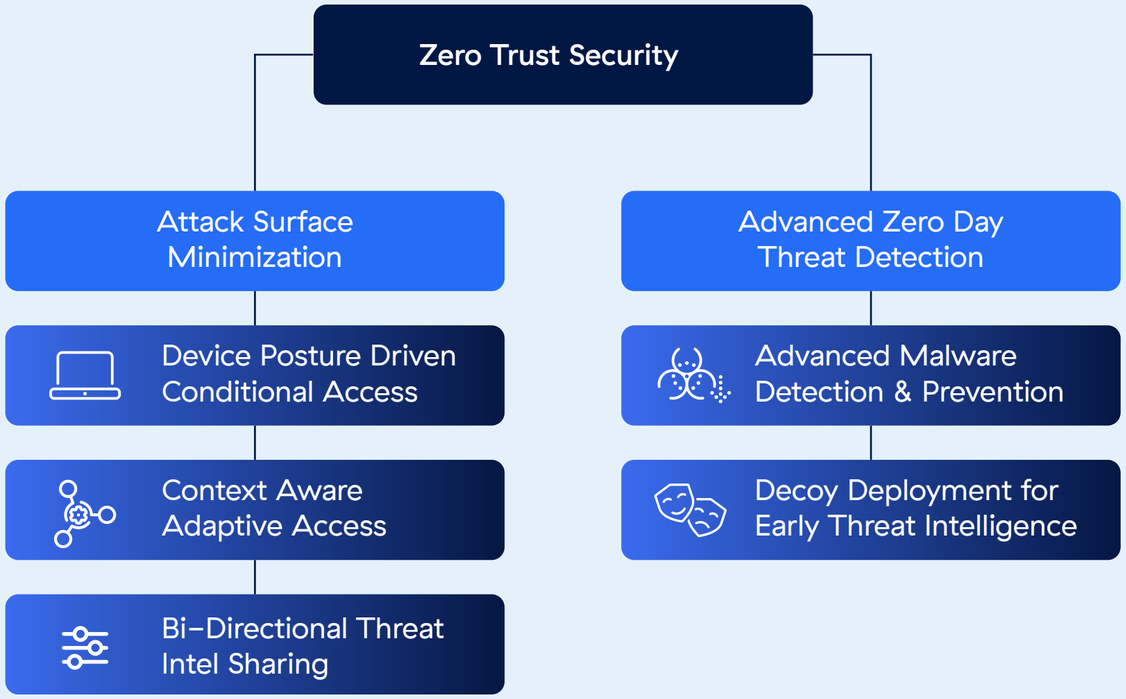
- **Threat Intelligence Sharing to Strengthen Defense Posture**
  CrowdStrike shares valuable threat intel on indicators of compromise (IoCs) with Zscaler, enabling it to enhance its custom block lists by blocking malicious domains and URLs for proactive threat prevention on the network.

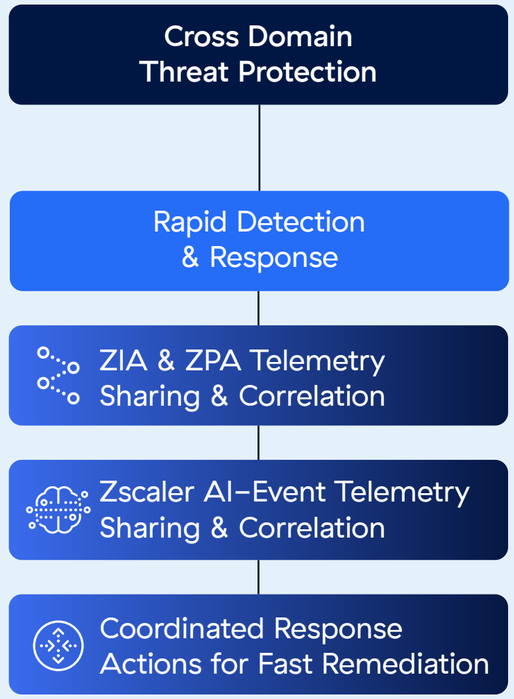
- **Adaptive Access with Real-Time Context for Risk Assessment and Decision Making**
  Zscaler leverages Zero Trust Assessment (ZTA) device scores and device security incident signals from CrowdStrike to enforce adaptive access controls. Adaptive policies dynamically respond to real-time risk fluctuations, ensuring precise, context-aware decision making and policy enforcement.

- **Advanced Malware Detection and Prevention**
  Zscaler's advanced cloud sandbox detects zero-day malware and immediately triggers quarantine workflows through CrowdStrike Falcon. This allows security teams to isolate infected endpoints quickly, improve decision-making, and neutralize threats before they can spread.

- **Deploying Decoys for Early Threat Intelligence**
  Zscaler Deception deploys decoys to lure attackers away from critical systems, enabling early breach detection in the attack cycle. High-confidence alerts are shared with CrowdStrike Falcon to refine threat response workflows and remove compromised files, creating faster, more effective defenses.

HOW WE DO IT: OUR JOINT DEFENSE-IN-DEPTH INTEGRATION FRAMEWORK





- **ZIA and ZPA Telemetry Sharing and Correlation**
  Zscaler shares network telemetry from ZIA and ZPA with CrowdStrike Next-Gen SIEM to enable enhanced threat visibility and detection across domains. When threats are detected, cross-platform workflows restrict user access and isolate critical applications, preventing unauthorized activity while ensuring rapid threat containment.

- **AI-Event Telemetry Sharing and Correlation**
  Zscaler shares AI-event logs with CrowdStrike Next-Gen SIEM to correlate critical AI-based security insights. By cutting through the noise, the solution delivers enhanced visibility, faster detection, and protection against unauthorized AI misuse, ensuring robust defenses across applications and endpoints.

- **Automating and Orchestrating Threat Intel Sharing for Coordinated Policy Actions**
  Through automation and synchronized workflows, Zscaler and CrowdStrike facilitate streamlined threat intelligence sharing and coordinated response actions. SecOps teams benefit from Falcon Fusion's built-in SOAR workflows delivering closed-loop remediation between ZIA's advanced sandboxing, CrowdStrike Next-Gen SIEM, and ZIA's policy enforcement engine.

Solution Highlights

Unified Zero Trust Security: Dynamic authentication and adaptive access policies secure users and data—anywhere, anytime—against rapidly evolving and AI-powered attacks.

Cross-Domain Threat Protection: Real-time sharing of threat intelligence and telemetry enables rapid detection, investigation, and response to threats across endpoints, networks, and applications.

Enhanced Threat Defense: Synergistic integration delivers deep malware-free and zero-day attack detection, driven by advanced sandboxing, deception, and device posture assessments.

Automated and Coordinated Responses: Automated incident response and coordinated workflows streamline security operations for faster containment and reduced risk.

Learn more at https://www.zscaler.com/partners/crowdstrike ⟶

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 SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Zero Trust Everywhere