Unified Zero Trust in Action:

How Zscaler and CrowdStrike Deliver Cross-Domain Threat Protection

PARTNER BRIEF

Introduction

The cyber threat landscape is accelerating at an unprecedented pace, with attackers reducing detection windows to just 48 minutes[1]—and as fast as 51 seconds[2] in some cases. Coupled with a 79%[3] increase in malware-free attacks, adversaries are leveraging advanced tactics like credential theft and trust exploitation, rendering traditional, malware-focused defenses insufficient.

Adding to this complexity is the rapid adoption of AI, which has introduced a new set of vulnerabilities. Enterprises are transferring over 3.6 petabytes of sensitive AI-driven data, making it a prime target for attackers seeking to disrupt business operations and steal intellectual property. Limited visibility across attack surfaces and static, reactive policies have left organizations unable to respond proactively to these emerging risks.

These challenges are compounded by fragmented security architectures, where siloed tools and unintegrated platforms create inefficiencies, drive up costs, and open exploitable vulnerabilities. To combat this, enterprises must adopt integrated solutions between best-of-breed platforms.

[1, 2, 3] CrowdStrike 2025 Global Threat Report

Zscaler and CrowdStrike: Tackling Complex Cybersecurity Challenges Through Collaboration

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.

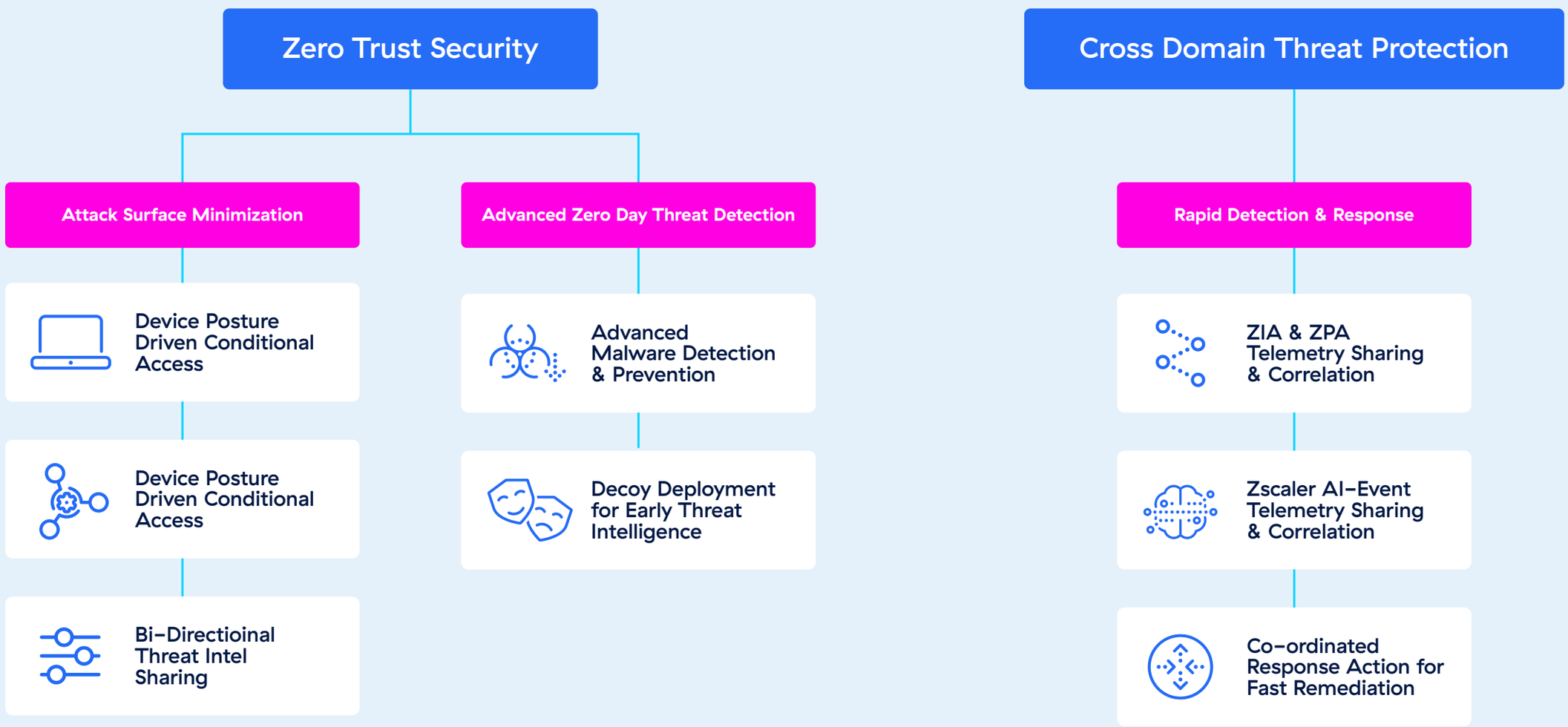
Together, they leverage a shared Zero Trust philosophy, setting the industry standard for inline security, secure access, endpoint protection, and advanced threat detection and response. This partnership aligns with customers' key priorities, focusing on stronger security, cost efficiency, and simplified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

Integration Deep Dive

Zscaler and CrowdStrike have developed a seamless defense-in-depth framework that combines the principles of Zero Trust security with cross domain threat protection, delivering layered defenses to address today's advanced threat landscape. Designed to minimize attack surfaces, detect emerging threats, and accelerate responses, this framework empowers enterprises with robust, actionable security.

How we do it: Joint defense-in-depth integration framework



Zero Trust Security

Zscaler and CrowdStrike safeguard access and reduce vulnerabilities through shared intelligence to enforce zero trust through every interaction.

- **Attack Surface Minimization:** Zscaler and CrowdStrike work together to reduce the attack surface by ensuring that only safe, trusted devices can access company applications and data. Zscaler automatically adjusts access based on real-time risk assessments and active security alerts about each device from CrowdStrike. In addition, CrowdStrike's latest threat intelligence helps Zscaler proactively block harmful websites and threats. These integrations provide businesses with smarter Zero Trust-based protections that constantly adapt to changing risks, making it much harder for attackers to break in or cause disruption.

- **Advanced Zero Day Threat Detection:** Zscaler and CrowdStrike protect businesses from zero day threats. Zscaler uses advanced sandboxing technology and up-to-date device insights from CrowdStrike to quickly spot and isolate unknown malware before it can spread. In addition, Zscaler sets decoys to catch attackers early, sending reliable early warnings and intelligence to CrowdStrike. The integrated capabilities help organizations stay a step ahead of new and emerging threats and respond before damage can occur.

Cross Domain Threat Protection

Zscaler and CrowdStrike ensure rapid detection, correlation, and remediation of threats across enterprise networks and endpoints.

- **Rapid Detection & Response:** Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) platforms share and correlate threat telemetry with CrowdStrike Falcon Insight XDR, enabling unified threat detection across network traffic, endpoints, and workloads for broader visibility. Zscaler also shares AI-powered event telemetry with CrowdStrike, allowing for deeper threat correlation and faster identification of anomalies and AI-generated threats. This coordinated integration powers automated response workflows, so organizations can contain and remediate threats quickly, reduce triage time, and minimize operational impact with precise, unified actions.

By uniting their cloud-native platforms, Zscaler and CrowdStrike empower enterprises to shift from cyber risk to proactive resilience, delivering seamless, layered security built on Zero Trust and cross-domain threat protection to address today's advanced threats.

This defense-in-depth approach ensures enterprises can adopt a proactive stance in fighting cyber risks, combining best-in-class Zero Trust principles with cross-domain visibility, detection, and response for optimal resilience. Zscaler and CrowdStrike integrations support the following new 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.

- **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.

Better Together 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.

Leverage Zscaler & CrowdStrike Integrations for Unified Defense Against Evolving Threats

Organizations can no longer rely on siloed security tools or outdated approaches to tackle AI-driven attacks and non-traditional vulnerabilities. Enterprises need adaptive, integrated cybersecurity ecosystems built to address advanced threats with speed, intelligence, and multi-layered defense strategies.

The strategic partnership between Zscaler and CrowdStrike delivers precisely that—a unified approach combining Zscaler's cloud-native networking and Zero Trust capabilities with CrowdStrike's industry-leading endpoint detection and response expertise. Together, these solutions ensure enterprises stay resilient against the rising tide of AI-driven threats and malware-free attack techniques.

Aligned with customer priorities, the partnership reduces complexity and drives cost efficiency by delivering integrated solutions that outpace adversaries, streamline security efforts, and maintain robust defenses in real time. The Zscaler and CrowdStrike partnership represents the future of cybersecurity: powerful, adaptable, and purpose-built for the challenges of today's sophisticated threat landscape.

Call to Action

Learn more at **www.zscaler.com/partners/crowdstrike**
Download our **Zscaler and CrowdStrike Deployment Guide**

About CrowdStrike:
CrowdStrike has redefined security with the world's most advanced cloud-native platform that protects and enables the people, processes and technologies that drive modern enterprise. CrowdStrike secures the most critical areas of risk — endpoints and cloud workloads, identity, and data — to keep customers ahead of today's adversaries and stop breaches. Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence on evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities — all through a single, lightweight agent. With CrowdStrike, customers benefit from superior protection, better performance, reduced complexity and immediate time-to-value. Learn more at crowdstrike.com.

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