How to Deliver a Unified, Cross-domain Defense with Zscaler and CrowdStrike

See, strike, and move with machine-like speed to safeguard the AI era

AT-A-GLANCE

In the AI era, attack windows are accelerating, yet many enterprises are constrained by fragmented security architectures. The resulting gaps in security are easy to exploit, but hard for human defenders to surface and contain. Zscaler and CrowdStrike close these gaps with an integrated, cross-domain architecture that combines shared risk signals, threat intelligence, high-fidelity telemetry, and AI-driven automation so teams can see, move, and strike with machine-like precision.

The Challenge: High Costs of Fragmented Defenses

Agentic attacks are the new baseline today. Increasingly, bad actors are leveraging AI to move at machine speed, shrinking time to compromise from days or weeks to a matter of minutes. In this frenetic threat landscape, human defenders simply can't keep pace.

Fragmented architectures compound the issue—weakening security postures, adding operational complexity, and slowing down containment efforts. Common challenges associated with a fragmented approach include:

Siloed visibility: The continued use of legacy endpoint, network, and cloud tools can increase hidden attack surfaces, as these disjointed solutions weren't designed to operate together, nor can they provide a unified view of the threat landscape.

Slow threat detection: Overwhelming alerts and false positives create noise, leaving analysts without critical context to act quickly on high-priority threats due to the heavy amount of manual correlation that is required to trigger and complete an investigation.

Being outpaced by new threats: Teams are further hampered by rigid policies and rules, a lack of shared intel or risk signals across tools, and tedious workflows that require swiveling between multiple management consoles to complete routine tasks.



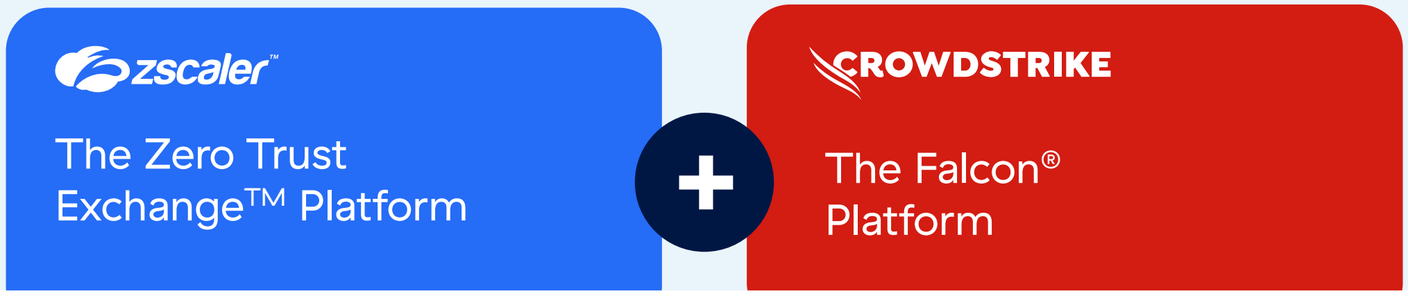
The Solution: Zscaler and CrowdStrike for Unified, Cross-Domain Defense

Combatting modern threats requires an ecosystem of advanced, integrated solutions. Zscaler and CrowdStrike join forces to deliver complementary solutions that unify security across domains with an architecture that was engineered for modern needs rather than retrofitted to legacy models.

By combining the strengths of their cloud-native platforms, Zscaler and CrowdStrike help enterprises shift from cyber risk to proactive cyber resilience through rich signal sharing, bi-directional threat intelligence, correlated network and endpoint telemetry, and cross-platform automation.

In total, Zscaler and CrowdStrike deliver more than 10 customer-driven solutions designed to:

- **Exchange Signals, Enforce Trust:** Exchange signals across devices, identities, and networks to enforce adaptive trust and reduce exposure.
- **Share Intel, Stop Threats:** Share telemetry and intelligence across domains to improve correlation and enable coordinated response.
- **Automate with AI, Supercharge the SOC:** Apply AI to supercharge security operations, accelerate triage, and extend analyst capacity.



Unified Cross-Domain Architecture

See: Unified visibility and threat intel sharing across endpoints, networks, identities, and beyond

Move: Adaptive, risk-aware policies based on the health of your users and devices

Strike: Advanced AI-powered detection, response, and risk management

©2026 Zscaler, Inc. All rights reserved.

EXCHANGE SIGNALS, ENFORCE TRUST:

Ensure only healthy devices can reach critical enterprise apps

Maintaining a comprehensive, real-time risk profile for every active session on every managed endpoint is critical to strengthening your security posture. Zscaler and CrowdStrike ensure only trusted, compliant devices can reach your critical enterprise apps and data, including SaaS-based solutions or private workloads hosted in the public cloud.

CrowdStrike Falcon calculates a real-time Zero Trust Assessment (ZTA) score by evaluating 120+ OS and sensor configuration settings, patch status, firewall/encryption settings, sensor health, and active threat detections. To grant conditional access to corporate resources, Zscaler policies are incorporated into the ZTA score and are enforced inline between your users' devices and their applications. When the ZTA score is below the desired threshold set by IT, device access is blocked. If it's equal or above the threshold, access is allowed or restricted, based on established policies.

To maintain user productivity, Zscaler Browser Isolation can also be used to isolate restricted devices or groups of users. Better yet, policy enforcement is done "behind the scenes," meaning it's completely non-disruptive from a user experience perspective. This adaptive Zero Trust approach continuously responds to changing risks, making it significantly more difficult for attackers to exploit vulnerabilities without unnecessarily compromising workforce access.

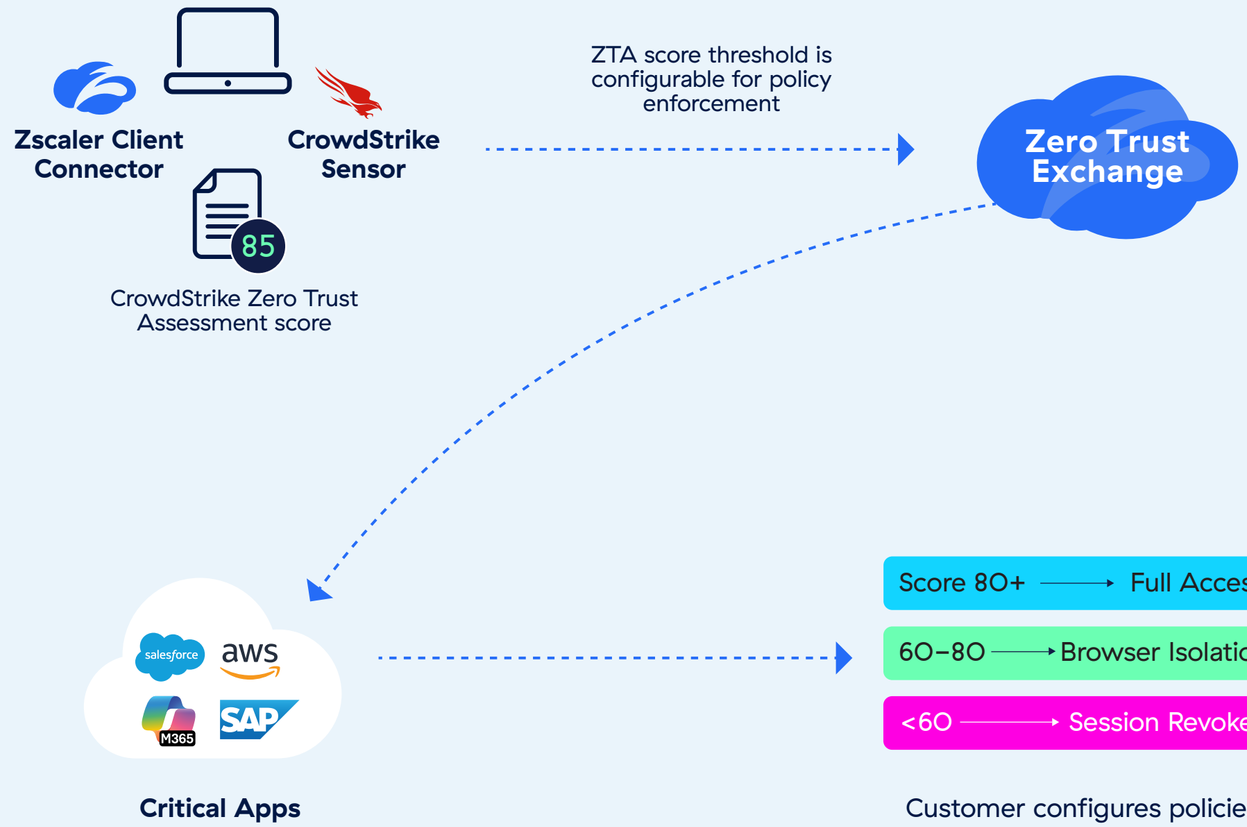


Figure 1: Zscaler and CrowdStrike enforce conditional access to critical applications based on the real-time health and behavior of all endpoints.

©2026 Zscaler, Inc. All rights reserved.

SHARE INTEL, STOP THREATS:

Turn detections from one platform into instant protections across both for a self-reinforcing intelligence loop

Zscaler and CrowdStrike excel in advanced zero-day threat detection through extensive, bi-directional intelligence sharing. Continuously enriching threat feeds across your CrowdStrike and Zscaler tenants enables you to block new, emerging threats with high-confidence alerts and automated containment actions.

For example, Zscaler Deception uses decoys and lures to keep attackers away from real enterprise assets. This fake surface attack intercepts threats—human or agentic—and gives security teams a detection control that only notifies them of confirmed threats and breaches. File hashes and indicators of compromise from Deception are shared instantly with CrowdStrike Falcon, arming it with attacker Tactics, Techniques, and Procedures (TTPs), infrastructure details, and lateral movement indicators specific to that environment.

At the same time, high-fidelity threat indicators on endpoints that are discovered within a customer's CrowdStrike tenant are automatically shared with Zscaler Internet Access (ZIA), blocking known-bad infrastructure before users can reach it. This creates a self-reinforcing intelligence loop across CrowdStrike and Zscaler platforms for defense in depth and stronger cyber protection.

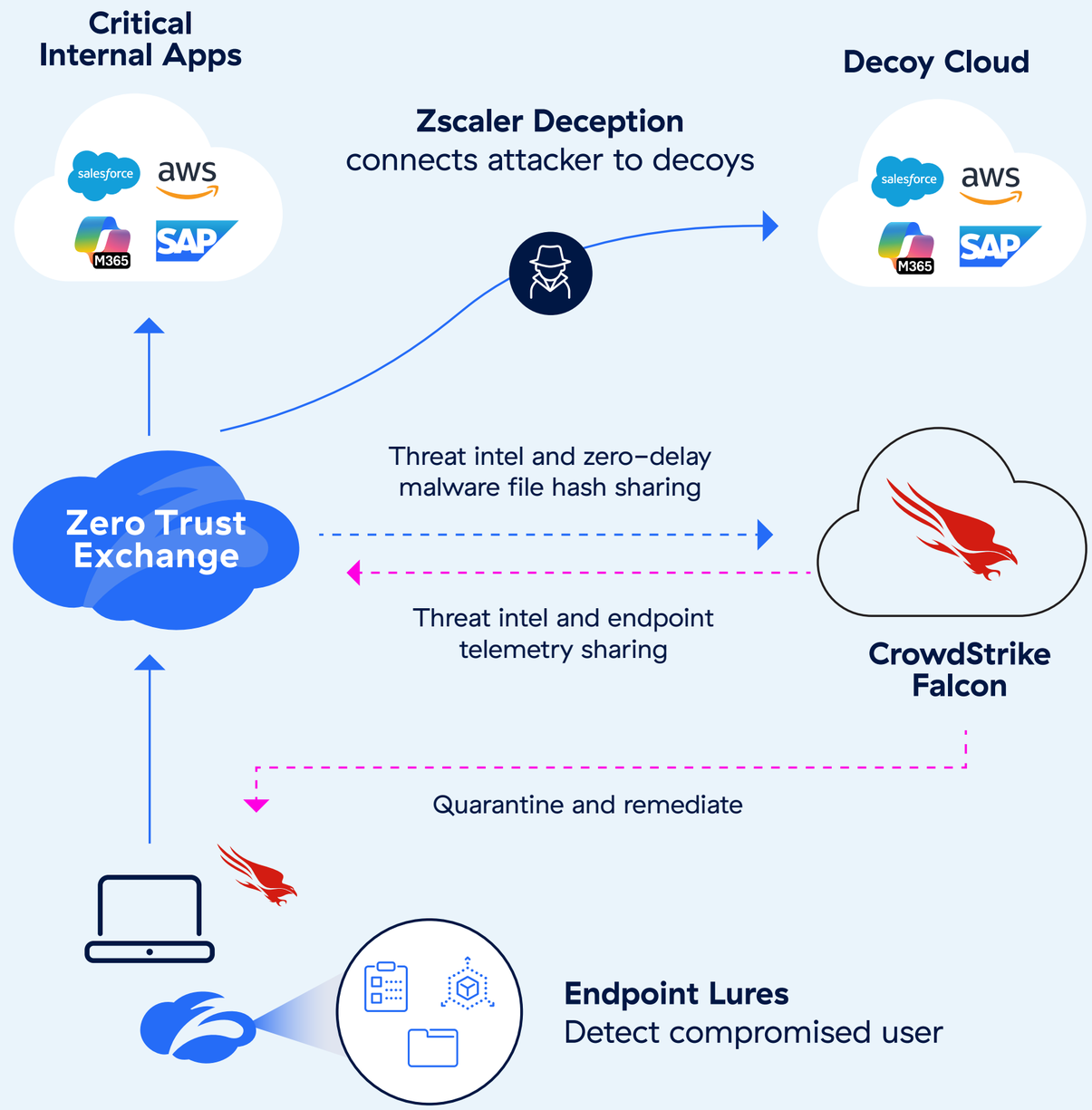


Figure 2: Zscaler and CrowdStrike share threat intelligence, enabling automated containment actions across platforms when an indicator of compromise is detected.

©2026 Zscaler, Inc. All rights reserved.

AUTOMATE WITH AI, SUPERCHARGE THE SOC:

Stream Zscaler telemetry and AI event data into CrowdStrike Falcon Next-Gen SIEM for enhanced visibility and faster triage

Zscaler and CrowdStrike help SecOps teams find the proverbial needles in the haystack by surfacing high-priority threats and coordinating response actions across platforms.

CrowdStrike FalCon Next-Gen SIEM ingests logs from Zscaler Internet Access and Zscaler Private Access without requiring any without requiring any tedious configurations. The network telemetry from Zscaler is automatically correlated alongside CrowdStrike endpoint, identity, and cloud data, pinpointing multi-stage attacks that would otherwise go undetected across siloed tools.

In addition, Zscaler inspects AI activity such as prompts and responses, then sends the resulting event data to Falcon Next-Gen SIEM to correlate critical security insights. By cutting through the noise, the solution delivers enhanced visibility, faster detection, and stronger protection against AI misuse, ensuring robust defenses across applications and endpoints.

Investigations are further accelerated through automation and synchronized workflows. SecOps teams benefit from Falcon Fusion's built-in SOAR workflows that deliver closed-loop remediation between Zscaler's advanced sandboxing, CrowdStrike Next-Gen SIEM, and Zscaler's policy enforcement engine. Eliminating handoffs between teams, streamlining workflows, and providing full context in a single console dramatically compresses investigation timelines, ultimately improving operational efficiency and cyber resilience.

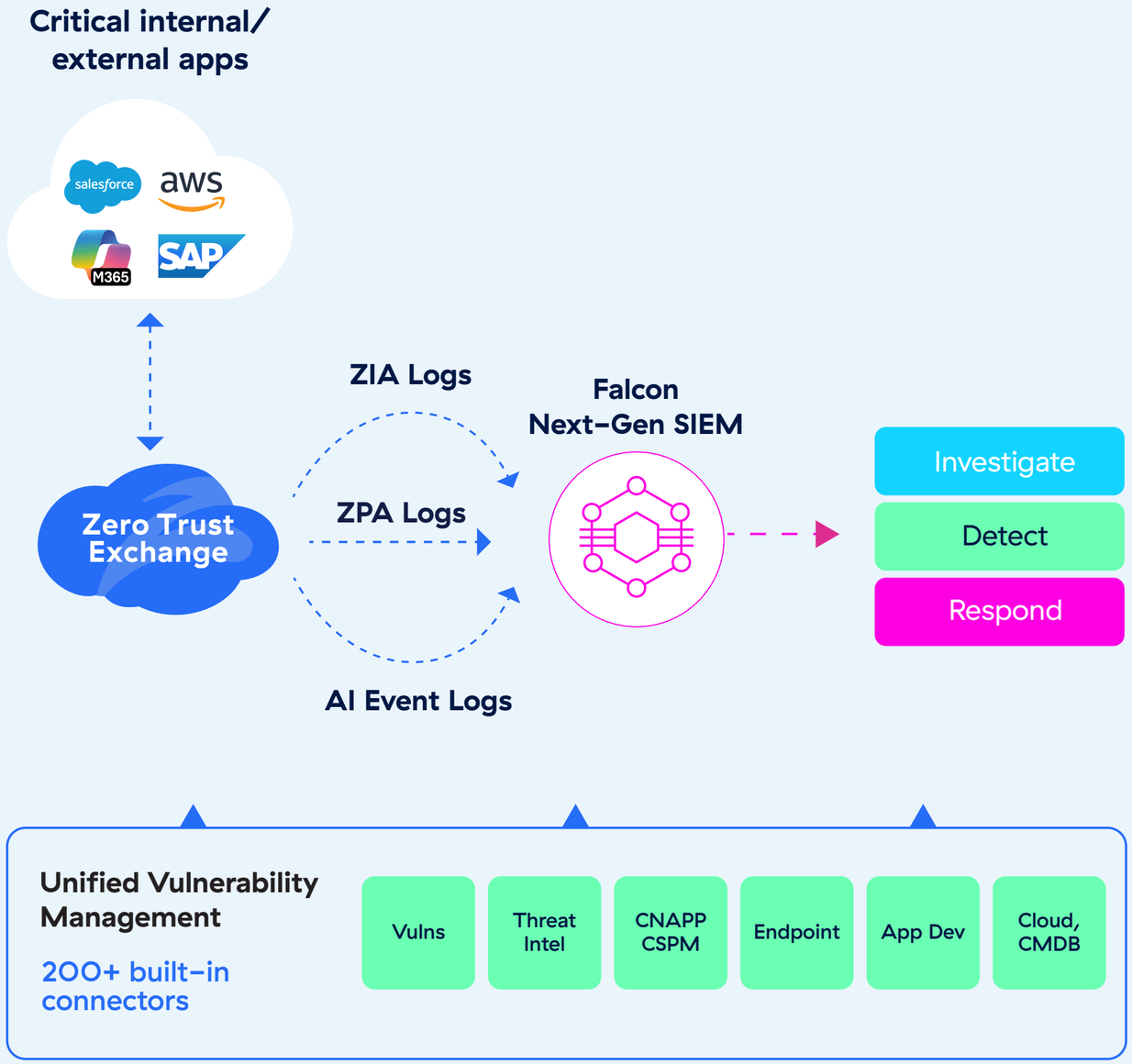


Figure 3: Falcon Next-Gen SIEM ingests network telemetry and AI event data from Zscaler, correlating rich insights in a single view to quickly pinpoint high-priority threats and accelerate triage.

©2026 Zscaler, Inc. All rights reserved.

Transform Security Outcomes with CrowdStrike and Zscaler

MINIMIZE RISK

Stop lateral movement and enforce zero trust access controls automatically across network and endpoint boundaries.

SIMPLIFY OPERATIONS

Eliminate blind spots and find elusive threats by correlating network telemetry directly with endpoint identity signals.

MAXIMIZE SAVINGS

Consolidate legacy point solutions into a unified architecture to reduce SecOps overhead and operational friction.



©2026 Zscaler, Inc. All rights reserved.

WHAT OUR CUSTOMERS ARE SAYING

Thousands of leading companies worldwide trust Zscaler and CrowdStrike to unify defenses across security domains.



"Zscaler and CrowdStrike are the only ones out there with a zero trust solution that is cloud native — forging the path to innovation. We brought Zero Trust access to our staff worldwide in nine days."

NICOLE DARDEN FORD, CISO



"With Zscaler providing visibility into web and SaaS traffic, CrowdStrike on the endpoint, and Okta as our identity layer, the DXC security team has a wealth of tools to conduct targeted investigations when incidents arise, allowing us to respond faster."

JIMMIE OWENS, GLOBAL CISO



"We decided to pursue a cloud-first strategy to reduce the attack surface and secure endpoints. The CrowdStrike-Zscaler integration has really allowed us to defend United in ways we weren't able to before."

SEAN MASON, MANAGING DIRECTOR OF CYBER DEFENSE

©2026 Zscaler, Inc. All rights reserved.

Ready to Learn More? Visit www.zscaler.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**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 **Zscaler, Inc. (Worldwide HQ) • 4401 Great America Parkway • Santa Clara, CA 95054** **zscaler.com**

zscaler™

Act Fast.
Stay Secure.