Zscaler and CrowdStrike Expand Strategic Partnership with Integrations to Unify Cross-Domain Security

September 2, 2026

New initiatives integrate leading platforms, automate cross-domain response, and enforce real-time Zero Trust enforcement policies.

Zscaler is expanding our long-standing, strategic partnership with CrowdStrike to automate complex security workflows and leverage industry standards for real-time, adaptive Zero Trust policy enforcement.

As part of this initiative, CrowdStrike will expand Project QuiltWorks to include Zscaler. First launched in April 2026, Project QuiltWorks is an industry-wide security coalition that unites frontier AI models from labs like OpenAI and Anthropic with cybersecurity providers, systems integrators, cloud platforms, and insurers.

Industry-standard Adaptive Access

Zscaler and CrowdStrike continue to help organizations stop cross-domain attacks, reduce complexity, and strengthen security across the enterprise.

The two companies will release an integration using the OpenID Shared Signals Framework (SSF). This industry-standard approach allows the CrowdStrike Falcon® platform to continuously evaluate user risk and share that context with Zscaler's Adaptive Access Engine (AAE) in real-time. If suspicious behavior is detected on the endpoint, Zscaler can automatically and dynamically adjust access based on the current risk posture.

Native Automation with Falcon Foundry and Zscaler OneAPI

To further reduce operational complexity, Zscaler and CrowdStrike are developing a native CrowdStrike Falcon® Foundry application built on Zscaler OneAPI. This integration surface spans the entire Zscaler portfolio, including Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), Zscaler Digital Experience (ZDX), Zscaler Client Connector, and Zscaler Authentication Services.

The application provides:

- **Unified investigation**: Analysts can trigger Zscaler enforcement actions directly from within the Charlotte Agentic SOAR interface.
- **Automated response:** Charlotte Agentic SOAR can leverage Zscaler context for end-to-end automated remediation.
- **Zero infrastructure:** The integration runs natively inside the Falcon platform with no middleware, connector, or separate infrastructure to deploy.

Unified Telemetry and Cross-Domain Visibility with Falcon Next-Gen SIEM

Modern adversaries operate across multiple attack surfaces, moving seamlessly from compromised endpoints and stolen credentials to cloud applications and network paths. To close security blind spots, Zscaler telemetry and actionable AI-event metadata stream directly into CrowdStrike Falcon® Next-Gen SIEM, delivering unified, cross-domain visibility in a single console.

- **Automated, Unified Data Ingestion**: Network event logs from ZIA and ZPA, along with Zscaler AI-event logs, stream continuously and automatically into Falcon Next-Gen SIEM with no manual configuration or complex pipelines required.
- **Cross-Domain Threat Correlation:** By combining Zscaler's rich network and web telemetry with Falcon endpoint, identity, and cloud data, SecOps teams can automatically detect and reconstruct multi-stage attack chains that evade traditional, siloed security tools.
- **AI-Powered Threat Detection and Governance:** Ingesting Zscaler Private AI telemetry centralizes security event data (such as AI app interactions, risky chatbot prompts, and policy violations), enabling higher-fidelity alerts, cutting through alert noise, and providing real-time visibility into AI-specific risks.
- **Accelerated Triage and Long-Term Compliance:** Analysts can conduct end-to-end investigations from a unified interface with complete context across user behavior and network traffic, while automated log parsing and retention simplify audit and compliance requirements without supplementary tooling.

Unified, Cross-Domain Defense to Safeguard the AI Era

Organizations continue to adopt AI solutions at an unprecedented clip. But the resulting threat landscape will be impossible to contain using legacy, fragmented security tools.

The latest advancements to our partnership with CrowdStrike highlight our continued commitment of protecting the AI-powered enterprise through a

tightly integrated, cross-domain defense. By unifying Zscaler's Zero Trust enforcement with CrowdStrike's leading detection and response capabilities, we are eliminating the silos that attackers commonly exploit.

Read more about our strategic partnership with CrowdStrike, including key use cases and other joint solutions we deliver to thousands of enterprise customers worldwide.

Forward-Looking Statements

This blog may include discussion of unreleased services or features. Any unreleased services or features referenced here are still in development and subject to change. Customers should make their purchase decisions based upon features that are currently available.