Solution Brief

Netskope and CrowdStrike

Netskope and CrowdStrike share threat intelligence, risk scores, and device posture data between the Netskope One platform and the CrowdStrike Falcon platform. Security teams get unified visibility across web, cloud, and private applications, backed by adaptive access policies that support zero trust principles.

Quick Glance

- **Exchange threat intelligence.** Share indicators of compromise between platforms in real time.
- **Unify investigations.** Stream Netskope logs and AI risk events into Falcon Next-Gen SIEM.
- **Strengthen zero trust.** Pair CrowdStrike device and identity risk with Netskope's own scoring for adaptive access.
- **Validate device posture.** Confirm the Falcon agent is active before granting cloud and web access.
- **Sync identity data.** Keep users and groups aligned between platforms with automatic system for cross-domain identity management (SCIM) provisioning.

"We improved our security without adding friction. The sharing of security intelligence is key to helping protect everyone."

Duane Monroe,
Manager Cyber Security, Aspen Skiing Company

The challenge

Security teams manage more point products than ever, and each new tool risks creating gaps. Without shared context across platforms, threats can slip through the seams between endpoint, cloud, and AI defenses, putting data, assets, and reputation at risk. Zero trust principles call for removing implicit trust, enforcing least-privilege access, and continuously reassessing risk as conditions change. But when endpoint, cloud, and AI tools operate in isolation, without sharing risk views, that's difficult. Organizations need a way to unify threat intelligence, risk scoring, and policy enforcement across the security stack they already have, without adding complexity or replacing tools they trust.

The Netskope and CrowdStrike solution

Netskope inspects traffic and applies access, threat and data protection controls across web, SaaS, cloud services, private applications, and AI usage. CrowdStrike Falcon protects endpoints, workloads, identities, and data through a single lightweight agent. Together, the two platforms share telemetry, risk signals, and now AI risk events. This equips security teams with one connected view of risk across endpoint, cloud, and AI, with the ability to investigate and respond from either console, and neutralize threats with an automated, intelligence-led response.

netskope + CROWDSTRIKE

Shared threat intelligence across endpoint and cloud

Security teams need threat intelligence that moves as fast as attackers. Point products that don't share data leave gaps between endpoint and cloud defenses, and attackers only need one gap.

Netskope Cloud Threat Exchange shares indicators of compromise, including malicious URLs, file hashes, and data loss prevention (DLP) file hashes between CrowdStrike and Netskope through a ready-to-use plugin. Netskope identification of malware in the cloud can inform CrowdStrike endpoint prevention, and malware CrowdStrike detects on the endpoint updates Netskope's own blocklists, all in near real time. Teams can mark indicators stale, old, or unused directly in Cloud Threat Exchange, so shared intelligence stays current on both sides.

For teams building on CrowdStrike Falcon Foundry, the Netskope Direct to Zero Trust App extracts, normalizes, and deduplicates indicators from Netskope malsite and malware alerts, then pushes CrowdStrike-detected indicators back into Netskope URL and File Lists, a second, native path to the same shared intelligence.

Key capabilities include:

- Bi-directional IOC sharing between platforms in near real time
- Cloud-discovered malware can inform endpoint prevention, and endpoint-discovered malware updates cloud blocklists
- Indicator lifecycle management, including marking stale or unused IOCs
- A native Falcon Foundry app for teams standardized on CrowdStrike's app framework

> Netskope and CrowdStrike protect the entire AI transaction lifecycle, combining network-level AI data protection with endpoint-level AI threat detection for complete, cross domain security.

Unified investigations, including AI risk

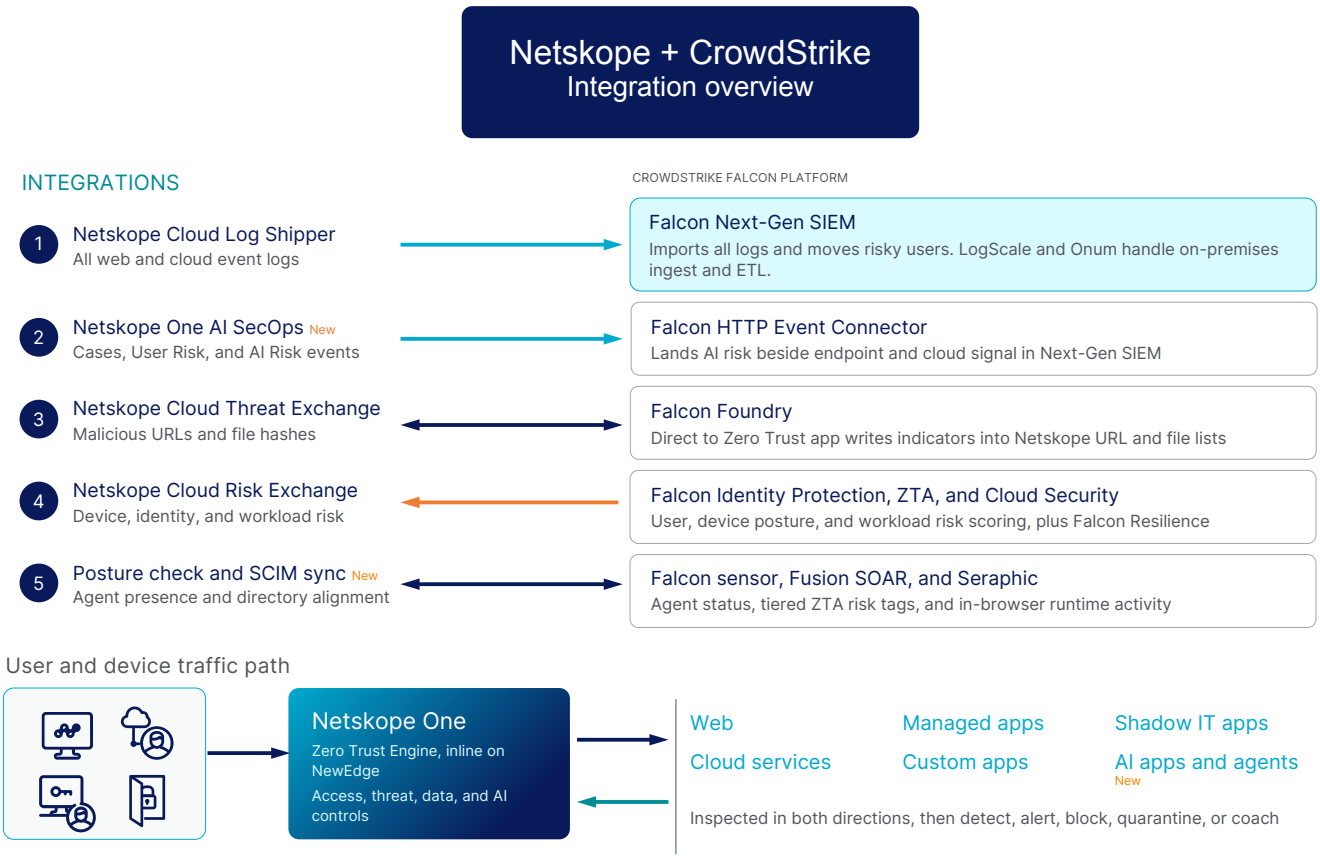
Investigations move faster when analysts aren't switching between tools to piece together the picture. Netskope shares event logs and alerts for web and cloud activity directly with the CrowdStrike Falcon platform, unifying telemetry from endpoints and the security service edge.

Netskope Cloud Log Shipper moves logs into Falcon Next-Gen SIEM and LogScale without added infrastructure. Once ingested, Netskope logs feed Falcon's log management and SIEM dashboards, parsers, and saved searches, giving analysts real time context next to endpoint data, enabling them to build custom dashboards tracking web traffic, daily bandwidth, top visited domains, and data upload patterns.

Netskope One AI SecOps also delivers Cases, User Risk, and AI Risk events into Falcon Next-Gen SIEM in near real time, through Outbound Webhooks and a Falcon HTTP Event Connector, giving analysts a shared, near-real-time view of AI risk alongside endpoint and cloud signal. That same event stream is also the trigger for a documented verdict-and-response pattern, covered under Zero Trust Access, Risk Signal, and Response, that can turn a specific AI risk case into a Netskope-side action.

Key capabilities include:

- Flexible log ingestion: Move web and cloud logs into Falcon Next-Gen SIEM and LogScale using either the Netskope Cloud Log Shipper for direct streaming or LogScale for on-premises ingest
- AI SecOps Cases, User Risk, and AI Risk events delivered through Outbound Webhooks
- Enhanced observability through dashboards, parsers, and saved searches to track daily bandwidth, top visited domains, and upload patterns
- A single console for cross-domain investigation and response



Zero trust access, risk signal, and response

Zero trust principles call for removing implicit trust, enforcing least privilege access, and continuously reassessing risk. That depends on your platforms sharing a common view of who and what is risky.

CrowdStrike device health and identity risk feed directly into Netskope's conditional access: Falcon Zero Trust Assessment scores, Falcon Identity Protection risk scores, and Falcon Cloud Security indicators of attack and misconfiguration all pass into Netskope through Cloud Risk Exchange. Netskope's own User Confidence Index pairs with those signals inside Netskope's policy engine, so access decisions reflect device, identity, and user risk together.

Teams can also build Falcon Fusion SOAR workflows directly: one resolves a device from a ZTA score change and applies a Netskope risk tag through the Device Tags API. A newer pattern starts from a Netskope AI SecOps event, has a published CrowdStrike AI Agent return a verdict, and, only after validation and approval, applies a device tag, a UCI recommendation, or an access restriction.

Netskope also checks whether the CrowdStrike Falcon agent is active on Windows and macOS endpoints, applying adaptive access policy based on the result. Netskope and CrowdStrike keep user and group records in sync using SCIM.

Key capabilities include:

- CrowdStrike device, identity, and cloud workload risk feeding Netskope conditional access through Cloud Risk Exchange
- Two Falcon Fusion SOAR patterns: ZTA-driven device tagging, and verdict-gated response from an AI SecOps event
- Device posture checks that trigger adaptive access policy in real time
- Automatic user and group provisioning through SCIM

Validate Device Posture in Adaptive Access Policy Controls

Netskope can evaluate if the CrowdStrike Falcon agent processes are running on Windows and macOS endpoints and apply adaptive access control policies based on the result. For example, Netskope One SSE can allow uploads to cloud services only from endpoints that are secured by the Falcon platform.

Device posture can be combined with application risk, application activity, company or personal application instance, user confidence index scoring, data sensitivity, and other variables for content and context in adaptive access control policies to provide least privilege access based on Zero Trust principles.

Together, Netskope and CrowdStrike integrate to provide a secure hybrid work environment for any user, device, or location in support of your transformation steps and Zero Trust principles.

About CrowdStrike

CrowdStrike (Nasdaq:CRWD), a global cybersecurity leader, protects critical areas of enterprise risk: endpoints, cloud workloads, identity, and data. Powered by world-class AI and threat intelligence, the CrowdStrike Falcon® platform delivers automated protection, hyper-accurate detections, and reduced complexity via a single lightweight agent.

Learn more: www.crowdstrike.com

CROWDSTRIKE