Solution Brief

Netskope and CrowdStrike

By integrating the Netskope One platform and the AI-native CrowdStrike Falcon platform, IT and security teams can seamlessly share threat intelligence and risk scores, unify visibility across web, cloud services, private applications, and validate device posture in adaptive Security Service Edge (SSE) policy controls to streamline security operations and safeguard against advanced threats.

Key Use Cases

- **Exchange Threat Intelligence.** Automate bi-directional sharing of indicators of compromise (IOCs) for threat intelligence between solutions with Cloud Threat Exchange.
- **Export Logs for Investigations.** Unify visibility and response for enhanced investigations with near real-time log streaming using Netskope Cloud Log Shipper.
- **Enable Zero Trust Principles.** Exchange and normalize risk scores for users and devices between solutions with Cloud Risk Exchange.
- **Validate Device Posture.** Ensure secure agent posture with adaptive policy controls for web and cloud access.
- **Seamless Integration Experience.** The Netskope Cloud Exchange platform provides ready-to-use plug-ins between solutions for fast time-to-value.

"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

In today's cybersecurity landscape, organizations grapple with escalating costs and technology stack complexity driven by multiple point products, creating gaps in visibility and weakening overall security posture. Without unified defenses and context surrounding threats, organizations are left open to potentially catastrophic consequences, as adversaries exploit vulnerabilities to compromise assets, data, and reputation, incurring long-term damage and additional costs.

In addition to the need for multiple layers of threat and data protection are the enactment of Zero Trust principles to remove implicit trust, enable least privilege access, and continuously monitor to refine controls – all in an environment shifting with network, security, application, and data transformations.

The Solution

Netskope and CrowdStrike

The Netskope Intelligent SSE and the CrowdStrike Falcon platform deliver multiple integrations for a seamless security stack to protect devices, users, apps, and data. With deep visibility, Netskope inspects across ALL traffic, including web and SaaS applications, cloud services, and private applications with powerful access controls, threat and data protection capabilities. The Falcon platform delivers advanced protection for critical areas of enterprise risk – endpoints, workloads, identities and data – with its single lightweight agent and unified AI-native platform. The CrowdStrike and Netskope integrations empower organizations to unify SSE with rich security telemetry and response capabilities from across the enterprise in the Falcon console for accelerated threat investigations.

netskope

CROWDSTRIKE

Exchange Threat Intelligence Between CrowdStrike and Netskope

Netskope Cloud Threat Exchange (CTE) enables a The Netskope Cloud Threat Exchange (CTE) module enables a seamless plug-in integration to automatically share IOCs including malicious URLs, file hashes and DLP file hashes between CrowdStrike and Netskope. Organizations benefit from near real-time intelligence across both platforms to neutralize threats faster with the ability to manage IOCs within CTE including the validity of IOCs, e.g., stale, old, or unused. Netskope CTE also utilizes shared threat intelligence across multiple domains, providing a holistic perspective on threats within the environment.

CTE is a private integration for a customer's own security stack, no charge to Netskope customers, and has proven its scale and performance managing over 1 million IOCs per day for a multinational firm. Customers with managed security services may opt to have CTE managed where it remains a private integration between defenses.

Netskope Advanced Threat Protection includes multiple detection engines that detect sophisticated zero-day threats and targeted attacks, including advanced threat detection engines such as: anti-malware, heuristics and pre-execution analysis, multi-stage cloud sandboxing, and machine learning (ML)-based malware classifiers for portable executable (PE) files, Office files, PDF files, and malicious URLs in files. For threats detected in the background, Patient Zero alerts are provided for exposed users to determine if a file has been seen by Netskope and to know its malicious or benign status, and sandboxing includes MITRE ATT&CK® analysis. Threat prevention also includes a web intrusion prevention system (IPS), remote browser isolation (RBI) of risky websites, and cloud firewall policy controls on egress traffic.

> CTE [Cloud Threat Exchange] has proven its scale and performance managing over 1 million IOCs per day for a multinational firm.

Export Netskope Logs for CrowdStrike Falcon Next-Gen SIEM Investigations, AI Correlation

Netskope integrates with the Falcon platform to share relevant Netskope event logs and alerts for cloud security edge activity to improve visibility and unify telemetry from endpoints and additional domains. The Netskope Cloud Log Shipper (CLS) module provides a seamless integration for high-performance log export

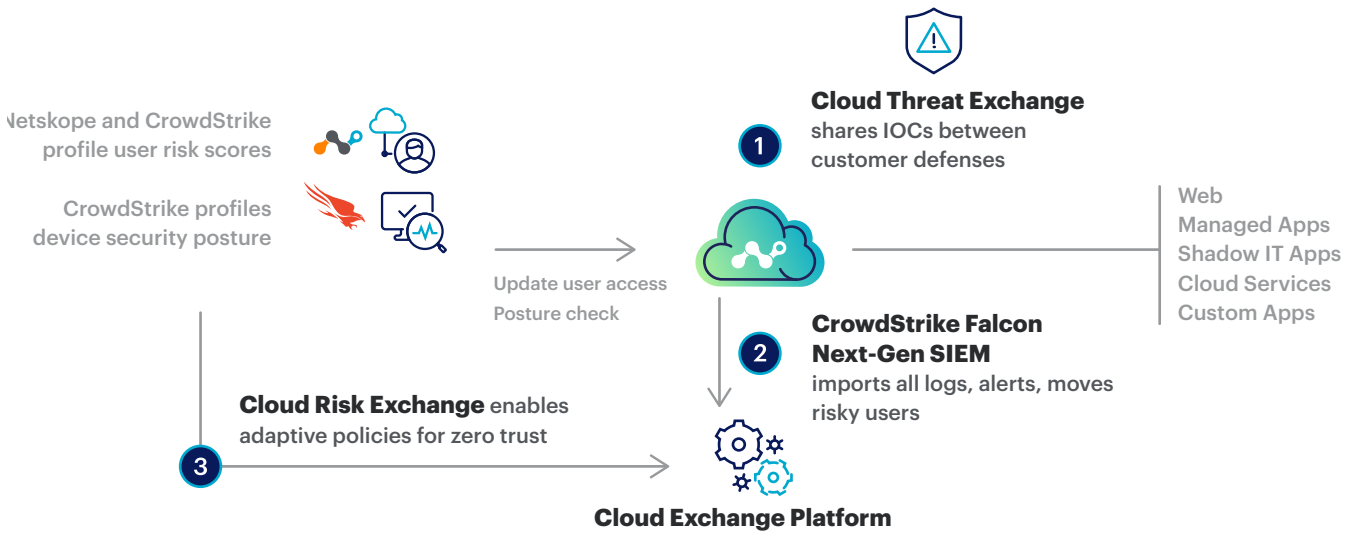
> Netskope Cloud Log Shipper (CLS) provides a seamless integration for high performance log export for timely response and investigations with CrowdStrike.

for timely response and investigations with CrowdStrike. This sharing of intelligence maximizes cross-platform effectiveness for accelerated investigations and reduces time to remediate.

Ingestion of Netskope event logs and alerts into the Falcon platform, with log management and next-generation SIEM capabilities, enables enhanced observability via dashboards, parsers, and saved searches to answer relevant questions with added context, allowing analysts to explore threats and vulnerabilities and gain valuable insights from all logs in real time. Alerts can then be set to initiate desired workflows to streamline operations.

Netskope event logs contain rich details for user web traffic, managed apps, shadow IT unmanaged apps, cloud platform services, and public-facing custom apps. Details also include company versus personal app instances, app risk and app activity.

Joint customers of Netskope and CrowdStrike can use the integration for optimized real-time threat detection, investigation, response and hunting through the seamless ingestion and correlation of relevant telemetry to stop the most sophisticated attackers and novel threats.



Enable Zero Trust Principles Across Your Integrated Security Stack

At the heart of Zero Trust principles are removing implicit trust, enabling least privilege access, and continuously monitoring to refine policy controls. Netskope and CrowdStrike support these principles across endpoints and security service edge activity, while exchanging risk scores via the Netskope Cloud Risk Exchange (CRE) module. Netskope Intelligent SSE calculates a user confidence index (UCI) score based on user activity, alerts, events, anomalies, and machine-learning correlations. UCI scoring can be used in adaptive policy controls to support Zero Trust principles and be exchanged via CRE with CrowdStrike Falcon.

The CrowdStrike Falcon Zero Trust Assessment (ZTA) provides real-time insight into device health regardless of location, network, and user – and across a variety of touchpoints including hardware, firmware, and operating systems – sharing actionable risk scores to enforce real-time conditional access to resources. The Falcon ZTA scores support Zero Trust principles and can be exchanged via CRE with Netskope.

Netskope CRE also creates a single view into multiple connected systems' risk values for individual users and devices. As scores are consumed into the CRE database, they are mapped to a normalized value range and can be weighted as needed to create a single score per user, and a daily average across all users/devices.

Finally, Netskope CRE working in conjunction with the Falcon platform can assess Falcon ZTA scores and trigger reclassification of the device based on its overall risk, enabling Netskope to continuously (or as scheduled) reassess device posture and apply the appropriate policy.

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 Intelligence 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, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, 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.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

CROWDSTRIKE