Solution Brief

Netskope and CrowdStrike

Modern security architecture is increasingly built around the integration of endpoint and security service edge (SSE) solutions. Netskope and CrowdStrike integration shares threat intelligence, exchanges risk scores, exports Netskope event logs for XDR investigations, and validates device posture in adaptive SSE policy controls. Netskope Cloud Exchange modules simplify the integration process and automate workflows.

Key Use Cases

- **Exchange Threat Intelligence.** Automate bi-directional IOC sharing for threat intelligence between solutions with Cloud Threat Exchange.
- **Export Logs for Investigations.** Update XDR for 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 endpoint agent posture in adaptive policy controls for web and cloud access.
- **Seamless Integration Experience.** Cloud Exchange modules provide ready to use plug-ins between solutions.

> "With Netskope [and CrowdStrike] we are protecting devices anywhere, anytime."
>
> Systems Architect,
> Large Enterprise Healthcare Company

The Challenge

Protecting users, devices, apps, and data in a hybrid work environment no longer defined with perimeters requires seamless integration and automation between security defenses. A symbiotic security stack needs to interoperate using content and context, threat intel, activity logs, risk scores, and device posture awareness.

Alongside 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 providing a great user experience for any device or location.

The Solution

Netskope and CrowdStrike

Netskope Intelligent SSE and CrowdStrike Falcon platforms leverage multiple integrations for a seamless security stack to protect devices, users, apps, and data. Netskope inspects five lanes of user traffic for web, SaaS, Shadow IT, IaaS, and custom apps with multiple threat and data protection defenses. CrowdStrike Falcon protects endpoints on or off networks with a light-weight agent and cloud scale AI as one of the largest data platforms for security. Netskope is also part of the CrowdStrike XDR Alliance to share cross-platform intelligence and speed investigations.

netskope CROWDSTRIKE

Exchange Threat Intelligence Between CrowdStrike and Netskope

Netskope Cloud Threat Exchange (CTE) enables a seamless plug-in integration to automatically share IOCs including file hashes and malicious URLs between CrowdStrike and Netskope. Customers benefit from real-time intelligence across both platforms to neutralize threats faster with the ability to manage IOCs within CTE including decay time. CTE also incorporates threat intel from other security defenses, threat intelligence providers, IOC sharing services, XDR, SIEM, and SOAR platforms.

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 anti-malware, heuristics and pre-execution analysis, multi-stage cloud sandboxing, and ML-based malware classifiers for 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 while the RetroHunt API enables security analysts to determine if a file has been seen by Netskope and its malicious or benign status, and sandboxing includes MITRE ATT&CK analysis. Threat prevention also includes web 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 XDR Investigations

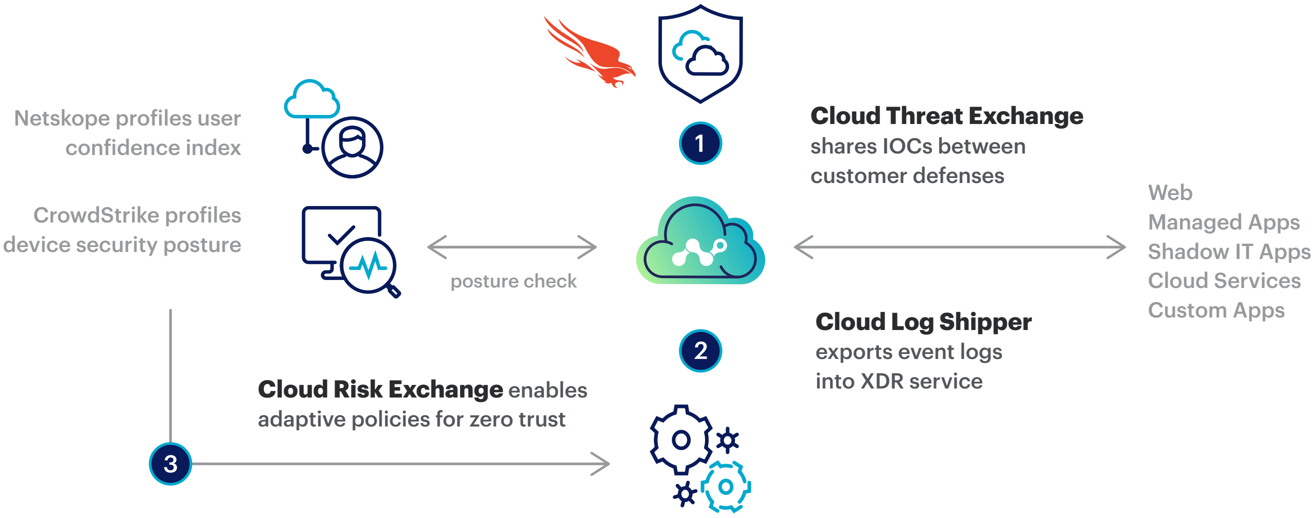
As a part of the CrowdStrike XDR Alliance, Netskope integrates with CrowdStrike to share relevant Netskope event logs and alerts for cloud security edge activity to improve visibility and combine telemetry from endpoints. This sharing of intelligence maximizes cross-platform effectiveness for accelerated investigations and reduces time to remediate.

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

Ingestion of Netskope event logs and alerts into the Humio database is the first step into XDR by enabling enhanced observability via dashboards, parsers, saved searches to answer relevant questions with added context, 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 traffic of web, 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. Netskope Cloud Log Shipper (CLS) provides a seamless integration for high performance log export for timely response and investigations with CrowdStrike.

Joint customers with both solutions using CLS will benefit from optimized real-time threat detection, investigation, response and hunting through the seamless ingestion and correlation of relevant telemetry to stop the most sophisticated of attackers and novel threats.


Netskope profiles user confidence index
CrowdStrike profiles device security posture
posture check
1
Cloud Threat Exchange shares IOCs between customer defenses
Web
Managed Apps
Shadow IT Apps
Cloud Services
Custom Apps
2
Cloud Log Shipper exports event logs into XDR service
3
Cloud Risk Exchange enables adaptive policies for zero trust

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 controls. Netskope and CrowdStrike support these principles across endpoints and security service edge activity, plus integrate to exchange risk scores with Netskope Cloud Risk Exchange (CRE).

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 and other security solutions.

CrowdStrike Falcon calculates a zero-trust assessment (ZTA) for endpoints delivering real-time security posture assessments across all endpoints regardless of location, network, and user -- and across a variety of touchpoints including endpoint hardware, firmware, and operating system versions -- to produce an actionable risk score. ZTA scoring supports zero trust principles and can be exchanged via CRE with Netskope and other security solutions.

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 Falcon can assess ZTA score 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 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 endpoint devices that are secured by CrowdStrike Falcon.

Device posture can be combined with app risk, app activity, company or personal app 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® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

CROWDSTRIKE

netskope

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything, visit netskope.com.