SOLUTION BRIEF

Netskope Cloud Exchange

The Netskope Cloud Exchange (CE) provides customers with powerful integration tools to leverage investments across their security posture. CE consumes valuable Netskope telemetry and external threat intelligence and risk scores, enabling improved policy implementation, automated service ticket creation, and exportation of log events from the Netskope Security Cloud.

KEY USE CASES

- **Share threat intelligence.** Automate bidirectional IOC sharing between your defenses including Netskope, endpoints, email gateways, and SIEMs.
- **Automate service tickets.** Improve workflows where Netskope alerts create service tickets in IT service management and collaboration tools.
- **Exchange risk scores.** Normalize multiple risk scores and invoke investigations for significant changes in user or device risk scoring.
- **Export logs.** Improve security operations with rich event and alert logs into your SIEM, data lake, or XDR/MDR service.

> **"The path forward is a security overlay based on Zero Trust principles to protect sensitive data on the web and in the cloud."**
>
> **Netskope Cloud and Threat Report, July 2021**

THE CHALLENGE

Remote working is the new normal, putting users, apps, and data at the center secured by a security services edge (SSE) with identity services, detection and response, and endpoint integrations. Organizations require integration tools with ready-to-use plug-ins for their SSE cloud architecture.

Given more than half of web traffic is now cloud related and two-thirds of employees are working remote, on-premises security appliances are less than ideal. The impact is security stack consolidation into cloud SSE platforms creating new integration points. While customers face similar challenges of timely threat intelligence, workflow automation, and collecting logs, they also desire to analyze app, user, and identity risk scores for adaptive policy controls in relation to Zero Trust principles.

THE SOLUTION

Netskope partners across the cybersecurity ecosystem with email security, endpoint security, identity services, SIEM, SOAR, and IR solutions, enabling customers to deploy an integrated and automated cloud security stack. CE enables Netskope customers to easily share threat intelligence, automate service tickets from alerts, exchange and normalize risk scores, plus export web and cloud logs. The net result of leveraging CE is consolidation, less complexity, faster time to action, and a lower cost of operations.

CLOUD THREAT EXCHANGE

Netskope Cloud Threat Exchange (CTE) is a near real-time threat ingestion, curation, and sharing tool that enables Netskope customers and technology partners to bidirectionally exchange IOCs. Security teams can integrate up-to-the-minute intelligence feeds that contain malicious URLs and file hashes, plus DLP file hashes, into their security infrastructure products, such as endpoints, firewalls, secure web gateways, and cloud access security brokers.

CTE is a lightweight application that ingests, manages, and shares threat IOCs and DLP file hashes as part of the CE platform. Sharing threat intelligence is configurable between any two connected systems. For instance, a customer can facilitate sharing between different security solutions or even multiple Netskope cloud tenants within their security stack.

> **CTE is a near real-time threat ingestion, curation, and sharing tool that enables Netskope customers and technology partners to bidirectionally exchange IOCs.**

The CTE dashboard provides information on how frequently IOCs have been seen and from what systems, enabling customers to determine the scope of an attack surface. Customers can also configure when IOCs are timed-out due to staleness, plus choose which IOC sources to trust when they are provided with conflicting (e.g., “safe” versus “suspicious”) information.

Ready-to-use CTE plug-ins include: CrowdStrike, Cybereason, FireEye (using API module from Helix), GitHub (for DLP prevention), Microsoft Defender, Microsoft MCAS, Mimecast, Proofpoint, SentinelOne, ServiceNow, ThreatQuotient, VMware Carbon Black, plus STIX/TAXII, MISP, and the sample plug-in.

CLOUD TICKET ORCHESTRATOR

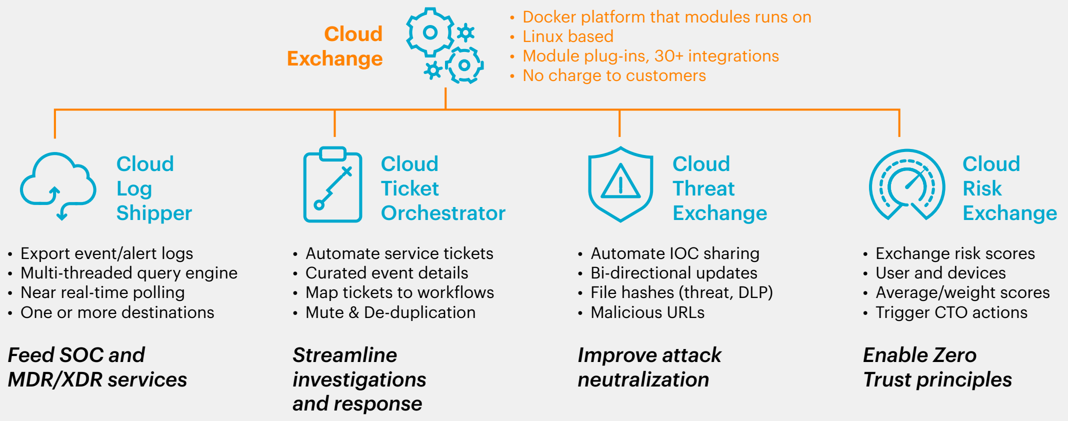
Netskope Cloud Ticket Orchestrator (CTO) enables your organization to programmatically and automatically open tickets on IT service management (ITSM) and collaboration systems, streamlining how the tickets are made and effectively mapping them to workflows in those systems.

Set business rules within CTO for intelligent service ticket creation based on alerts issued by Netskope. Automatically map tickets to specific workflows in your preferred ITSM or collaboration system and minimize noise by curating the type and volume of ticket notifications you want to see through Mute and Deduplication features.

Improve and automate process workflows by turning threat and data protection alerts into tickets with curated event details to aid investigations and response. Plus, link business rules to ITSM and SecOps investigation queues so that the system can instantiate tickets at different places on a single platform without creating multiple configurations in CTO. Within CTO, see a list of all tickets or notifications created in connected systems, including metadata about the ticket and a URL link to the ticket in the other system, plus sort and filter tickets created and drill into each ticket.

Ready-to-use CTO plug-ins include: Atlassian Jira, ServiceNow (ITSM and SecOps), Slack, PagerDuty, Twilio, and generic email, plus other compliant notification systems.

> **Improve and automate process workflows by turning threat and data protection alerts into tickets with curated event details to aid investigations and response.**



Cloud Exchange

- Docker platform that modules runs on
- Linux based
- Module plug-ins, 30+ integrations
- No charge to customers

Cloud Log Shipper

- Export event/alert logs
- Multi-threaded query engine
- Near real-time polling
- One or more destinations

Feed SOC and MDR/XDR services

Cloud Ticket Orchestrator

- Automate service tickets
- Curated event details
- Map tickets to workflows
- Mute & De-duplication

Streamline investigations and response

Cloud Threat Exchange

- Automate IOC sharing
- Bi-directional updates
- File hashes (threat, DLP)
- Malicious URLs

Improve attack neutralization

Cloud Risk Exchange

- Exchange risk scores
- User and devices
- Average/weight scores
- Trigger CTO actions

Enable Zero Trust principles

CLOUD RISK EXCHANGE

Netskope Cloud Risk Exchange (CRE) 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. By leveraging business logic, security analysts can match individual scores, score combinations, or weighted scores as nested, plus define triggers to send notifications via CTO plug-ins to ITSM and collaboration systems.

The CRE dashboard displays the average score of all tracked users or devices, the scores from the previous day and today with a delta between these scores, and the score trend over a configurable time frame. The dashboard also displays the top 10 riskiest users with the ability to filter and find individual user or device weighted scores and adjust as required. Individual plug-in weighting can be modified with the ability to test and validate the effect by observing the predicted new percentage of each risk category.

CRE supports Zero Trust principles to investigate user and device risk profiles of interest leveraging CTO automated workflows. Ready-to-use CRE plug-ins include: CrowdStrike (device), Netskope (user), Proofpoint (user), and SecurityAdvisor (user).

CLOUD LOG SHIPPER

Netskope Cloud Log Shipper (CLS) enables organizations to export the rich event logs from Netskope inline and out-of-band security solutions into SIEMs, data lakes, and syslog formats. Security operations centers (SOCs) and XDR/MDR services can extend their depth of visibility and context with Netskope SSE, NG SWG, CASB, ZTNA, CSPM/SSPM, and CFW solution logs.

CLS regularly and persistently executes polls against the Netskope RESTAPI gateway to extract raw JSON formatted event and alert logs to push a newly formatted version out to one or more receivers, configured as a plug-in. CLS does this using a sophisticated algorithm using a multi-threaded query engine, working within rate limits

(4 queries/second), and handling error responses and datasets larger than its pagination limit (10,000 logs per response) to deliver all requested logs during initial seeding and near real-time activities.

Ready-to-use CLS plug-ins include: AlienVault, Azure Sentinel, CrowdStrike Humio, Google Chronicle, Google Cloud Security Command Center, IBM QRadar, LogRhythm, Micro Focus ArcSight, Microsoft Cloud Application Security, Rapid7, and generic (configurable) SYSLOG CEF.

Netskope also has direct integrations with Exabeam, Securonix, Splunk, and Sumo Logic for log export. Direct cloud storage integrations are available for AWS S3 buckets, Azure Blob storage, and Google Cloud Platform storage.

ABOUT CLOUD EXCHANGE

Netskope Cloud Exchange (CE) platform and the four modules are no charge for customers where one or more modules can be activated at a time. CE is deployed as a docker-based solution wherever Linux can be run and on systems that support docker. Cloud Exchange requires very little compute and storage resources to run—a minimum of two (2) vCPU, 20 GB of storage, and 4 GB of RAM—and has been tested on Ubuntu and CentOS. CE supports most identity services for local login or single sign-on, role-based access controls for the UI and API tokens, access is secured with TLS v1.3 with the option of customer-generated certificates, and provides multi-instance/tenant support for more than one Netskope platform. CE includes automated checks for updated or newly published plug-ins and provides syslog messages to report platform functionality, audit logs, and system errors.

netskope

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, Netskope is fast everywhere, data centric, and cloud smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.