Solution Brief

Netskope Cloud Exchange

Netskope Cloud Exchange (CE) provides customers with powerful integration tools to leverage investments across their security stack. CE consumes valuable Netskope telemetry, external threat intelligence and risk scores, 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, device and application risk scoring.
- **Export logs.** Improve security operations bringing rich event and alert logs into your SIEM, data lake, or XDR/MDR service.

Ensure that all of your security defenses share intelligence and work together to streamline security operations. Netskope customers can use Cloud Exchange to share IOCs, import threat intel, export event logs, automate workflows, and exchange risk scores.

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 log collection, they also need to analyze application, 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, Incident Response, XDR, threat intelligence and network solutions, enabling customers to deploy an integrated and automated cloud security stack. CE has four modules - Cloud Log Shipper (CLS), Cloud Threat Exchange (CTE), Cloud Ticket Orchestrator (CTO) and Cloud Risk Exchange (CRE) that enable Netskope customers to easily export cloud and web logs, share threat intelligence, automate service tickets from alerts, and exchange and normalize risk scores. The net result of leveraging CE is consolidation, less complexity, faster time to action, and lower cost of operations.

Cloud Threat Exchange

Netskope Cloud Threat Exchange (CTE) is a near realtime 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, file hashes and 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. 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: AWS GuardDuty, Carbon Black, CrowdStrike, Cybereason, Feedly, Digital Shadow, GitHub (for DLP prevention), HarfangLab, Google Mandiant, Illumio, Microsoft Defender, Microsoft MCAS, Mimecast, Palo Alto Networks Panorama, Proofpoint, Security Scorecard, SentinelOne, ServiceNow, Skyhigh, Sophos, ThreatConnect, ThreatQuotient, Trend Micro, VMware Carbon Black, plus STIX/TAXII, MISP, and the sample plug-in.

Cloud Ticket Orchestrator

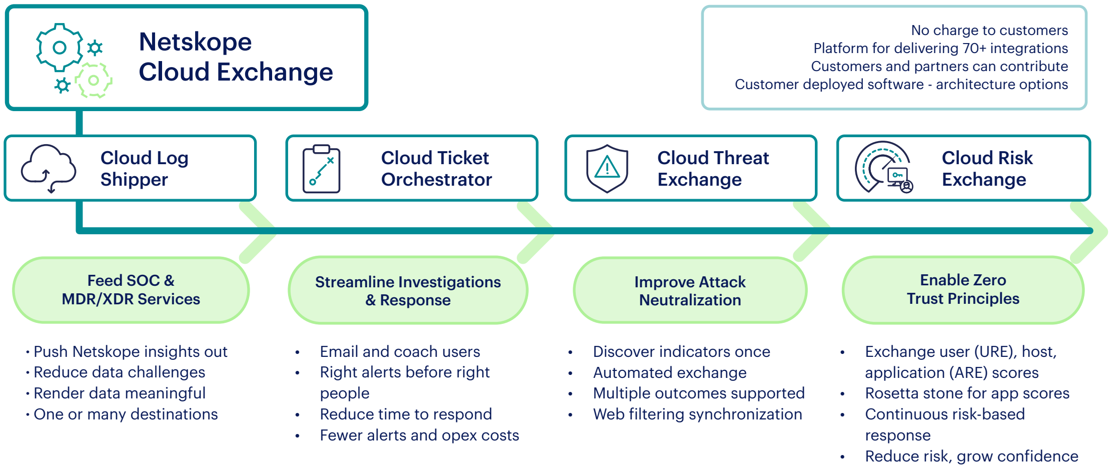
Netskope Cloud Ticket Orchestrator (CTO) enables your organization to programmatically and automatically open tickets on IT service management (ITSM) and collaboration systems, streamlining how the tickets are made and effectively mapping them to workflows in those systems.

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. CTO displays a list of all the tickets or notifications created in connected systems, as well as metadata about the ticket and a URL link to the ticket in the other system. You gain the ability to sort and filter ticket listings and drill down into individual tickets.

Ready-to-use CTO plug-ins include: Atlassian Jira, Microsoft Teams Notifier, ServiceNow (ITSM and SecOps), Slack, PagerDuty, Telegram, Twilio, Webhook, 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.



Netskope Cloud Exchange

No charge to customers
Platform for delivering 70+ integrations
Customers and partners can contribute
Customer deployed software - architecture options

Cloud Log Shipper

Feed SOC & MDR/XDR Services

- Push Netskope insights out
- Reduce data challenges
- Render data meaningful
- One or many destinations

Cloud Ticket Orchestrator

Streamline Investigations & Response

- Email and coach users
- Right alerts before right people
- Reduce time to respond
- Fewer alerts and opex costs

Cloud Threat Exchange

Improve Attack Neutralization

- Discover indicators once
- Automated exchange
- Multiple outcomes supported
- Web filtering synchronization

Cloud Risk Exchange

Enable Zero Trust Principles

- Exchange user (URE), host, application (ARE) scores
- Rosetta stone for app scores
- Continuous risk-based response
- Reduce risk, grow confidence

Cloud Risk Exchange

Netskope Cloud Risk Exchange (CRE) creates a single view into multiple connected systems' risk values for users, devices and applications. 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/or per application and a daily average score across all users/devices and/or applications. 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, devices, or applications, the scores from the previous day and current day with a delta between these scores, and the score trend over a configurable time frame. The dashboard also includes User Risk Exchange (URE) workflows for users and Application Risk Exchange (ARE) workflows for applications, with the ability to filter and find individual user/device or application weighted scores and adjust as required. Individual plugin 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, device and application risk profiles of interest leveraging CTO automated workflows. Ready-to-use CRE plug-ins include: Azure AD, BeyondCorp, BitSight (application), CrowdStrike (device), CrowdStrike Falcon Identity Protection (User), KnowBe4 (user), Mimecast (Training Awareness safe score), Netskope (user), Okta (user) via URE, Proofpoint (user), Security Advisor (user), Security Scorecard (application), ServiceNow (application), and ThirdParty Trust (application).

Cloud Log Shipper

Netskope Cloud Log Shipper (CLS) enables organizations to export 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, ArcSight, AWS Cloud Trail & Security Lake, AWS S3 WebTx, AWS S3 events and alerts, Bitsight ThirdPartyTrust, CrowdStrike LogScale (Humio), Elastic, Google Chronicle, Google Cloud Security Command Center, Google GCP Storage, IBM QRadar, Kafka, LogRhythm, Micro Focus ArcSight, Microsoft Azure Sentinel, Microsoft Azure Monitor, Microsoft Azure Cloud Storage, Microsoft Cloud Application Security, Rapid7, Secureworks, Solarwinds, Syslog and WebTx with Splunk, generic (configurable) SYSLOG CEF, and WebTx.

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) and its four modules are available to all customers. One or more modules may be activated at a time.

1. **Using in-house resources:** Netskope Cloud Exchanve is available to customers at no charge and customers may use in-house resources and staff to deploy and manage the solution. CE is deployed as a docker-based solution wherever Linux can be run and on systems that support docker. CE requires very little compute and storage resources to run—a minimum of 4 vCPU, 4 GB of Memory, 40 GB of storage—and has been tested on Ubuntu, Redhat, 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.
2. **Support for Virtual Machines (VM) and for High Availability (HA) Clusters:** The VM form factor enables organizations to integrate their siloed security solutions across AWS, Azure, GCP & VMware, hybrid/multi-cloud environments. It also provides some hardening by removing the need for CE to connect to Github or Docker.
    - Support for HA with Active-Active clustering enabling resiliency across the CE deployment with a minimum of 3 nodes.
    - Improved performance to maximize throughput. Improved diagnostics for effective troubleshooting/debugging saving valuable time and effort.