LogRhythm

Joint Solution Brief

LogRhythm and Netskope

Benefits

- Accelerate detection of URLs and files that should be restricted or quarantined
- Allow administrative manual and automated custom functionality
- Speed response with enhanced investigative capabilities

Solution Overview

To stay on top of threats, it's important to understand what's occurring in your network. LogRhythm has partnered with Netskope to deliver network visibility, real-time data, and threat protection. LogRhythm and Netskope are integrated using the Cloud Log Shipper module of Netskope Cloud Exchange. This enables all or selected event and alert logs from Netskope to be sent to the LogRhythm SIEM platform. The LogRhythm SmartResponse™ integration for Netskope improves threat intelligence feeds by helping analysts automate the quarantining and restriction of suspicious URLs and files.

As logs are ingested into LogRhythm SIEM, the LogRhythm SmartResponse for Netskope uses the Netskope RESTful API to add suspicious URLs, files, and SHA-256 hashes to Netskope's restrict list or collection of quarantined files. This can be performed from custom LogRhythm AI Engine rule sets or manually from the Web Console. The SmartResponse also stores a local copy in the LogRhythm List Manager. If a threat feed indicates questionable browsing habits in LogRhythm, a security analyst can use the SmartResponse to add the suspicious URL or file to the LogRhythm list and Netskope's custom URL or file lists.

netskope

About LogRhythm and Netskope

LogRhythm and Netskope have formed a strategic partnership to help organizations around the globe enhance their security and integrate with existing infrastructure to offer unified protection. LogRhythm offers extensive support and integration across Netskope's products, which offers cloud-native solutions to businesses for data protection and defense against threats in cloud applications, cloud infrastructure, and the web. Together, LogRhythm and Netskope empower security teams to navigate a changing threat landscape with confidence.

Log Collection

Securing any security operations center (SOC) begins with high-fidelity and trustworthy log data. While other vendors outsource their log collection taxonomy to the SOC analyst, LogRhythm provides normalized log source data curated by dedicated security experts with dozens of years of security experience. Netskope's integration with LogRhythm is enabled by Netskope Cloud Log Shipper, which regularly polls the Netskope API gateway to extract raw event and alert logs and quickly forwards them via Syslog.

The LogRhythm Machine Data Intelligence (MDI) Fabric normalizes structured and unstructured data. Our security teams review these sources and ensure that relevant security data is normalized with other consumable security data. The results are trusted logs and alerts that allow for precision rule creation and comprehensive remediation efforts in the event of an attack.

How It Works

LogRhythm SIEM collects logs from every device, application, and sensor in an environment. MDI Fabric classifies and contextually structures every log message.

LogRhythm ingests Netskope logs into LogRhythm SIEM. Data is then parsed and normalized to the LogRhythm schema using features such as our patented TrueTime™ process, which records the actual time of occurrence, automatically correcting time zone, device clock offsets, and collection offsets. Normalized data is used by LogRhythm SIEM for analysis, storage, and reporting via a consolidated dashboard of all security events. If an alarm is detected, it is logged and displayed in LogRhythm's Web Console for centralized investigation and action.

How Automated Workflows Work

To streamline security response workflows, organizations can use SmartResponse which is part of LogRhythm's security orchestration, automation, and response (SOAR) solution. LogRhythm's SmartResponse accelerates response to cyberattacks to minimize damage, eliminating manual intervention by security analysts. This advanced capability is delivered to end users through the SmartResponse for Netskope. While LogRhythm has a dedicated engineering team that builds actions, this is by nature an open framework that enables Netskope customers to modify actions or write their own custom integrations to protect their unique IT or OT environments.

The LogRhythm SmartResponse for the Netskope integration contains actions that are configured to automatically trigger in the event of an alarm, or manually through the analyst workflow. The actions can be configured to require approval before execution. For example, an admin may notice malicious file activity alarming on a machine and confirm that it is an abnormality. Using LogRhythm's SmartResponse for Netskope, the admin can manually load the file hash into a file list used for prevention. If the file is detected on other machines and matches the SHA-256 hash, the admin can automatically prevent the file from being added. The same functionality can also be added to specific rule sets, such as the detection of a hacking tool. If detected on a machine, it can automatically be added to the restrict list. Admins can also add URLs for malicious web pages to the restricted list as well. The action and associated use cases are highlighted in the table below.

Action	Description	Use Case
Create Netskope V2 Configuration File	Execute this response and rerun it before using other available actions whenever you change the fixed-value parameter	Functionality must run first, before other SmartResponse functions can execute
Add URL to List	Add a URL or file to a custom list with the option to restrict	Adds URL or file to Netskope's restrict list if found to be suspicious, during an investigation
Block Quarantined Files	Remove the quarantined file	Deletes the quarantined file
Get Alerts	Retrieve alerts generated by Netskope, including policy, DLP, and watch list alerts with provided filter	Displays alerts
Get Quarantined Files	Retrieve quarantined files for a specified time	Displays quarantined files
Remove URL from List	Remove URL or file from Netskope's restrict list	Unrestrict url
Restore Quarantined Files	Restore quarantined files to quarantine profile in Netskope dashboard	Restores files in Netskope quarantined files