Joint Solution Brief

Netskope Security Cloud

LogRhythm Automates Blacklisting of Suspicious URLs and Files

Solution Overview

To stay on top of threats, it's important to understand what's occurring in your network. The LogRhythm SmartResponse™ (SRP) automation plugin for Netskope improves threat intelligence feeds by helping analysts automate the blacklisting of suspicious URLs and files.

As logs are ingested into the LogRhythm NextGen SIEM Platform, the Netskope SRP uses the Netskope RESTful API to add suspicious URLs, files, and SHA-256 hashes to Netskope's blacklist. This can be performed from custom AI Engine rule sets or manually from the Web Console. The SRP 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 Netskope SRP to add the suspicious URL or file to the LogRhythm List and Netskope's blacklist.

Log Collection

Securing any SOC begins with high-fidelity and trustworthy log data. While other vendors outsource their log collection methodology to the SOC analyst, LogRhythm provides log sources reviewed by dedicated security experts with dozens of years of security experience. Netskope's integration with LogRhythm is enabled by Netskope Cloud Log Shipper, which pulls logs from the APIs and forwards them via Syslog.

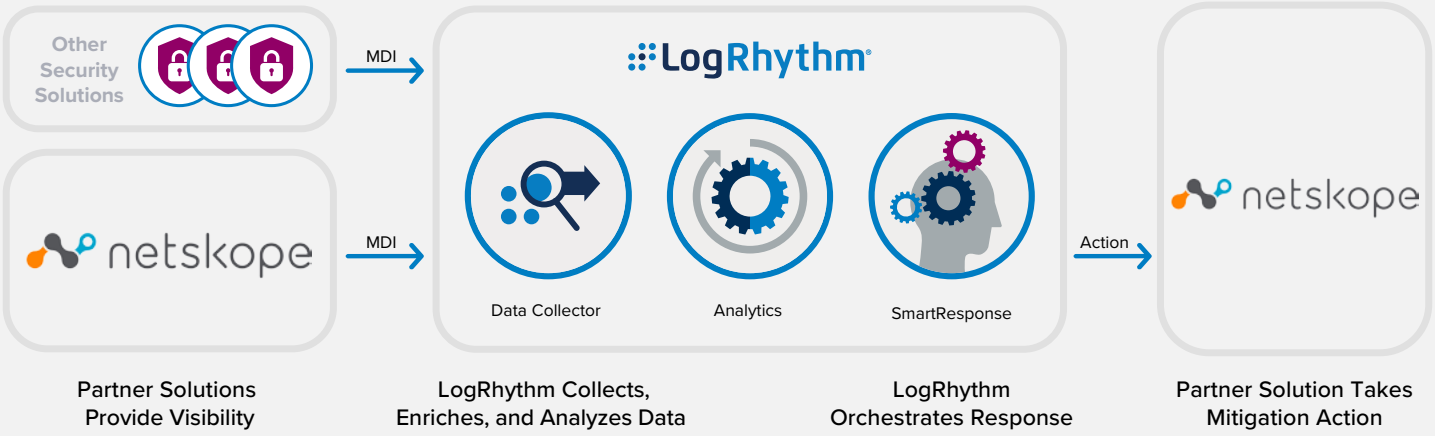
The LogRhythm Machine Data Intelligence (MDI) Fabric optimizes and stabilizes the optimal route of collection for over 1,000 log sources. Our security teams review these sources and ensure that relevant security data is normalized with other consumable security data. The results are trusted logs and alerts that allow for precision rule creation and comprehensive remediation efforts in the event of an attack.

Benefits

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

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 for 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. Our flexible deployment options ensure that you get the best fit for your organization—no matter what your goals and environmental needs may be.



How Data Collection Works

The LogRhythm NextGen SIEM Platform 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 the LogRhythm NextGen SIEM Platform. 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 the LogRhythm NextGen 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 Automation Works

SmartResponse automation accelerates response to cyberattacks, eliminating manual intervention by security analysts. This advanced capability is delivered to end users through a SmartResponse plugin that works with Netskope.

While LogRhythm has a dedicated engineering team that builds plugins, this is by nature an open framework that enables customers to modify plugins or write their own custom integrations to protect their unique IT or OT environments.

The Netskope plugin contains an action that executes automatically in response to an alarm or manually through an analyst's workflow. The action 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 the Netskope SRP, the admin can manually blacklist the file. If the file is detected on other machines and matches the SHA-256 hash, the admin can automatically prevent the file from being added.

An admin can also add the same functionality to a specific rule set such as the detection of a hacking tool. If detected on a machine, it will automatically be blacklisted. Admins can also blacklist URLs for malicious web pages.

The example action and associated use cases are highlighted in the table below.

Action	Description	Use Case
Blacklist URL or File	This action adds the plugin's threat list (URLs and files) to Netskope's blacklisted files and maintains a local copy in the LogRhythm List Manager.	An analyst encounters a suspicious file in the course of an investigation and adds it to Netskope's blacklist. An analyst has a threat feed that alarms on known malicious sites. If detected in the system based on an AIE filter, the Netskope SRP can automatically blacklist the site.

For more information, request a LogRhythm demo.

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301

www.logrhythm.com