Zscaler Internet Access

Streamline website access control with LogRhythm's centralized data collection and automation

Benefits

- Simplify log ingestion and contextualize Zscaler log data
- Accelerate detection of unwanted or deny listed URLs
- Use a single console to investigate and block suspicious website access
- Speed response with enhanced investigative capabilities

Solution overview

Understanding what's occurring in your network and what websites employees are visiting is crucial to protect your organization. With a Zero Trust approach on many organizations' minds, it's imperative to have the right tools to protect networks from threats. The LogRhythm SmartResponse™ for Zscaler Internet Access gives greater insight into network activity and enables remediation actions from the LogRhythm console.

As logs are ingested from Zscaler's Nanolog Streaming Service (NSS) into the LogRhythm SIEM platform, the LogRhythm SmartResponse for Zscaler can automatically blacklist the URL in Zscaler, when a banned keyword or URL is detected. The security administrator can add or obtain information from Zscaler categories (i.e., business use, legal liability, productivity loss, and privacy risk) when investigating suspicious activity via the Web Console or Mediator Server. The team can also use the SmartResponse to create custom categories. If an alarm detects a custom set of rules, users can pull the Zscaler log policy information to add to a LogRhythm alarm for further investigation.

About LogRhythm and Zscaler

LogRhythm and Zscaler work together to help organizations around the globe increase network insight and confront a variety of cloud access security challenges faced by the modern SOC. LogRhythm SIEM and Zscaler Cloud Protection and Internet Access come together to facilitate a modern Zero Trust architecture. LogRhythm and Zscaler empower security teams to navigate a changing threat landscape with confidence. Together, LogRhythm and Zscaler are ready to defend.

Log collection

Securing an organization's systems and networks 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. LogRhythm Machine Data Intelligence (MDI) Fabric optimizes and stabilizes the ideal route of collection for over 950 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.

Zscaler Nanolog streaming service enables the transmission of consolidated user activity logs seamlessly to LogRhythm SIEM in real time. The logs are customizable by analysts for relevancy before being sent to LogRhythm.

How it works

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

Zscaler Nanolog Streaming Service (NSS) collects and consolidates Zscaler DNS, firewall, and web logs from users globally. Security analysts have the ability to customize and configure log filteration for relevancy into the NSS feeds, which specify which logs will be streamed. The logs are then streamed to the LogRhythm platform as syslogs in real time. From there they are 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 then sent to LogRhythm SIEM for analysis, storage, and reporting, via a consolidated dashboard of all security events.

How automated workflows work

To streamline security response workflows, organizations can use LogRhythm SmartResponse™, which is part of LogRhythm's security orchestration, automation, and response (SOAR) solution. SmartResponse can be manually executed in the Web Console and Mediator, as well as attached to custom AI Engine rules in LogRhythm to execute if that alarm rule ever triggers.

The LogRhythm SmartResponse for Zscaler performs several actions including blacklisting a URL, getting policy information, and adding a URL category. It simplifies running actions between the SIEM and Zscaler by centralizing day-to-day security tasks to a single console. Actions and their use cases are provided in the table on the following page.

SmartResponse for Zscaler

Action	Description	Use Case
Create Zscaler SRP configuration file	Execute this response and rerun it before using other available actions whenever you change the fixed-value parameter	Functionality that must be run first, before other SmartResponse functions can execute
Add new URL category	Adds a URL category	Add a new custom URL category
Add URL to category	Adds a URL to existing category	Add a custom URL to an existing category
Denylist URL	Adds a URL to the denylist	Add malicious URL to denylist
Add URL to allowlist	Adds a URL to the allowlist	Add a trusted URL to the allowlist
Get policy information	Displays information about a URL filtering policy	Fetch information about an existing policy
URL lookup	Displays the category for the specified URL	Obtain URL category of a malicious URL
List user	Retrieves a list of all users and allows filtering by name department or group	Displays list of all the users
Remove URL from denylist	Removes the specified URL from the denylist	Remove URL from denylist