Joint Solution Brief

Zscaler Internet Access

LogRhythm's Automated Workflow and Centralized Data Collection Streamline Website Access Control

Solution Overview

Having greater visibility into 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™ plugin (SRP) for Zscaler Internet Access gives you greater insight into network activity and enables remediation actions from the LogRhythm console.

As logs are ingested into the LogRhythm NextGen SIEM Platform, the SRP can automatically blacklist the URL in Zscaler when a banned keyword or URL is detected. Your 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. Your team can also use the plugin to create custom categories. If an alarm detects a custom set of rules, you can pull the Zscaler log policy information to add to a LogRhythm alarm for further investigation.

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.

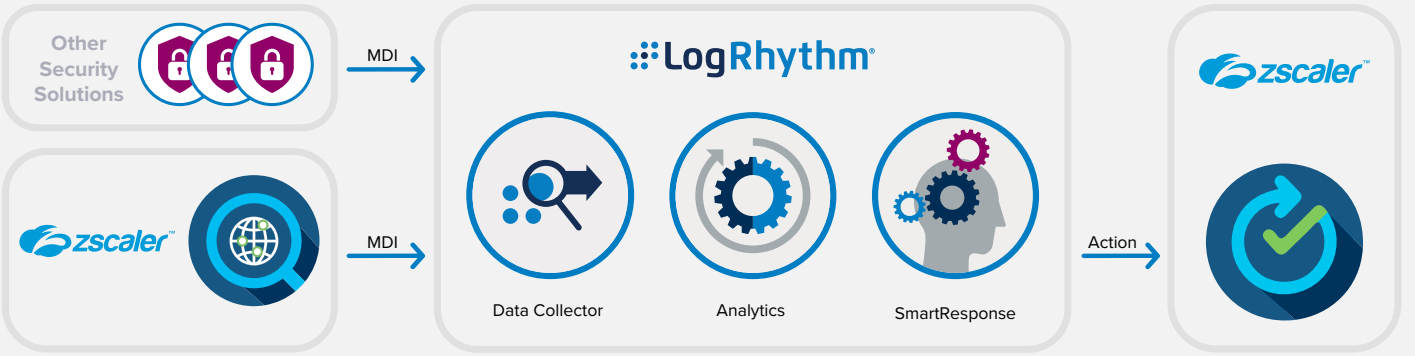
LogRhythm Machine Data Intelligence (MDI) Fabric optimizes and stabilizes the ideal route of collection for over 1,000 log sources. Our security teams review these sources and ensure that relevant security data is normalized with other consumable security data. The results are trusted logs and alerts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

Benefits

- Simplify log ingestion
- Accelerate detection of unwanted/blacklisted URLs
- Use a single console to investigate and block suspicious website access
- Speed response with enhanced investigative capabilities

About LogRhythm and Zscaler

LogRhythm and Zscaler partner to confront a variety of cloud access security challenges faced by the modern SOC. LogRhythm's NextGen SIEM Platform and Zscaler Cloud Protection and Internet Access combine to create a modern Zero Trust architecture that is the security backbone of Fortune 500 companies across the globe.



How Data Collection Works

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

Getting Zscaler logs is simple with the preconfigured dropdown format for LogRhythm. Logs are streamed to the LogRhythm platform where 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 the LogRhythm NextGen SIEM Platform for analysis, storage, and reporting via a consolidated dashboard of all security events.

How Automated Workflows Works

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

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

SmartResponse Actions for Zscaler Internet Access

Action	Description	Use Case
Add URL Category	This action adds a custom url category in Zscaler.	An analyst runs this action to add a new custom URL category.
Blacklist URL	This action adds a URL to the blacklist in Zscaler.	During an investigation, an analyst discovers a potentially malicious URL and runs this action to blacklist it.
Create Zscaler SRP Configuration File	Whenever you change the fixed-value parameters, you must execute this action and rerun it before using the plugin's other available actions.	This is required for the SmartResponse plugin to function.
Get Policy Information	This action displays information about a URL filtering policy.	During an investigation, an analyst runs this action to get information about a policy.
Get URL Category	This action displays the Zscaler category for the specified URL.	During an investigation, an analyst discovers a potentially malicious URL and runs this action to get its Zscaler URL category.
Remove URL From BlackList	This action removes the specified URL from the Zscaler blacklist.	During an investigation, an analyst runs this action to remove the URL from the blacklist.

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

www.logrhythm.com