LogRhythm

Joint Solution Brief

# Cisco Secure Endpoint

## LogRhythm's Automated Workflow and Centralized Data Collection Helps Speed Malware Detection

## Benefits

- Accelerate detection, containment, and removal of advanced malware
- Simplify monitoring via a centralized dashboard
- Standardize and automate response for error-free outcomes

## Solution Overview

The fight against today's advanced threats calls for advanced malware security. Cisco® Secure Endpoint provides comprehensive protection, detection, response, and user access coverage to defend against threats to an organization's endpoints. The integration between LogRhythm SIEM and Cisco Secure Endpoint helps security analysts benefit from the security technology and expertise of two industry leaders and offers organizations increased visibility into threats to their endpoints and enriched context regarding suspicious activities.

Cisco Talos experts analyze millions of malware samples and terabytes of data per day and push that intelligence to Cisco Secure Endpoint which correlates against files, telemetry data, and file behavior. LogRhythm can ingest and normalize data from Cisco Secure Endpoint and perform additional scenario and behavioral-based analytics on this data, as well as incorporating other log and machine data from throughout the environment. Security teams can visualize high-priority events in a dashboard within LogRhythm's centralized console and are empowered to proactively defend against new and emerging threats. Intelligence is further used to help analysts map incidents to MITRE ATT&CK™ techniques, which can assist in the development of mitigation, detection, and response actions.

CISCO

### About LogRhythm and Cisco

LogRhythm and Cisco work together to help organizations around the globe increase network visibility and secure their IT environments. LogRhythm offers extensive support for and integration across Cisco's product portfolio, automatically incorporating, normalizing, and contextualizing log flow and event data captured from over two dozen Cisco products. The combined solution helps security teams to identify behavioral anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence.


## Log Collection

Securing any security operations center (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 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.

## How Data Collection Works

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

When used with Cisco Secure Endpoint, LogRhythm platform connects to the Cisco Secure Endpoint API and collects all available logs. The logs are then parsed and normalized to the LogRhythm schema before they are sent to the LogRhythm SIEM platform for analysis, storage, and reporting via a centralized dashboard of all security events. For example, connection attempts to restrict listed websites will be detected by Cisco Secure Endpoint. This type of connection attempt 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™ automation, which is part of LogRhythm's security orchestration, automation, and response (SOAR) solution. SmartResponse accelerates response to malware threats to minimize damage, eliminating manual intervention by security analysts. This advanced capability is delivered to end users through SmartResponse that works with the Cisco Secure Endpoint. While LogRhythm has a dedicated engineering team that builds actions, this is by nature an open framework that enables Cisco customers to modify actions or write their own custom integrations.

The LogRhythm SmartResponse for Cisco Secure Endpoint contains multiple actions, which are configured to execute automatically in response to an alarm, or manually through analyst workflow. Each action can be configured to require approval before execution.

## SmartResponse Automated Actions for Cisco Secure Endpoint

| Action | Description | Use Case |
|---|---|---|
| Add File to File List | Add a specified file to an existing file list for action | Runs this action to add a suspected malicious file to a blocking file list or a simple detection file list |
| Create Cisco Secure Endpoint 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 |
| Display File Lists | Display available file lists of the specified file list type | Display the available file lists in the specified list category |
| Display Groups | Fetch the list of groups in Cisco Secure Endpoint | List computers that have observed user activities and to display the groups in Cisco Secure Endpoint V2 |
| Get Computers by User Activities | Retrieve info from Cisco Secure Endpoint API for the specified username and display a list of associated computers in the LogRhythm Console | Displays computers based on a specific user's activities |
| Get Events in a Computer's User Trajectory | Display the latest events in specified computer's trajectory. A maximum of 100 events can be listed and filtered by username | Fetch the latest events based on a specific computer's user trajectory |
| Get Infected Computers List | Retrieve vulnerability information from Cisco Secure Endpoint API for the specified SHA-256 hash function and displays a list of potentially infected computers in the LogRhythm Console | Displays a list of potentially infected computers |
| Get Latest Events | Display latest event based on a specific filter.<br>A maximum of 100 events can be listed.<br>The following are available:<br>• No Filter<br>• By Host Name<br>• By Group Name<br>• By Start Date (newer than date) | Displays latest events by computer, group, event type, or date |
| Get Vulnerabilities | Retrieve vulnerability information from Cisco Secure Endpoint for the specified host name and display in the LogRhythm Console | Displays vulnerabilities for the specified host name |
| Isolate Computer | Isolate a specified computer | Isolates a potentially infected computer |

# SmartResponse Automated Actions for Cisco Secure Endpoint

| Action | Description | Use Case |
|---|---|---|
| Move Child Groups into Another Group | Fetch the list of computers that have observed activity and move them into the existing/new group in Cisco Secure Endpoint by their Hostname | Moves the child groups in a specified parent group based on Child and Parent Group |
| Move Computers by Hostname | Fetch list of computers that have observed activity and move them into an existing or new group in Cisco Secure Endpoint by their Hostname | Moves the computer in a specified group the basis of Hostname |
| Move Computer by Internal IP Address | Move computers that have observed malicious activity into the existing/new group in Cisco Secure Endpoint by their IP address | Moves the computer in a specified group based on internal IP |
| Move Computers by User Activities | Fetch list of computers that have observed activity by a given username and move them into the existing/new group in Cisco Secure Endpoint | Moves the computer in a specified group name based on user activities |
| Stop Isolation on Computer | Stop isolation of a computer | Reconnects the previously isolated computer after confirming it is not infected |

**For more information, request a LogRhythm demo.**
**logrhythm.com/schedule-online-demo**

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 330 // +65 6222 8110 // +61 2 8019 7185

**www.logrhythm.com**