Joint Solution Brief

Cisco Secure Endpoint

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

Solution Overview

The fight against today's advanced threats calls for advanced malware security. Cisco® Secure Endpoint provides sophisticated capabilities to protect organizations across the attack continuum: before, during, and after an attack. Integration with the LogRhythm NextGen SIEM Platform builds upon these capabilities, helping security teams centralize detection of malware threats and reduce response time. The LogRhythm NextGen SIEM collects and analyzes Cisco Secure Endpoint logs to help security teams quickly understand the scope of an attack via a centralized dashboard. Attack containment and remediation is accelerated by LogRhythm's automated workflows that trigger action by the Cisco Secure Endpoint.

Technology & Threat Research

The combined solution helps security analysts benefit from the security technology and expertise of two industry leaders. Cisco Talos experts analyze millions of malware samples and terabytes of data per day and push that intelligence to Cisco Secure Endpoint. Cisco Secure Endpoint then correlates files, telemetry data, and file behavior against this context-rich knowledge base to proactively defend against known and emerging threats.

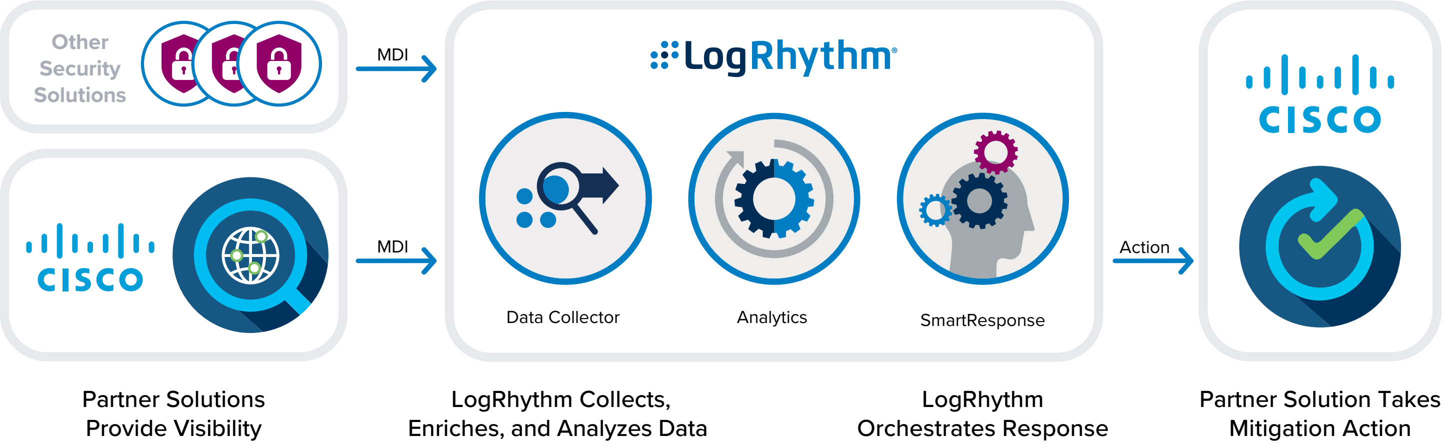
LogRhythm Labs, which developed and maintains the SmartResponse™ for Cisco Secure Endpoint, also provides threat research. Research is core to keeping up with and understanding attacker tactics and techniques. The Threat Research team helps security analysts detect and respond to attacks by creating analytic content such as Threat Detection modules and AI Engine content that ensure environments are adequately protected from new and emerging threats. The team also operationalizes intelligence it gathers from incidents to help analysts map to MITRE ATT&CK techniques that can be used to develop mitigation, detection, and response actions.

Benefits:

- Accelerated detection, containment and removal of advanced malware
- Simplified monitoring via a centralized dashboard
- Standardized and automated response for error-free outcomes

About LogRhythm and Cisco

LogRhythm and Cisco have formed a strategic partnership 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. Our flexible deployment options ensure the best fit for any organization — no matter what the goals and environmental needs may be.


Other Security Solutions
MDI
MDI
LogRhythm
Data Collector
Analytics
SmartResponse
Action
Partner Solutions Provide Visibility
LogRhythm Collects, Enriches, and Analyzes Data
LogRhythm Orchestrates Response
Partner Solution Takes Mitigation Action

How Data Collection Works

The LogRhythm NextGen SIEM Platform collects from every device, application, and sensor in an environment. Our Machine Data Intelligence (MDI) Fabric classifies and contextually structures every log message. The result? Deep intelligence into over 800 unique data source types.

When used with Cisco Secure Endpoint, LogRhythm Open Collector connects to the Cisco Secure Endpoint API and collects all available logs in JSON format. The logs are then parsed and normalized to the LogRhythm schema before they are sent to the LogRhythm NextGen SIEM for analysis, storage, and reporting via a centralized dashboard of all security events. For example, connection attempts to blacklisted websites will be detected by Cisco Secure Endpoint. This type of connection attempt is logged and also 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 a SmartResponse plugin that works with the Cisco Secure Endpoint. While LogRhythm has a dedicated engineering team that builds plugins, this is by nature an open framework that enables Cisco customers to modify plugins or write their own custom integrations.

The Cisco Secure Endpoint plugin 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. Example actions and their use cases are provided in the table on the next page.

SmartResponse Actions for Cisco Secure Endpoint

Action	Description	Use Case
Add File to File List	This action adds a specified file to an existing file list for action.	An analyst runs this action to add a suspected malicious file to a blocking file list or a simple detection file list.
Create Cisco Secure Endpoint V1 Configuration File	Whenever a fixed-value parameters change, analysts must execute this action and rerun it before using the plugin's other actions.	This is an action that is required for all use cases. It allows other action items to use custom API credentials.
Display File Lists	This action displays the available file lists of the specified file list type.	An analyst runs this action to view the available file lists in the specified file list category.
Get Computers by a User's Activities	This action retrieves information from Cisco Secure Endpoint API for the specified username and displays a list of associated computers in the LogRhythm Console.	An analyst runs this action to get computers based on a specific user's activities.
Get Events in a Computer's User Trajectory	This action displays the latest events in a specified computer's trajectory. A maximum of 100 events can be listed and filtered by username.	Analysts use this action to get the latest events based on a specific computer's user trajectory.
Get Infected Computers List	This action retrieves 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.	After an Alarm trigger indicates suspicious activity, an analyst runs this action to view a list of potentially infected computers.
Get Latest Events	This action displays the latest events based on a specified filter. A maximum of 100 events can be listed with filtering options such as: • No Filter • By Event Type • By Host Name • By Start Date (newer than date) • By Group Name	After an alarm trigger indicates suspicious activity, an analyst runs this action to view the latest events by computer, group, event type, or date.
Get Vulnerabilities	This action retrieves vulnerability information from Cisco Secure Endpoint API for the specified host name and displays it in the LogRhythm Console.	After an alarm trigger indicates suspicious activity on a host, an analyst runs this action to view vulnerabilities for the specified host name.
Isolate Computer	This action isolates the specified computer if isolation is available for it. To perform this action, analysts must have read-write access to the Cisco Secure Endpoint API.	An analyst runs this action to isolate a potentially infected computer.
Stop Isolation on Computer	This action stops isolation of the specified computer. To perform this action, analysts must have read-write access to the Cisco Secure Endpoint API.	An analyst runs this action to stop isolation of a computer after confirming it is not infected.

For more information, request a LogRhythm demo.

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