LogRhythm® vmware®

Joint Solution Brief

VMware Carbon Black Cloud Endpoint Standard

LogRhythm's Centralized Data Collection and Automation Boosts Protection Against Modern Cyberattacks

Solution Overview

Threat actors today are employing more sophisticated attacks with the end goal to inflict damage. This is where VMware Carbon Black Cloud Endpoint Standard can help. The VMware Carbon Black solution is a next-generation antivirus (NGAV) and endpoint detection and response (EDR) solution that protects against the full spectrum of modern cyberattacks. By using VMware Carbon Black Cloud's universal agent and console, the solution applies behavioral analytics to endpoint events to help users detect, prevent, and respond to cyberattacks.

Integrating with the LogRhythm NextGen SIEM Platform enables SOC teams to use a single pane of glass to oversee Carbon Black and other disparate security solutions. LogRhythm collects and analyzes file and folder data with other flow, event, and machine data. Analysts are alerted to suspicious activity via LogRhythm's prebuilt endpoint activity dashboard and orchestrate action by the VMware Carbon Black Cloud Endpoint Standard agent and other security elements.

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.

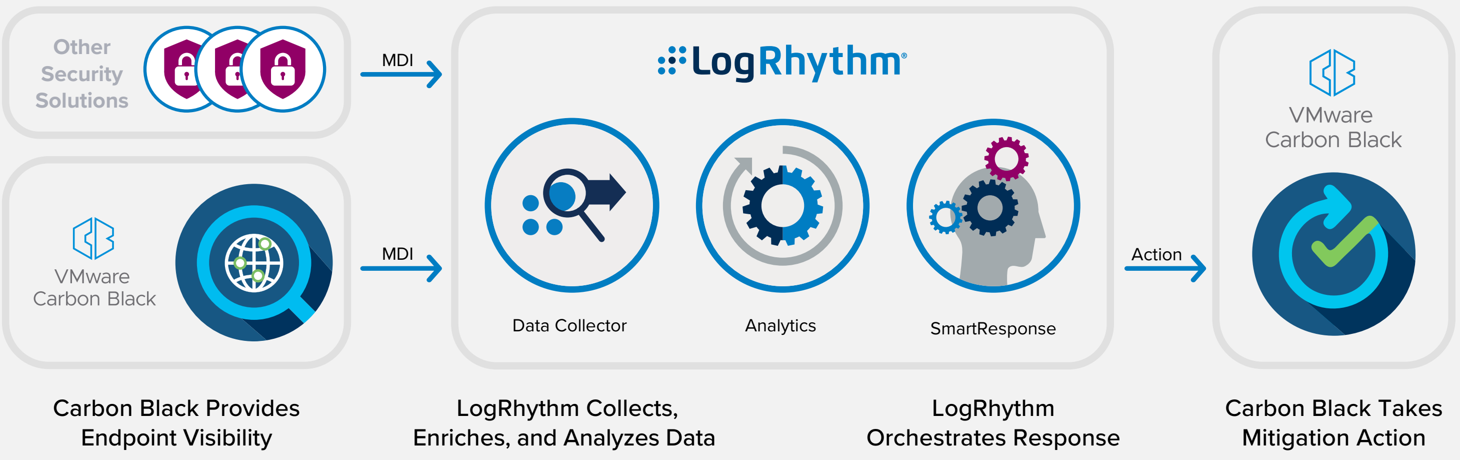
The Machine Data Intelligence (MDI) Fabric that optimizes and stabilizes the optimal route of collection for over 1000 log sources. Our security teams review these sources and ensure that relevant security data is normalized with other consumable security data. The results are trusted logs and alerts that allow for precision rule creation and comprehensive remediation efforts in the event of an attack.

Benefits

- Simplify management of security issues within multivendor environments via a single pane of glass
- Enhance data collection and analytics for dashboard alerting and investigation
- Reduce time to threat detection with automated response

About LogRhythm and Carbon Black

LogRhythm and Carbon Black are working together to help organizations around the globe increase network visibility and protect against modern cyberattacks. LogRhythm offers extensive support for and integration across Carbon Black's product portfolio. The combined solution empowers security teams to identify behavioral anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence.


Other Security Solutions
VMware Carbon Black
MDI
MDI
LogRhythm
Data Collector
Analytics
SmartResponse
Action
VMware Carbon Black
Carbon Black Provides Endpoint Visibility
LogRhythm Collects, Enriches, and Analyzes Data
LogRhythm Orchestrates Response
Carbon Black Takes Mitigation Action

How Data Collection Works

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

LogRhythm centrally collects Carbon Black logs using the VMware Carbon Black API. The logs are 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 then sent to the LogRhythm NextGen SIEM for analysis, storage, and reporting via a consolidated dashboard of all security events. For example, when an Alarm triggers and indicates suspicious activity on a device, an analyst can use a device ID to verify the status of that device to guide further action. This type of connection attempt 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 the Carbon Black's solutions. 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.

The Carbon Black Cloud Endpoint Standard 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 following page.

SmartResponse Actions for VMware Carbon Black Cloud Endpoint Standard

Action	Description	Use Case
Change Device Status	This action applies a policy to a Carbon Black endpoint.	After an Alarm triggers, indicating suspicious activity, an analyst uses a device ID and policy name to apply a policy on a Carbon Black device.
Create Carbon Black Defense 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.	Required to be filled out in order for all other actions to work.
Create Policy	This action creates a policy in Carbon Black Cloud Endpoint Standard.	After an Alarm triggers that indicates suspicious activity on a host, an analyst uses this action to create a specific policy in response.
Delete Device	This action deletes a specified device.	An analyst may need to delete the device.
Delete File	This action deletes a specified file or directory on a target host.	An analyst discovers unnecessary or potentially malicious files on a host and runs this action to delete them.
Device Status	This action queries the device status of a target host.	After an Alarm triggers that indicates suspicious activity on a device, an analyst uses a device ID to check the status of that device and guide further response.
Directory List	This action lists directories or files in a specified directory path.	An analyst runs this action to get a full list of files within a directory and compares the results to a list of known malicious files.
Dump Memory	This action performs a full memory dump of a target host.	After an Alarm triggers that indicates suspicious activity on a host, an analyst runs this action to dump the memory on the host and send a dump file to a specified output target.
Get File	This action copies a specified file to a designated output location.	An analyst runs this action to quickly copy the contents of a file from one machine to another for forensic imaging.
Kill Process	This action kills a specified process on a target host.	An analyst determines that a process is unnecessary and runs this action to kill it.
Process List	This action lists all processes on a specified host.	After an Alarm triggers that indicates suspicious activity on a host, an analyst uses a device ID to get a list of all processes running on that host.
Quarantine Device	This action quarantines a specified device.	An analyst runs this action to quarantine the device.

For more information, request a LogRhythm demo.