LogRhythm

Joint Solution Brief

VMware Carbon Black Enterprise EDR

Speed threat detection and remediation within online, connected environments

Benefits

- ✓ Accelerate investigations with continuous endpoint visibility
- ✓ Simplify security monitoring and alerting of multi-vendor environments via a centralized dashboard
- ✓ Integrating for easy deployment, automated updates, and elastic scalability

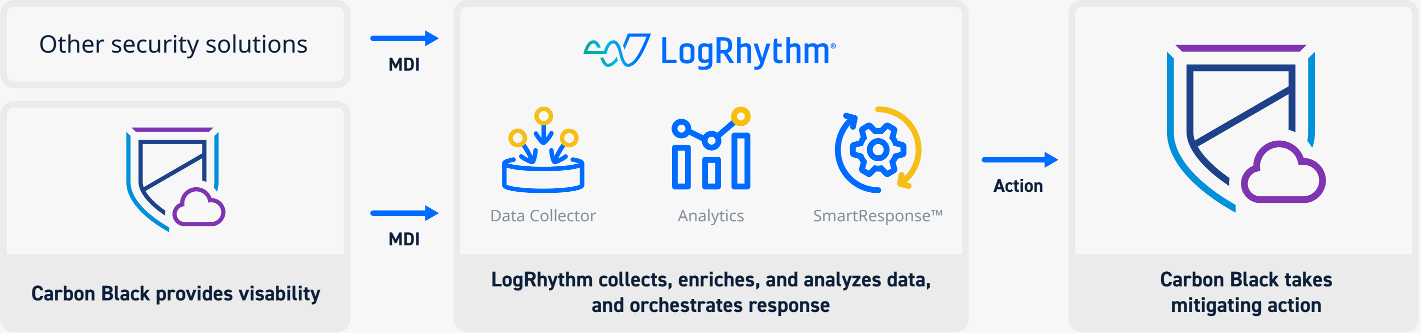
Solution Overview

LogRhythm SIEM integrates with VMware Carbon Black Enterprise EDR to enable security operations centers (SOCs) and incident response (IR) teams to use a single application to oversee threat hunting and incident response. VMware Carbon Black sensor continuously collects data, sending it to the Carbon Black Cloud while integrating with LogRhythm to collect and analyze file and folder data with other flow, event, and machine data, to immediately provide the most complete picture of an attack.

Analysts are alerted in the LogRhythm Web Console to alarms associated with the VMware Carbon Black Enterprise EDR agent. Console actions are then performed using LogRhythm's SmartResponse™ automated actions for VMware Carbon Black Enterprise EDR, thus reducing the investigation time from days to minutes. This provides teams the power to proactively hunt for threats, uncover suspicious behavior, disrupt active attacks, and address gaps in defenses before attackers can.

About LogRhythm and Carbon Black

LogRhythm and VMware work together to help organizations around the globe increase visibility and protect against modern cyberattacks. LogRhythm offers extensive support and integration across VMware's product portfolio. 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. LogRhythm and VMware empower security teams to navigate a changing threat landscape with confidence.


Other security solutions
MDI
MDI
LogRhythm
Data Collector
Analytics
SmartResponse™
Action
Carbon Black provides visability
LogRhythm collects, enriches, and analyzes data, and orchestrates response
Carbon Black takes mitigating action

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.

How Data Collection Works

The LogRhythm SIEM platform collects from every device, application, and sensor in an environment while our MDI Fabric classifies and contextually structures every log message. 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 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 SmartResponse automated actions, which are part of LogRhythm's security orchestration, automation, and response (SOAR) solution. A LogRhythm SmartResponse automated action accelerates response to malware threats to minimize damage, eliminating manual intervention by security analysts. This advanced capability is delivered to end users through the Carbon Black SmartResponse automated action. While LogRhythm has a dedicated engineering team that builds actions, this is by nature an open framework that enables Carbon Black customers to modify actions or write their own custom integrations.

The VMware Carbon Black Enterprise EDR SmartResponse contains multiple actions that 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 Actions for Carbon Black Enterprise EDR

Action	Description	Use Case
Create Carbon Black Enterprise EDR Configuration File	Execute this action and rerun it before using other available actions whenever the fixed-value parameters change	This functionality must run first before other SmartResponse functions can be executed
Create Policy	Create a policy in Carbon Black Enterprise EDR	Use this action to create a specific policy in response to an alarm trigger for suspicious activity
Delete File	Delete a specified file or directory on a target host	Delete unnecessary and/or potentially malicious files on a host
Device Status	Query the device status of a target host	Use this action to check the status of a device that has triggered an alarm for suspicious activity
Directory List	List directories or files in a specified directory path	Receive a full list of files within a directory
Dump Memory	Perform a full memory dump of a target host	Use this action to dump the memory to a specified output target when an alarm triggers from a specific rule set
Get File	Copy a specified file to a designated output location	Copy the contents of a file from one machine to another for forensic imaging
Kill Process	Kill a specified process on a target host	Terminates unnecessary processes on a target host
Process List	List all processes on a specified host	List all actions on a host when an alarm triggers for suspicious activity on said host
Quarantine Device	Quarantine a specified device	Run this action to quarantine the device during an investigation

For more information, request a LogRhythm demo.
logrhythm.com/demo