Joint Solution Brief

VMware Carbon Black EDR

Speed Threat Detection and Remediation within Offline, Air-Gapped, and Disconnected Environments

Solution Overview

Carbon Black EDR is an incident response and threat hunting solution designed for security operations center (SOC) teams with offline, on-premises, or hybrid environments. Carbon Black EDR continuously records and stores comprehensive endpoint activity data, so that security professionals can hunt threats in real time and visualize the complete attack kill chain. It leverages the cloud-delivered aggregated threat intelligence, which is applied to the endpoint activity system of record for evidence and detection of identified threats and patterns of behavior.

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 in the LogRhythm Web Console to alarms associated with the VWware Carbon Black EDR agent. They can also perform console actions using the SmartResponse™ automation plugin for Carbon Black EDR, helping further simply day-to-day security operations.

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.

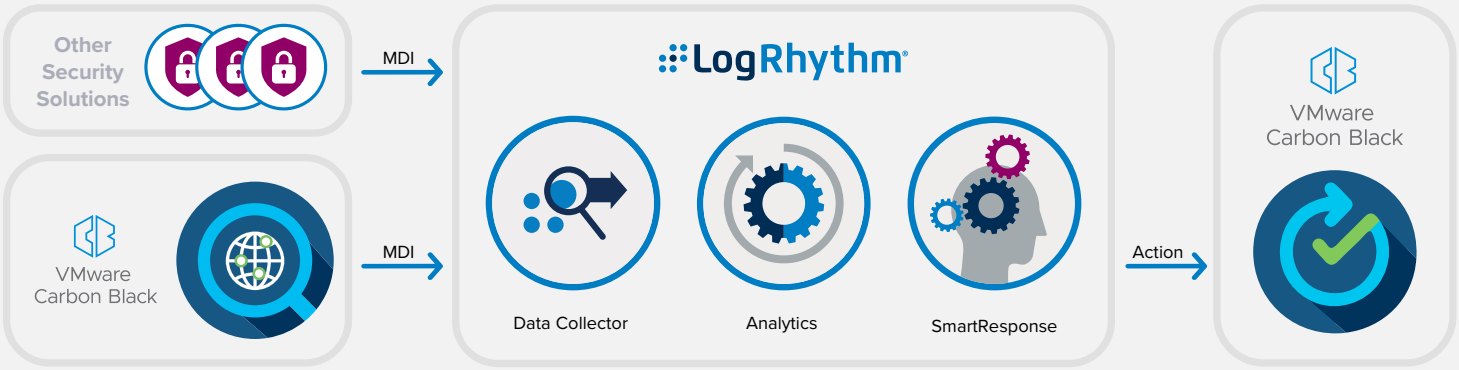
The LogRhythm Machine Data Intelligence (MDI) Fabric optimizes and stabilizes the optimal route of collection for over 1,000 log sources. Our security teams review these sources and ensure that relevant security data is normalized with other consumable security data. The results are trusted logs and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

Benefits

- Accelerate detection, containment, and removal of threats in standalone IT and OT environments
- Simplify security monitoring and alerting of multi-vendor environments via a centralized dashboard
- Standardize and automate response for rapid and error-free outcomes

About LogRhythm and Carbon Black

LogRhythm and Carbon Black are working together to help protect offline, on-premises or hybrid environments 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 threats, and to prioritize their responses based on accurate enterprise security intelligence.



How Data Collection Works

The LogRhythm NextGen SIEM Platform collects from every device, application, and sensor in an environment. 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 the host name to check the status of that host and guide further response. 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 Carbon Black 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 to protect their unique IT or OT environments.

The Carbon Black EDR plugin 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. Example actions and their use cases are provided in the table below.

SmartResponse Actions for VMware Carbon Black EDR

Action	Description	Use Case
Create CB Response V1 Configuration File	You must execute this action before using the plugin's other available actions and rerun it whenever the fixed-value parameters change.	This is required for all other SmartResponse functionality to work.
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.
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.
Dump Memory	This action performs a full memory dump of a target host.	After an Alarm triggers from a specific rule set, an analyst can trigger this SmartResponse plugin action to dump the 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.
Host Status	This action queries the status of a target host.	After an Alarm triggers that indicates suspicious activity on a host, an analyst uses the host name to check the status of that host and guide further response.
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.
Kill Process	This action lists all processes on a specified host.	After an Alarm triggers that indicates suspicious activity on a host, an analyst uses the host name to get a list of all actions on a host.

For more information, request a LogRhythm demo.

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

www.logrhythm.com