VMWare Carbon Black Cloud Enterprise EDR FedRAMP Integration Guide

VMware Carbon Black Cloud Enterprise Endpoint Detection & Response (formerly known as Carbon Black Threat Hunter) is a cloud-based threat hunting and incident response (IR) solution that delivers continuous visibility for top security operations centers (SOC) and IR teams. VMware Carbon Black Enterprise EDR is available for Endpoint Enterprise customers.
This integration supports API Ticket Creation.

This guide includes connection instructions for those who operate under the Federal Risk and Authorization Management Program (FedRAMP). See Carbon Black documentation on AWS GovCloud.

Deployment Type

This integration requires **vendor cloud** deployments through **port 443**.

If you already know that your environment supports **vendor cloud** deployments, continue to step 2. If you do not know about your organization's ability to support vendor cloud deployments, work with your internal team to ensure compatibility before continuing.

Required Information and Setup

To integrate GreyMatter with VMWare Carbon Black Cloud Enterprise EDR, collect the following details:

- URL
  - Default: https://<Hostname>.conferdeploy.net
- API Secret
- API ID
- Org Key

See instructions below to gather the required information.

Create an API Key

1. Within VMWare, open the **Settings**.
2. Click **API Access**.
3. Select **API Keys**.
4. Click **Add API Key** in the far right.
5. Give the API Key a unique name.
6. Select the appropriate access level provided in the permissions table below.
7. Choose a name to clearly distinguish the API from your org's other API Keys. (Example: Event_Forwarder_Test_Key).
8. Click **Save.**
9. Copy the API Key Credentials to somewhere secure for use in GreyMatter Connection Settings later.
   - API Secret Key (cannot be retrieved later)
   - API ID

If you do already have an API Key, view your credentials by clicking the dropdown arrow in the Actions column. Click API Credentials. If you have not restored the API Secret Key previously, reset it and copy it for later.

Configure API permission(s)

Navigate to **Settings > API Access > Access Levels > Add Access Level** and enable the API permissions below for each supported GreyMatter capability selected in Connector Specifications. For full details on how to create Custom Access Levels, see Carbon Black developer documentation.

Permissions and Functionality

Permissions

GreyMatter Capability	Action(s)	Required Permission
Investigate / Hunt	Get Fields Get Sources Perform Query	Create, Read, Delete
Asset Inventory	FETCH_ASSETS	Create, Read, Delete
Detect	Get Detection Records Update Detections	Create, Read, Update, Delete
	Perform GM Detect Query	Create, Read, Update, Delete
Intel Push	Intel Push	Create, Read, Update, Delete
Respond	Delete File	Create, Read, Update, Delete
	Ban Hash	Create, Read, Update, Delete
	Unban Hash	Create, Read, Update, Delete
	Isolate Host	Create, Read, Update, Delete
	Unisolate Host	Create, Read, Update, Delete
	Get Host Data	Create, Read, Update, Delete

Respond

Playbooks

Playbook Name	Description	Required Input Variables
Isolate Host	Specified host/IP is isolated from the network. Communications are limited to the technology console.	Hostname (Optional) Host ID (Optional)
Unisolate Host	Specified host/IP is no longer isolated from the network.	Hostname (Optional) Host ID (Optional)
Ban Hash	Adds the specified file SHA256 hash to a ban list to prevent execution on the network.	SHA256 File Hash
Unban Hash	Removes the specified file SHA256 hash to a ban list to allow execution on the network.	SHA256 File Hash
Delete File	Removes the specified malicious file from the specified active host.	File Path Hostname (Optional)

		Host ID (Optional
Enrich Host	Get endpoint metadata by submitting a hostname.	Hostname Host ID (Optional)

Investigate/Hunt

GreyMatter Investigate creates a search job and retrieves the events.

Asset Inventory

Asset Inventory provides a comprehensive overview of your digital environment by integrating directly with VMWare Carbon Black Cloud Enterprise EDR, providing real-time insights into what devices you own, their status, and potential risks.

Detect

VMWare Carbon Black Cloud Enterprise EDR supports **Detection at Source** (ReliaQuest and Vendor-Authored) and **Alert Ingestion.**

Intel Push

GreyMatter uses reputations API to push intel with VMWare Carbon Black Cloud Enterprise EDR. This enriches alerts that are pulled back from the direct source.

IOC Types: SHA256

By default, the IOC never expires.

Disclaimer: All customer data is classified and handled as 'Confidential' (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.