vmware Carbon Black

VMware Carbon Black Cloud Endpoint™ Standard

Integration - Technical Documentation

Cigent Technology Inc.
Website: www.cigent.com
Product: Dynamic Data Defense Engine (D3E)
Version: 2.0
Date: October, 2020

Contents

Overview

The Cigent Dynamic Data Defense Engine™ (D3E) is a new approach to data security, one that complements existing solutions and places the importance of protecting data above **all** else. D3E takes concepts used in threat containment and continuous authentication and applies them as close to the data stream as possible, bringing proactive protection directly to your data. D3E allows users to safely and easily access critically important information, even if the system is already compromised. The result is an unprecedented level of protection, detection, and response to cyberattacks, insider threats, and lost or stolen devices.

Cigent's management console is the centralized mechanism for monitoring, managing and controlling Cigent D3E deployments. Cigent's management console natively supports integration with Carbon Black Cloud Endpoint Standard management console providing increased value and security to users of both solutions.

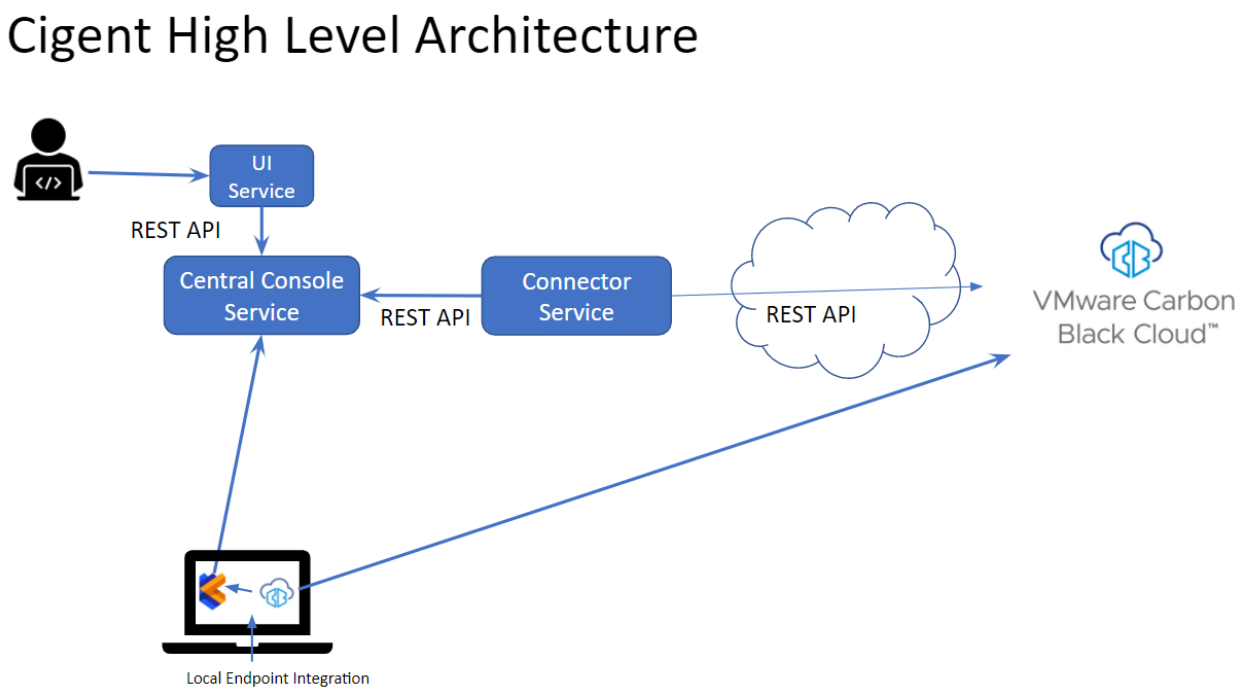
Key Benefits

Cigent D3E provides an additional response option for threats discovered by the VMware Carbon Black Cloud Endpoint Standard solution. This response ensures files designated as sensitive by the end user are protected by adding a second factor authentication requirement to access the files during the heightened security state. End users can continue to access their files while in heightened security state and even clear the threat should they or their SOC determine the threat has been remediated.

Cigent Product Integration Architecture

The Cigent Management Console Connector Service communicates directly with the Carbon Black cloud management console over the internet using REST APIs. No additional software or infrastructure is required by the customer to enable this integration.

Locally, Cigent D3E also monitors the VMWare Carbon Black endpoint via Microsoft Windows APIs and event log activity.



VMware Carbon Black Integration

There are two methods of integration both of which are controlled by the Cigent Central console.

Local integration enables monitoring of the state and threat detection status of the VMWare Carbon Black endpoint by the Cigent D3E endpoint residing on the same device. For example, when the Carbon Black endpoint detects a threat, Cigent D3E will immediately engage Activelock on the device even if the device is not connected to a network.

Console integration enables response to potential threat and policy enforcement activity in the Carbon Black Cloud management console by engaging Cigent D3E Activelock via the Cigent Central console. Alerts directed to the SIEM API key being monitored periodically by the Cigent Central console will cause D3E Activelock to be engaged for a single, group or all Cigent managed devices.

Integration Prerequisites

Both Cigent D3E and VMware Carbon Black Cloud Endpoint Standard agents need to be installed on devices on which users desire this additional layer of response.

Users must have administrative access to both Cigent and VMware Carbon Black's management consoles.

VMWare Carbon Black Cloud Integration Setup

Start by creating a SIEM API key specifically for use with the Cigent console integration. The API Access page is found under the Setting section of the Carbon Black console. See 'Manage API Access and Keys' in the Users Guide for help. Make note of the API ID for later use in configuring the Cigent console integration.

Next create notifications (Settings->Notifications) for Watchlist hits or Policy activity. Select the SIEM key created in the previous step in the 'How do you want to be notified?' section of the Add Notification window.

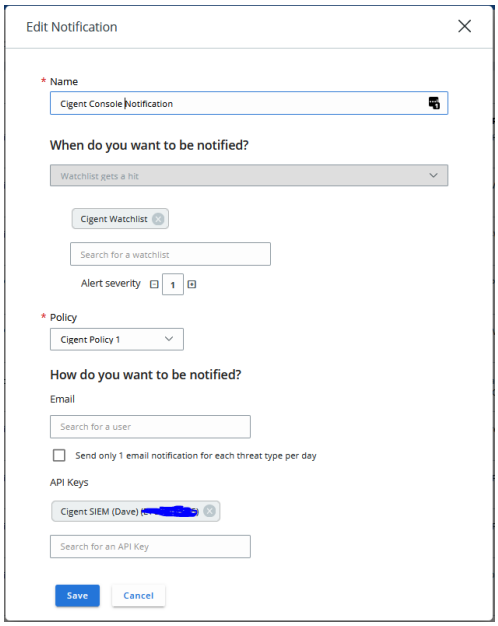


Figure 1- Example Cigent Console Notification

No special setup or configuration of the VMware Carbon Black Cloud Endpoint Standard agent is required to enable integration.

Cigent Console Integration Configuration

Navigate to https://central.cigent.com/integrations

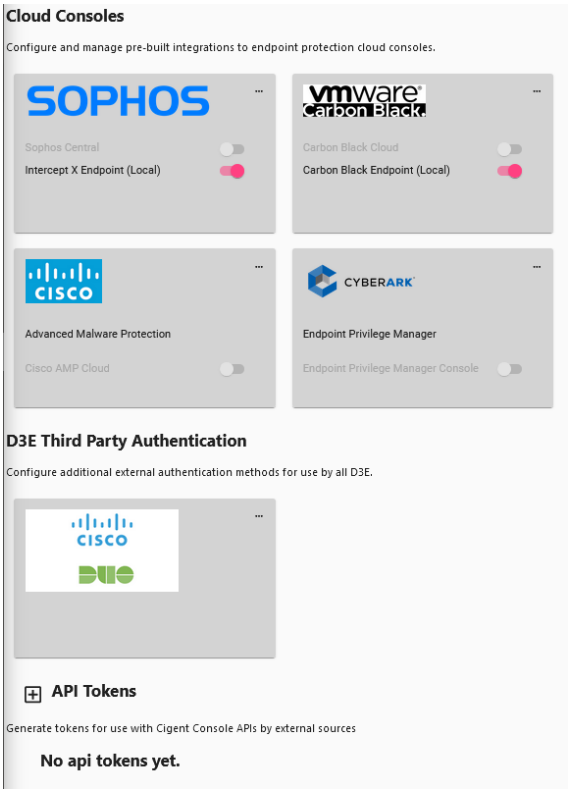


Figure 2Cigent Central Console Integrations page

By default, the 'Carbon Black Endpoint (local)' integration is enabled as indicated by the toggle switch. Administrators can disable the integration for all managed Cigent devices by toggling the switch.

To configure the Console integration, select ‘Set up’ from the menu available under the ellipse of the VMWare Carbon Black tile.

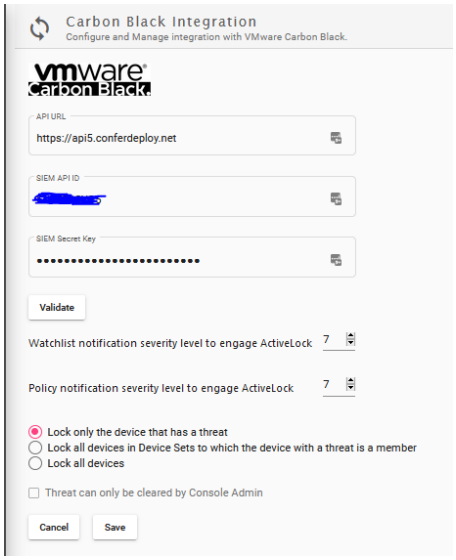


Figure 3 VMWare Carbon Black Integration configuration page

Enter the following information into the integration page:

API URL : Enter the API URL for your Carbon Black cloud console.

SIEM API ID : The SIEM API key created in the previous section.

SIEM Secret Key : The API Secret Key. This can be found by selecting the API Key row from the API Access page and selecting API Credentials from the dropdown menu at the far right of the row.

Next, click Validate to test that the Cigent Central console can successfully connect to the Carbon Black console using the provided API information.

Proceed by selecting the minimum severity level for both Watchlist hits and Policy activity notifications at which to engage Cigent D3E Activelock. These values will be used for all Watchlist hits and Policy notifications.

Finally, choose the scope of response to the notification.

- Lock only the device that has a threat
    - This will engage Activelock only on the device with the threat
- Lock all devices in Device Sets to which the device with a threat is a member

- If the device with a threat is a member of a Device Set (group) in the Cigent Console, all members of the group will engage Activelock. For example, if the device is a member of the HR Device Set, all members of the HR device set will engage Activelock.

- Lock all devices
  - All devices under management by the Cigent Console will engage Activelock.

Choose whether the threat can only be cleared by the Console Admininistrator (future.) Checking this option will hide the ability for the D3E user to clear the threat on the endpoint. This functionality will be enabled in an upcoming release.

Click save to return to the main Integrations page. The VMWare Carbon Black tile is now white indicating it has been configured.

To enable the integration, toggle the switch next to 'Carbon Black Cloud'.

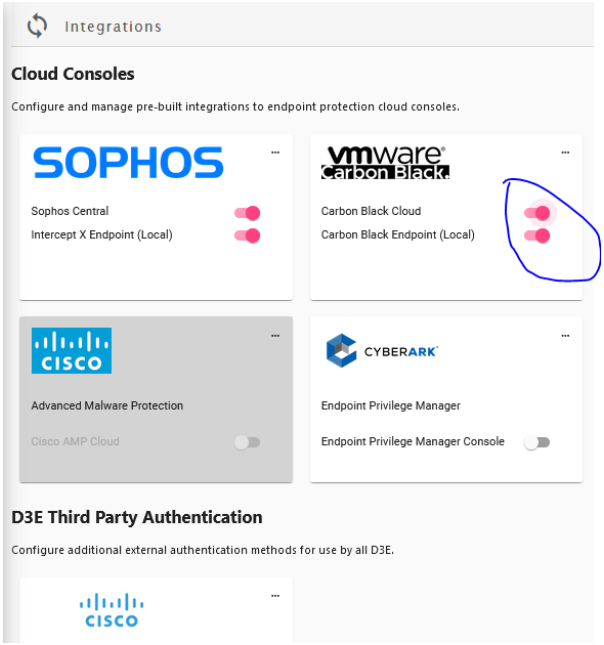


Figure 4 Local and Console Carbon Black integration enabled

Testing the Console Integration

You can test the console integration by generating a threat on an endpoint having both Carbon Black and Cigent D3E installed. Within a minute of generating the threat, D3E should display a message indicating ActiveLock has engaged from the console due to a Carbon Black threat.

You can also review the threats in the Threat History page even after the threats are cleared.

Cigent D3E Endpoint Installation

Refer to “Quick Start Guide for Cigent D3E” for Cigent D3E installation guidance available on the Cigent Support site. https://support.cigent.com/kb/faq.php?id=105

VMware Carbon Black Cloud Endpoint Standard agent installation

Refer to VMware Carbon Black Cloud Endpoint Standard agent installation documentation for guidance.

No special setup or configuration of the VMware Carbon Black Cloud Endpoint Standard agent is required to enable integration.