AppDefense Appendix
Cb Defense Integration Configuration Guide

Table of Contents

Overview

The integration of Cb Defense and AppDefense provides a comprehensive data center endpoint security solution. It allows security and IT operations teams with enhanced visibility into complex, multi-guest applications, their related network traffic, and suspicious endpoint behaviors. It also helps lock down intended state of data center endpoints, detect escalating application risk profiles, and prevent attacks in real-time. All the response could be triggered automatically with greater precision.

Cb Defense is a cloud-based next-generation anti-virus solution that prevents malware and non-malware attacks. Cb Defense provides visibility into events that take place on endpoints. Cb Defense consists of a lightweight sensor that is deployed to the endpoint and an analytics engine on the backend that provides advanced behavioral analytics, robust searching for incident response, configuration, and reporting.

Requirements

AppDefense and Cb Defense joint solution requires the following configuration:

- vCenter 6.5+
- ESX 6.5a and above
- Guest OS Windows 2008 R2, 2012, 2016 - 64 bit
- Cb Defense Sensor
- VMware Tools
- AppDefense Appliance version 1.1.0 or above
- NSX 6.3 & above (optional)
- vRA 7.2 (optional)
- Puppet Enterprise (optional)
- Recommended browser - IE, Chrome

Note: Please refer to Cb Defense user guide for Cb Defense Sensor software and hardware requirements.

Provision API Key for Cb Defense Integration

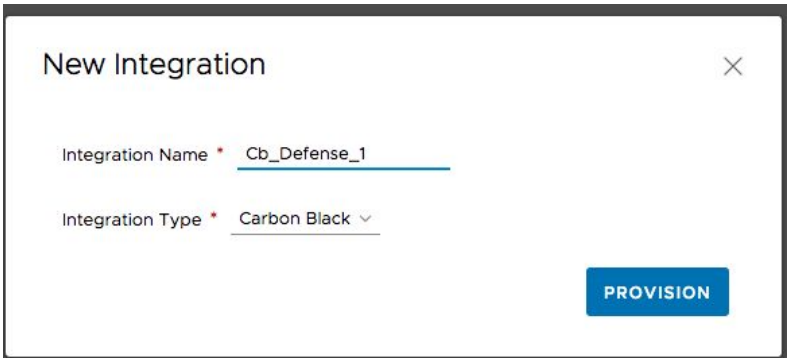
Users will need to provision API key for Cb Defense to enable the VMware Integration in the Cb Defense console. Please refer to “Enable the VMware Integration” section in Cb Defense user manual Appendix F for details.

To provision AppDefense API key for Carbon Black Integration:

- Login to AppDefense console
- Click on the settings cog at the bottom left of AppDefense console, and select Integrations.
- Click on the Provision New API Key at the upper right of the screen.
- Fill in the Integration Name.

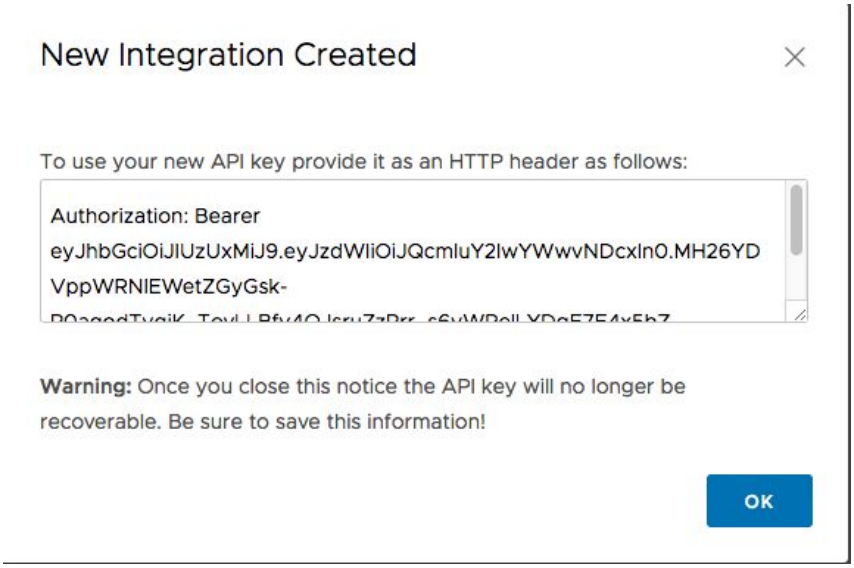
- Select “Carbon Black” in the Integration Type drop down list.

Figure 1 Integration Type



- Click on Provision. The API key will be generated and displayed in the popup windows.
- Take a note of the authorization key. The authorization key will need to be stored secretly and cannot be retrieved from AppDefense once the dialog is closed.

Figure 2 API Key Provisioning



- Copy this key. Please only copy the key without “Authorization: Bearer”. This key will be required to enable VMware AppDefense in the Cb Defense console. Please refer to Enable the VMware Integration section in Cb Defense user manual Appendix F for details.

Viewing Cb Defense Alert

After user enables VMware AppDefense on Cb Defense, new Cb Defense threat category Alerts should start to show up in the AppDefense console. Synchronization between two systems occurs every few minutes. User may experience some delay in Cb Defense alerts.

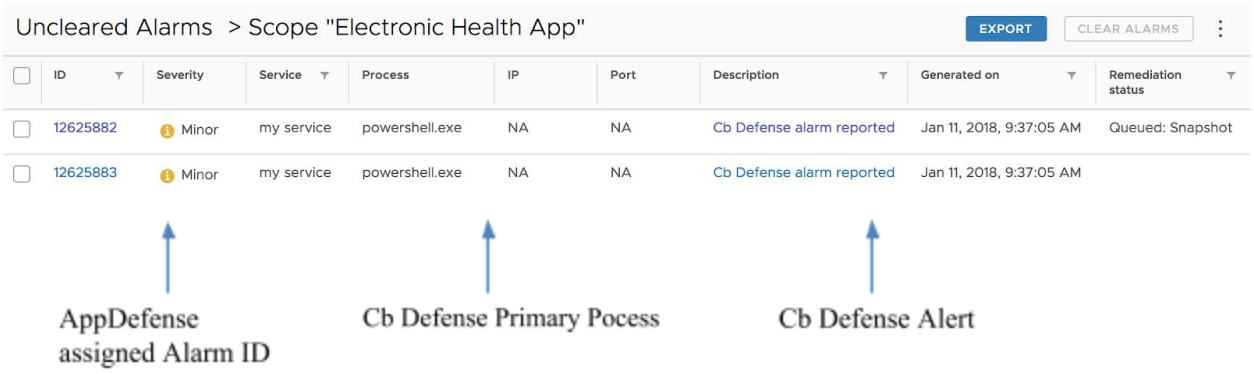
Please be aware that only threat category Cb Defense alerts will be integrated to AppDefense.The monitored category alerts will only be presented in the Cb Defense console.

Cb Defense alerts are managed and presented on AppDefense Console with the full application context. VMware AppDefense provides a compact view of a Cb Defense alert. The Cb Defense alert ID will provide a link to the Cb Defense alert Triage page for that alert.

To view Cb Defense alert in AppDefense alarm summary page:

- Log into the AppDefense Management Console.
- Click “Alarms” in the top-left corner will bring user to AppDefense alarm summary page.
- Cb Defense Threat Alert will be shown as “Cb Defense alarm reported” in the alarm summary page.
- User can filter “Description” column in the summary page to search for Cb Defense alerts.

Figure 3 Alarm Summary page



- The primary process of the Cb Defense alert will be shown in Process column.
- The alert severity show in the AppDefense console is based on Cb Defense alert priority score. Please refer to the following table for the mapping.

Table 1 AppDefense Alarm Severity Mapping

AppDefense Severity Level	Cb Defense Alert Priority Score
Minor	1-4
Severe	5-7
Critical	8-10

To view Cb Defense alert in alarm detail page:

- Click the alarm ID in the alarm summary page will bring user to the alarm detail page.
- Cb Defense alert Score, Threat Category, and primary process info (MD5 hash, Path, and CLI) will be shown in the upper left panel. Please see Table 2 for detail description.

Table 2 Cb Defense Alert Detail Description

Field	Description
Alert Score	The priority score prioritizes the relative importance of an Cb Defense alert. It maps to Cb Defense alert priority score.
Triggered By	Alert are triggered by Cb Defense
Threat Category	The category of the threat generated by Cb Defense. The value could be "Non-Malware", "Potential Malware", "Malware", or "PUPs"
MD5	Primary process MD5 hash value
Path	Primary process path
CLI	Primary process CLI

- AppDefense Scope context associate to the alert is shown in the upper-right panel.
- Cb Defense alert details are shown in the Detail Tab on the lower panel of the page. Please see Table 3 for detail description

Table 3 Cb Defense Alert Filed Description

Field	Description
Alert Details	
Reason	The reason for the alert.
Generated On	When the Cb Defense alert first received by AppDefense
Last Received	Last updated of the alert send by Cb Defense
Cb Defense Alert ID	Cb Defense assigned unique alert ID. The Alert ID will allow user to link back to Cb Defense Alert Triage page for that alert
OS	Device Operating System and version
Remediation Status	AppDefense Remediation Action taken for the alert
Parent Process details	
Process SHA256	Parent process SHA256 hash
CLI	Parent process CLI

- TTPs (Tactics, Techniques, and Procedures) is the threat indicators as categorized by Cb Defense. The TTPs associate to the alert are captured in the Threat Info Tab on the lower panel of alert detail page.

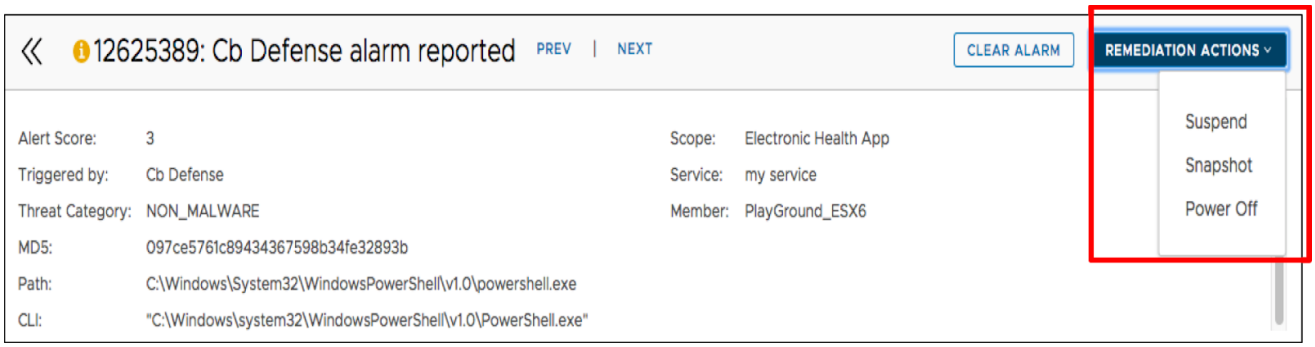
Taking Remediation on Cb Defense Alert

User can take AppDefense remediation actions against Cb Defense alerts. These remediation actions are different than Cb Defense remediations. By the time this document is published, AppDefense remediation actions will only be available in AppDefense. Cb Defense remediation action will not be available in the AppDefense console either.

To take remediation Action:

- Go to alarm detail page.
- Click the Remediation Actions drop down menu on the top right corner.

Figure 4 Remediation Actions



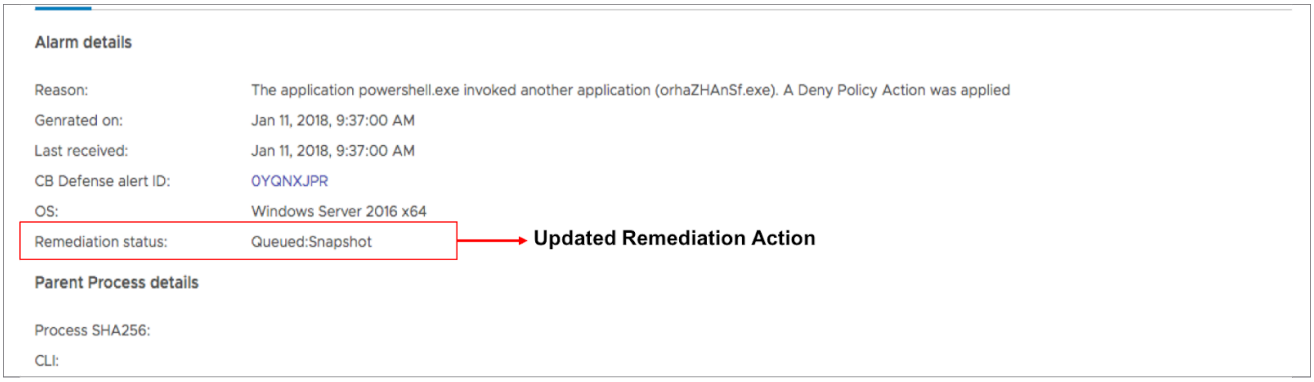
- Please refer to table 4 for remediation options.

Table 4 AppDefense Remediation Actions for Cb Defense Alerts

Field	Description
Suspend	Suspend the virtual machine that Cb Defense alert was triggered
Snapshot	Take snapshot of the virtual machine that Cb Defense alert was triggered
Power Off	Power off the virtual machine that Cb Defense alert was triggered
Quarantine	Quarantine the virtual machine that Cb Defense alert was triggered

- Please be aware that Quarantine remediation will only be available if NSX is deployed and configured.
- Select the desired remediation action. Confirmation window will pop up.
- Click the action button on the lower right corner to confirm.
- Once it is confirm the Remediation Status in the Alarm Details section will be updated accordingly.

Figure 5 Updated Remediation Status



Quarantine

Please be aware that AppDefense "Quarantine" remediation action will only be available if NSX is deployed and configured. The Quarantine remediation in the AppDefense manager console is different than Quarantine in Cb defense. User can quarantine virtual machine in both AppDefense (by using VMware NSX as an optional integration) and Cb Defense. Please refer to Cb Defense user guide for Cb Defense Quarantine capability details.

Once Quarantine remediation action is taken in the AppDefense console, the virtual machine connectivity will be blocked by NSX and the device will appear to be offline on Cb Defense console. Hence, users will not be able to take any actions on this device in Cb Defense until the device is removed from AppDefense Quarantine status.

AppDefense leverage the virtualization infrastructure, the system communicate with virtual machines through the hypervisor level. With this advantage, AppDefense can still communicate with the virtual machine and take actions on the device even if the same device has been quarantined in the Cb Defense console.

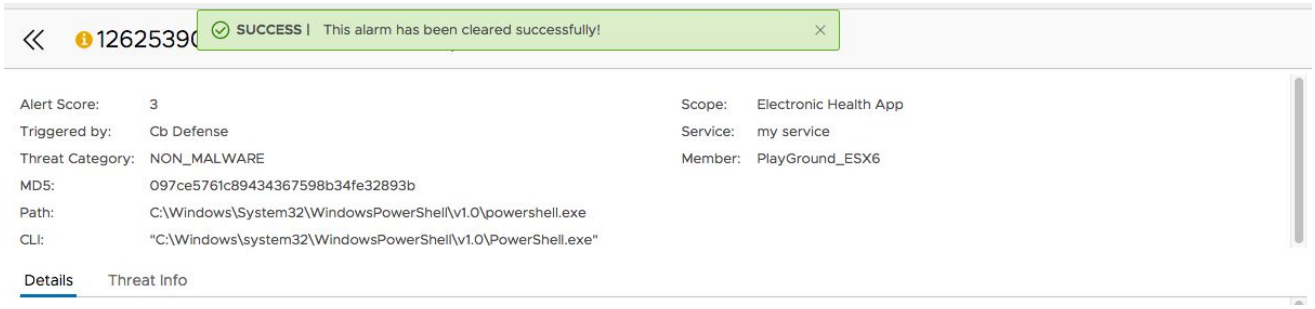
Clear Cb Defense Alert

User can clear Cb Defense alert in the AppDefense console. Please be aware that to clear Cb Defense alert in the AppDefense does not dismiss the alert in the Cb Defense Management Console. To dismiss Cb Defense alerts in the Cb Defense Console will not clear the Cb Defense alert in AppDefense either. Alert dismissal synchronization support will be available in the future phase of the integration project.

To clear Cb Defense alert:

- Go to the alarm detail page of the alert user would like to clear.
- Click the Clear Alarm button on the upper right corner in the alarm detail page.
- Once alarm is cleared a confirmation message will be show on top of the screen.
- The cleared alarm will be shown in the cleared Alarms section.

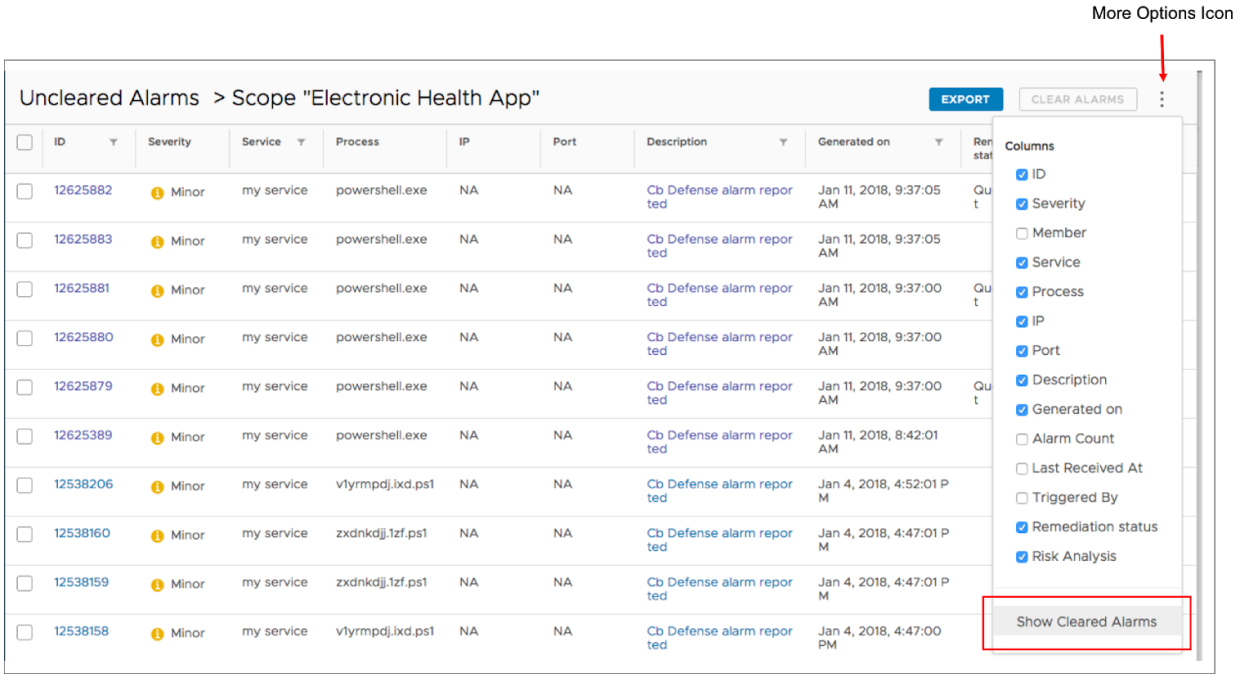
Figure 6 Clear Alarm Confirmation



To view cleared alarms:

- Click the more options icon on the alarm summary page.
- Select the "Show Cleared Alarms" at the end of the drop down list.

Figure 7 Cleared Alarms



- All the cleared alarms will be shown in the cleared alarm page including both cleared Cb Defense alerts and cleared AppDefense alarms.