

Carbon Black.



Cb Defense

April 2018 Update

Release Notes

April 2018

Carbon Black, Inc.

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

Email: support@carbonblack.com

Web: <http://www.carbonblack.com>

Copyright © 2011–2018 Carbon Black, Inc. All rights reserved. This product may be covered under one or more patents pending. Cb Defense is a registered trademark of Carbon Black, Inc. in the United States and other countries. Any other trademarks and product names used herein may be the trademarks of their respective owners.

General Notes

Starting the second week in April 2018, Cb Defense customers will receive an automatic upgrade to the Cb Defense Management Console. This document describes usability and performance improvements and bug fixes in the April release.

Features

New Malware Removal Page

A new **Malware Removal** page has been added to Cb Defense that allows you to view all known malware in your environment in one place. This page shows current malware in your environment and displays the devices that have this malware. Historical malware data that has been collected over the past six months is populated on the **Malware Removal** page. It can take several days for this data to populate for your organization.

On this page you can:

- Show the malware that has been **Detected** or **Deleted** based on the toggle switch at the top left of the page.
- Take action against malware (investigate, whitelist, blacklist, find in VirusTotal, and delete) by using the dropdown menu at the right of the malware.
- Navigate to the **Investigate** page via the **Investigate** icon at the right of the malware.

HASH	FILE	DEVICE	VECTOR	POLICY	FIRST SEEN	LAST DELETED	STATUS
12643...9d13	blackopsdropper.exe	PointofSalePC		Standard	9:15:43am Mar 13, 2018	--	Detected
a37dd...2a01a	svc.exe	ElectronicsPC		Standard	9:21:19am Mar 13, 2018	--	Detected
d1ac5...6d8e1	Transmission.dmg	demo4_mac_malware2	WEB	Standard	9:17:58am Mar 13, 2018	--	Detected
7096f...2a3d0	dum.exe	PointofSalePC		Standard	9:15:55am Mar 13, 2018	--	Detected
69a48...74263	cryptowall_69a480[1].exe	Marketing_PC01		Standard	9:15:22am Mar 13, 2018	--	Detected
69a48...74263	cryptowall_69a480[1].exe	Marketing_PC02		Standard	9:12:23am Mar 13, 2018	--	Detected
0b374...c9fbf	Mac.BackDoor.Worm_sample_2	SocialMediaMac		Standard	9:00:39am Mar 13, 2018	--	Detected
8a75f...879be	Locky-20170106.exe	trHostNamePC-2885		Standard	8:12:02am Mar 13, 2018	--	Detected
cff38...4567a	salty-20170106.exe	trHostNamePC-2885		Standard	8:12:07am Mar 13, 2018	--	Detected
f8f0b...b71f6	A0011424.exe	ShippingPC	UNKNOWN	Standard	8:16:04pm Mar 12, 2018	--	Detected
113be...11bf6	notepad2.exe	ShippingPC	UNKNOWN	Standard	7:05:30am Mar 13, 2018	--	Detected
89251...1ef16	caretowindropper.exe	ShippingPC		Standard	10:29:33pm Mar 12, 2018	--	Detected

Note: Only the first five and last five digits of the hash are displayed, but you can copy the entire hash to the clipboard.

Usability Improvements

TTP Color Consistency Update

Previously, the TTP color coding seen on the **Alerts** page was different from the color coding on the **Alerts Triage** page. Those differences have been reconciled, making it easier to scan an alert and recognize its associated TTPs.

Google Analytics

Added as a tool to help report traffic so that the product team can decide which features to invest in to help customers solve their problems. No PII will be collected.

Better Support for Condensed Browser Windows

Improved the page layouts in **Settings** to better adapt to narrow browser windows. The top navigation and **Settings** content should all adapt more gracefully as the browser window narrows.

Browsers Supported

- On Windows - Firefox, Chrome, and Edge
- On Mac - Safari, Firefox, and Chrome

Note that IE11 is not a supported browser.

Issues Resolved in April

ID	Description
EA-11745	Resolved an issue that resulted in the errors assigning sensors to Sensor Group when specifying a match "any" criteria.
EA-11610	Resolved an issue where search filters on the left hand panel of the Investigate page were not properly populating.

Issues Resolved in March

ID	Description
EA-11102	Fixes the ability to send the correct request to move sensors to Bypass mode.
EA-11411	Fix for the Administrators page where the DUO Settings button did not display after DUO was enabled.
EA-11212	Fix for Live Response API where Get did not revive a session.
EA-11700 EA-11751 EA-11716	Fix for Live Response where Get command returns an error
EA-11401	Fixed the Edit button alignment in the Sensor Groups pane (specific to Firefox).
EA-11448	Fix for Sensor Management auto-assign where auto-assigning all sensors was changing to manual assignment.
EA-10203 EA-11098	Fixed the information that is displayed on the Inbox page.
EA-10847 EA-11038 EA-11280 EA-11514 EA-11655 EA-11720 EA-11842	Fixed an issue with users being unable to uninstall inactive devices on the Sensor Management page.

Known Issues and Caveats

The following section lists known issues in this version of the Cb Defense backend/UI.

ID	Description
EA-7903 EA-7882	Automatic update of sensors from the cloud is currently disabled due to network bandwidth concerns. Manual push from the cloud is supported for 100 sensors at a time.

Carbon Black.

DSER-2951	Using Live Response to get or put a file greater than 2MB might be slow or not occur.
EA-11700 EA-11716 EA-11751	Live Response Get returns an Access Denied message in some situations.
	The Allow Uploads for Scan setting on the Policies configuration page is currently disabled while we transition this service to the Carbon Black Collective Defense Cloud.
EA-11745	Grouped sensors might fail to group properly if you use subnet conditions.
DSER-7298	In some situations, grouped alerts that are dismissed continue to automatically dismiss new alerts that are associated with that threat grouping. This can occur even if the Dismiss all future alerts option is not selected.

Cb Defense for VMware

Cb Defense for VMware is an optional solution that enhances Cb Defense to better secure the software-defined datacenter (SDDC) by integrating with VMware AppDefense and providing SDDC-focused functionality. The functionality that this document describes is only applicable for Cb Defense for VMware customers. Standard Cb Defense customers are not impacted by these enhancements.

Features

AppDefense alert injection

AppDefense alerts can be directly injected into the Cb Defense Management Console. This capability expands Cb Defense security alerting beyond endpoint events, providing a more complete security view of the datacenter. The supported alerts are:

1. Inbound Connections
2. Outbound Connections
3. Guest OS Integrity
4. AppDefense Module Integrity
5. Process Monitoring

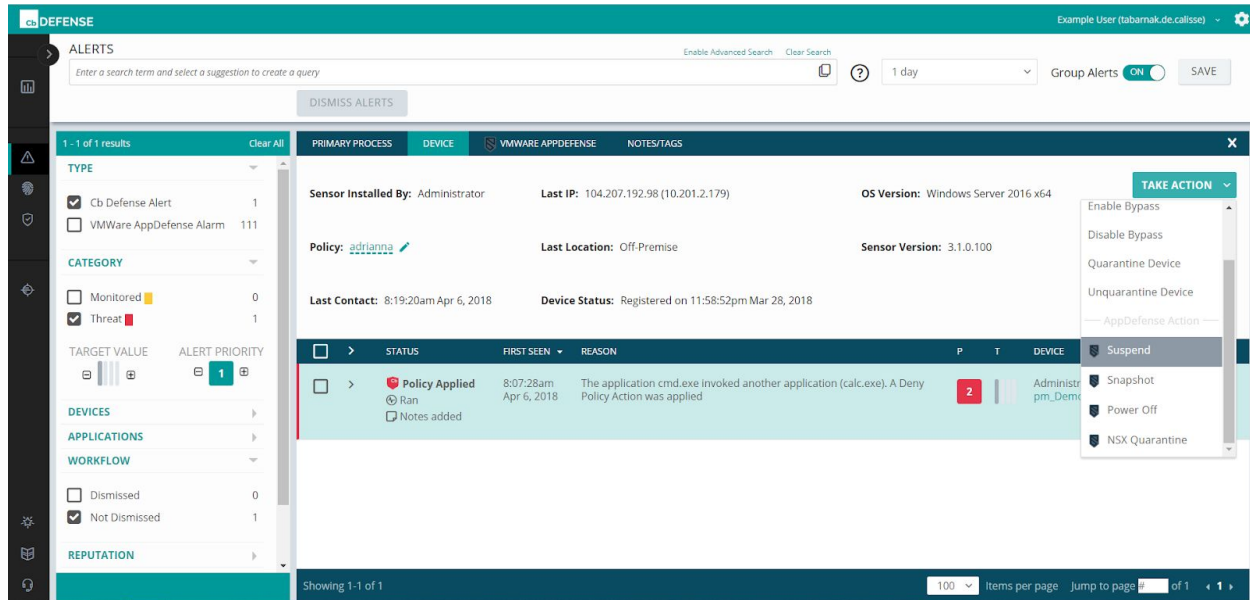
You can take actions on the virtual machines that are associated with alerts. Click the **Take Action** dropdown menu to view and select Cb Defense actions, including Live Response when it is enabled.

Cross-product remediations

You can use both Cb Defense and AppDefense remediation actions from either the Cb Defense Management Console or the VMware AppDefense Console. For alerts on virtual machines that have both Cb Defense and AppDefense installed, the **Take Action** dropdown menu from the **Device** tab on **Alerts List** and **Investigate** pages in Cb Defense offers AppDefense-specific remediation actions:

1. Suspend
2. Snapshot
3. Power Off
4. NSX Quarantine (when enabled)

Note: NSX Quarantine is only available if NSX is integrated with AppDefense.



In the AppDefense console, you can take the following Cb Defense actions:

- Add to Blacklist
- Cb Quarantine

Alert Action Status

Visibility into actions provides insight into what alert triage steps have been taken, regardless of if an action is taken in Cb Defense or AppDefense. In a multi-user scenario, this added context minimizes duplication of efforts and decreases manual information transfer between users. New fields include the following:

- Cb Defense
 - **Last action** added to the expanded section or **Reason** section of alerts.
- AppDefense
 - **Last Remediation Action** is added to AppDefense alerts and AppDefense Scope members.

Carbon Black.

The screenshot displays the Carbon Black Alerts interface. At the top, there's a search bar with the text "Enter a search term and select a suggestion to create a query" and buttons for "Enable Advanced Search" and "Clear Search". Below the search bar is a "DISMISS ALERTS" button. The main content area shows a table of alerts with columns for "STATUS", "FIRST SEEN", and "REASON". The first alert is "Policy Applied" with a status of "Ran" and a reason: "The application gc3sseob.5pg.ps1 invoked another application (foo_mar4.exe). A Deny Policy Action was applied". Below the table, there's a detailed view of the alert. It includes fields for "Last seen: 10:18:16pm Apr 4, 2018", "Alert ID: 3PELYK41", "Location at time of threat: OFFSITE", and "Threat Category: Non-Malware". A red arrow points to the "Last remediation action" field, which contains the text: "The last action was Cb Defense Quarantine taken in the Cb Defense console, it was successful." Below this, there's a list of actions taken, such as "fixed_port_listen", "unknown_app", "policy_deny", "run_unknown_app", "enumerates_processes", and "modify_process".

Last action is appended to all **Reason** locations in Cb Defense for alerts when both products are installed.