Carbon Black.

Cb Defense

October 2017 Update

Release Notes

October 2017

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

General Notes

Starting the first week of October 2017, 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 October release.

Search Improvements on Alerts List and Investigate

We've added suggestions to Search on Alerts List and Investigate, so you quickly search without having to recall exact syntax, and you can easily enter multiple search terms.

When you type in the Search textbox, Cb Defense suggests key-value pairs that match what you've typed. If you select a suggestion, it is added to the search bar and you can run the query, or type to add another key-value pair. When multiple key-value pairs are added to the query, there is an implicit AND between each key-value pair.

A few common examples of key-value pairs in this new search functionality include:

- TTPs
- Threat Category
- Reputation
- Device location
- Matches for partial IP addresses

Free-form and advanced search queries are still available: simply type your query and ignore the suggested matches. For more information, see the Cb Defense User Guide.

Improved Device Management

Delete Deregistered Devices

Deregistered devices can now be removed from Enrollment page to reduce clutter and make it easier to manage sensors and policies.

To manually delete deregistered devices, select the devices on the Enrollment page and click **Delete Deregistered Devices** on the **Take Actio**n dropdown menu. You can also automatically delete deregistered sensors after a period of time that you specify.

Auto-Deregister VDI Devices

You can set Cb Defense to automatically de-register virtual desktop sensors after they are inactive for a customizable period of time.

Usability Improvements

We've updated the console UX based on the following high-priority improvements:

- We've added support for the registry commands in Live Response.

- On the home page Dashboard, tool tips and some labels are improved to make the modules easier to understand.
- We've continued to make improvements on retaining information from page to page as you traverse the console.
- The ability to set the number of rows to display has been restored on the Alerts List and Investigate pages.
- Quarantine is available as an action on Alert Triage, Alerts List, and Enrollments pages. Therefore, under certain circumstances it has been removed from the Policy page. In this release, the Quarantine checkbox on the Policy page is hidden for any policy to which no devices are assigned.
- When whitelisting certificates from the Investigate page users now have the ability to add comments as to why they chose to take this action.

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 October

ID	Description
EA-9511	An issue with Private Logging is resolved.
EA-8143	Auto Upload and Manual Upload settings are decoupled.
EA-7939	Added the ability to add comments when whitelisting certs from the investigate page.
EA-10020	Resolved an issue that prevented some administrators from resetting their passwords.
EA-9646	Resolved an issue that led to inconsistent values for 'Signed by' and 'CA.'
EA-9541 EA-9914	Resolved an issue that caused hash URLs to be displayed incorrectly.
EA-9966	Resolved an issue that prevented Saved Searches from being deleted.

EA-9565	The "View Only" role can now change their own password in the Administrator page.
EA-9503	The ability to quarantine policies has been removed. To quarantine devices, use the **Quarantine devices** from the **Take Action** dropdown menu on the Alert Triage, Alerts List, and Enrollments pages.

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.
DSER-2951	Using Live Response to get or put a file greater than 2MB might be slow or not occur.
	The **Allow Uploads for Scan** setting on the policy configuration page is currently disabled while we transition this service to the Carbon Black Collective Defense Cloud.