Carbon Black.

Cb Defense

November 2017 Update

Release Notes

November 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 third week of November 2017, Cb Defense customers will receive an automatic upgrade to the Cb Defense Management Console. This document describes usability, performance improvements, and bug fixes in the November release.

Usability Improvements

We've updated the new UX based on the highest priority improvements you requested.

Home page

- We have added new filters on the Dashboard homepage that includes the ability to filter on Threat alerts, Monitored alerts and Priority Score of the alert.
- Both the panels themselves as well as the export of data from each panel take this filter into consideration

Search

- We have added key-name matching for the key-value pairs that create query chips. As you begin typing a key-name (such as reputation), a chip option will be automatically suggested.
- A new advanced search option at the top of the search bar allows you to toggle between advanced search and standard search. Advanced search lets you create complex queries that have multiple boolean operators (NOT, AND, OR) and parenthesis.
- A search status indicator (spinner) indicates that a query is running.
- You can now easily retrieve saved searches by searching for the saved search name and selecting the matching query chip.
- Granular reputation options (for example, *all.reputation, parent.reputation, target.reputation, primary.reputation*) are added to the Investigate page as key-value pairs. You can use these new options to create more precise searches.
- Granular hash options (*SHA256 hash, parent.SHA256, target.SHA256, primary.SHA256*) are added to the Investigate page as key-value pairs. You can use these new options to create more precise searches.
- The **Clear Search** option is added to all search bars.

Navigation

- The state of the Investigate and Alert pages are now retained When you execute a search, navigate away from the page and then return by using the navigation bar.
- With two-factor authentication enabled, the 2FA input box is automatically focused on page load, so you can login without needing to first select the input box.

Policies

- Path-based policy rules can now be edited. It is no longer necessary to delete and recreate an entire path-based policy rule to make changes.

Audit Log

- Timestamps provided in the Audit log CSV are no longer displayed in epoch time. They are automatically displayed in a human-readable format.

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 November

ID	Description
EA-10309	Resolved an issue that resulted in requiring a Certificate Authority when whitelisting by certificate.
EA-10479	Edited **Ransomware Policy Can Be Saved with Deny** operation.
EA-10150	Resolved an issue that prevented specifying a /32 CIDR block notation as an approved IP address for a Cb Defense connector.
EA-10075	Fixed suppression of an application hash when it has is a string of 0s.
EA-9991	Expiration date was exposed when using Company Installation Code
EA-9847 EA-10061	Analytics take auto-dismiss into account while updating a threat score.
EA-10258	Blocked or terminated events are not discarded by the behavior request filter.
EA-10064	Dismissing alerts always generated the with comment message even if there was no comment.
EA-10020	Failed login count was not being tracked as expected for failed admin logins.

EA-9254	Fixed the Investigate link to work properly in all instances.
EA-9042	Resolved an issue in the policy settings that resulted in the UI on Sensor was showing the word “false”.
EA-10149	Display Device ID on Enrollment page.
EA-9514	Display the API hostname to be displayed on the Connectors page.
EA-8934	When an existing policy Is renamed, the Enrollments Page Is now updated.
EA-9627	Investigate button on Alert defaults to Threat tab.

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.