Carbon Black.

Cb Defense

August 2017 Update

Release Notes

August 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 in the fourth week of August, existing Cb Defense customers will receive an automatic frontend/backend upgrade. This document describes usability and performance improvements and bug fixes in the August release.

Usability Improvements

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

Home page, Endpoints Health

- Issues with total and drilldowns is fixed.
- State of left navigation menu is now sticky (expanded or collapsed) across user sessions.
- Vertical empty space is reduced by 50%, which allows users to view more rows of data.

Search

- The search definition and selected filters are now displayed in the URL. When a search is defined, you can copy the page URL to send searches to others.
- Search definition is retained when the page is refreshed.
- Search definition is retained when using the browser's back and forward buttons.

Alert Triage

- Priority score is added to the top of the page.
- Target value is added to device information.
- Arrowheads are added to visualization.
- Difference between Read Memory and Access Target operations are clarified.
- Tooltips are added to Alert Behavior categories, TTP severity indicators, and device information.
- Alert Behavior categories better indicate that the spider graph can be manipulated by clicking on a label. Click on the center of spider graph to select all categories.
- "Hash Details" is renamed to "Process Details" in the Selected Process panel.

Alerts

- Ability to close alert detail top panel that opens when selecting an alert.
- The “Send to VirusTotal” option under the Take Action menu is renamed to “View in VirusTotal”. This option does not send, and has never sent, any data from Cb Defense to VirusTotal. Selecting “View in VirusTotal” opens a new browser tab that sends a hash query to VirusTotal’s website and displays the results.

Investigate

- When in an unambiguous alert context on the Investigate page, a button quickly takes you to the Alert Triage page.

Enrollment

- The manage sensors modal is updated to reflect the operating systems that are currently supported. Vista has been removed and Windows Server 2016 has been added.
- A company code is now automatically generated when a new organization is provisioned. This reduces the number of steps that administrators must take to deploy sensors..

Policies

- Navigating off of the policy page to another settings page with unsaved policy changes prompts users with a warning message about unsaved changes.
- The policy ID is now exposed in the URL for a selected policy. If the policy is renamed, the policy ID remains the same and can be located at the same URL.

Audit Log

- A new button enables users to export the log to CSV. Search and filter options are retained.
- End-user initiated bypasses are now indicated in the Audit Log. After a Cb Defense administrator enables the “Allow User to Disable Protection” policy setting and an end user toggles the local UI protection from ON to OFF, that action is recorded in as “Sensor Bypass Enabled (User Action)” in the audit log.

Performance Improvements

In the August release, improvements were made to the availability and reliability of the Cb Defense backend. Formerly, queued events were processed in batches with a new batch being processed every five minutes. The new process uses streaming technology with a very low latency that is measured in seconds. As a result, events and related alerts are visible within a much smaller time window.

Browsers Supported

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

IE11 is not a supported browser.

Issues Resolved in August (v 0.31.0)

ID	Description
EA-8955 EA-8883 EA-9096 EA-9331	Re-implemented rows per table in the new UI as it had appeared in the old UI. Number of rows per page is now configurable.
EA-9087	Resolved an issue where the audit log didn't properly display the admin who deleted a file.
EA-9131	Resolved issues that at times caused the full icon names or text details on the Alert Triage page to be cut off.
EA-8965	Audit log v3 API now produces the same results on every call.
EA-9361	Resolved an issue that prevented administrators from downloading the correct file from the inbox.
EA-9333 EA-9488	Resolved an issue that led users to delete a blocking and isolation rule other than the rule they intended to delete.
EA-9066	Resolved issues that caused the primary process tab to continue to display the last manually clicked event line.
EA-9042 EA-9304	Resolved an issue that caused the local UI to display "False" when the "Sensor UI Message" field on the policies page was not configured.

EA-9038 EA-9149 EA-9045	External IP is displayed as hostname in an event on the Investigate page.
EA-9386	Original event information is now displayed on Alert Triage & Investigate pages.
EA-9607	Audit Log messages now correctly indicate when devices are set to bypass.
EA-9465	Resolved an issue that allowed users to delete default policies.
EA-8143	The manual upload functionality is no longer coupled to the policy setting that controls the automatic upload.

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	File uploads/downloads that are greater than 1MB may be slow or not occur.
EA-9503	If an admin puts a device in quarantine through the Take Actions menu (alerts, investigate, or enrollment pages) or via the quarantine button on the Alerts Triage page, and then updates the policy that the device is in, the device will become unquarantined/active. The current workaround is to quarantine devices by moving them into the policy that is named “quarantine.”
DSER-3450	Time filters are reset when using the navigation bar to move between Alerts and Investigate pages.