Carbon Black Defense
May 2017 Update

Release Notes

May 15, 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 last week of May, existing Cb Defense customers will receive an automatic frontend/backend upgrade with new features. This document describes the new features and bug fixes.

New Features

Updated Dashboard

The Dashboard now provides additional modules and capabilities in an updated design:

- New *Attacks Stopped* and *Attacks Detected, No Action Per Policy* modules replace *Threats by Reputation* and *Policy Actions* sections.
- *Endpoint Health* module replaces *Device Health*, and includes additional data points.
- *Attacks by Vector* module replaces *Infection by Source.*
- You can view a report by policy.
- You can set a custom reporting period.
- You can export underlying data to CSV
- Some infrequently used items have been removed

Easy Access to Preventions and Detections

Two new menu items, *Preventions* and *Detections*, provide quick access to the Alerts List page in a filtered view to show preventions or detections, respectively.

New Alert Triage Page

Cb Defense now provides a graphical representation of an alert, together with detailed threat and process data to make it easier to understand and act on threats. Up and down arrows make it easy to traverse the alerts list without navigating back and forth to the Alerts List page. The Alert Triage page includes the following:

- Graphical alert with pan and zoom.
- Lets you select a process in the graph to view detailed information on that process.
- TTPs for the alert are grouped and visualized by type.
- A spider graph in the bottom panel provides a quick view of the attack profile and allows the user to explore TTPs that are related to the threat by category. *(Category descriptions are provided in the user guide)*

Direct Access to User Guide

The User Guide can be accessed from directly from the Cb Defense navigation bar.

Please see the User Guide for additional details on the new features.

Updated color palette

Cb Defense uses an updated color palette on all pages, as well as updated iconography, to increase page readability.

New UI architecture for select pages

The following pages have been migrated to a new UI architecture:

- Home page
- Alerts
- Investigate
- Log in Page

The new UI architecture improves application load time, maintainability, and security.

New API

An API has been added to move a device to a policy. Customers can now programmatically add devices to policies. This is impactful for customers that are heavily utilizing VDI.

Updated Audit Logs API to be RESTful are exposed via v3 APIs. This provides an improved experience when pulling logs from Cb Defense for third-party integrations.

Browsers Supported

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

IE11 is not a supported browser.

Issues Resolved in May (v 0.22.0)

ID	Description
EA-8346	Broken links; removed links to outdated sensor install and proxy guides.
EA-7975	Installing Flash player triggers level 7 threat.

EA-7938	Cert "Add" button in Investigate page is hidden after adding.
EA-8236	Blacklist confirmation dialog and additional logging of hashes.
EA-8033	Links in Cb Defense alerts are now properly URL encoded.
CIT-10709	Dismiss all for Alerts related to the PORTSCAN TTP now apply to the IP address as opposed to the pair of IP Address and application hash
EA-8840	Fixed enrollment errors.
CIT-10900	Management reports are now available through the home page CSV export.
EA-8743	Added “App Reputation (policy)” to blocking events details.
EA-7858	Fixed intermittent failures of sensor download updates from the backend.
EA-8077	Fixed enrollment errors where there is no pending user, but a user cannot be sent another invitation.
EA-8526	Fixed: moving large number of devices to a new policy had a limitation for 100 devices for one time.
EA-7843	Fixed: blocking events details did not have App Reputation (policy).
EA-8154	Blacklist option reflects the state of the hash.
CIT-10485	Alert dismissal is now logged in the audit log.

Known Issues and Caveats

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

ID	Description
EA-8143	Currently, the manual upload functionality is coupled to the policy setting that controls the automatic upload.