Carbon Black.

Cb Defense

January 2018 Update

Release Notes

January 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

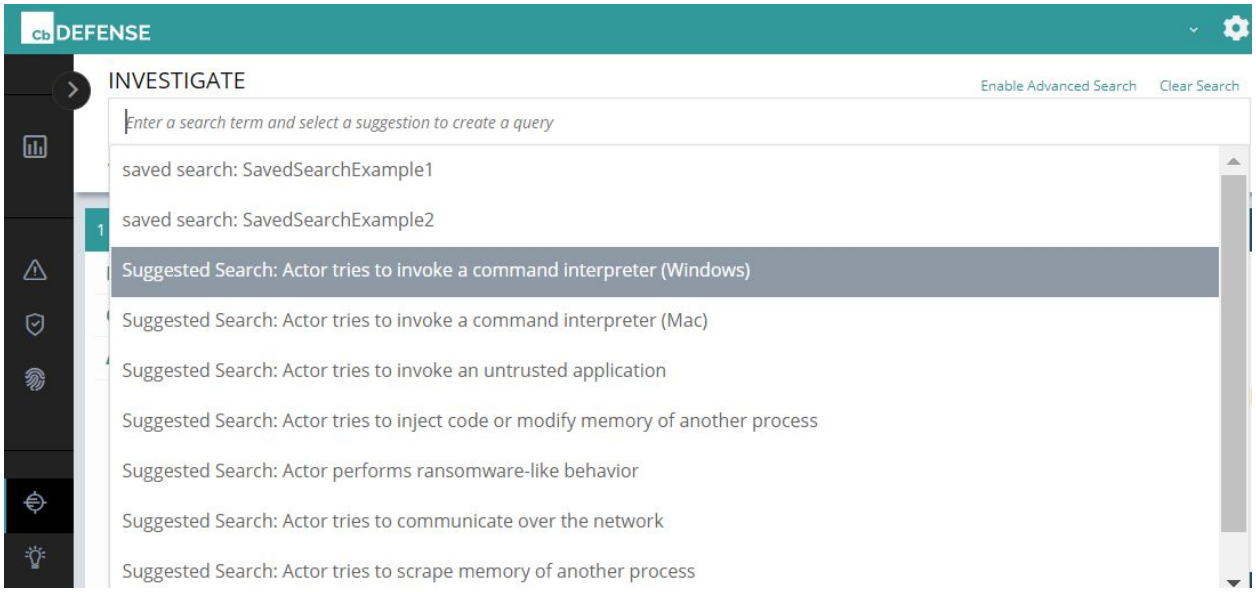
General Notes

Starting the second week in January 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 October release.

Features

Predictive Policy Searches

On the Investigate page, eight unique Suggested Searches have been added to help you predict how new policy rules would be applied to endpoints in your environment. As you click into the investigate search box, the suggested searches appear. Select one of the searches, which are each named after policy rule operations. The searches are made up of a combination of Threat Indicators and TTPs. Add a reputation to the search definition to determine what to enter in the application field of a new policy rule. Utilizing the reputation (application field) in tandem with the suggested search (operation field) helps you more easily map events in your environment so that you can created advanced policy rules.



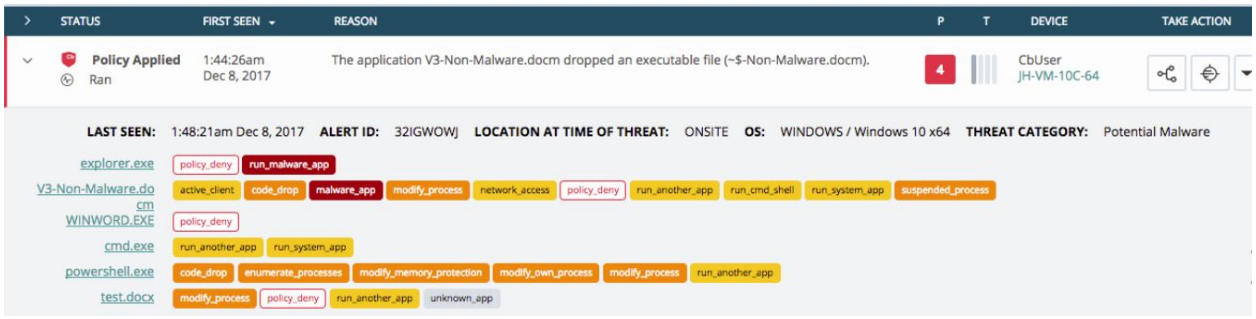
Usability Improvements

Cross Application

In this release, we have improved our users' experience with tables in the product by providing a consistent look and feel to all tables that are display in various pages. In addition to consistency, we have added the capability to store user preferences with respect to the number of rows shown per table. After a user makes a row count selection on a page the selection will be stored on a per user, per page basis.

Alert List

Added TTP severity colors to TTP tags associated with each alert.



Live Response

In the Live Response console, we have added the ability to cut and paste, tab complete the names for files and directories, and a link to display all alerts related to the device rather than just those that have occured over the past 24 hours.

Policy Page

We have added accordion behavior to the Permissions, Blocking and Isolation, and Uploads sections on the Policy Settings page to make it easier for you to narrow your focus to the specific rule set that you are interested in.

Carbon Black.

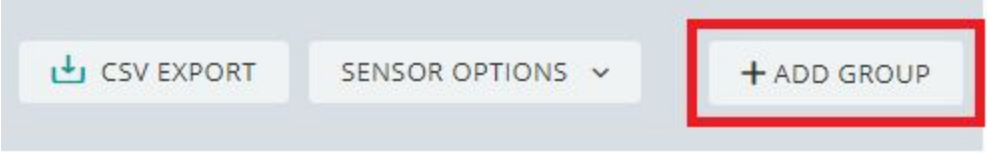
In coordination with the release of the Windows 3.1 sensor the following features will be enabled for all customers.

Sensor Management

The Enrollments page has been renamed to Sensor Management to more accurately reflect the capabilities that this page provides our users. In addition to renaming the page, we added the capability to group Cb Defense sensors using specific metadata about the device on which it is installed.

It is important to note that users are not required to create sensor groups and can continue to use the current methods of managing sensors and policies with no change in expected behavior.

To begin grouping sensors, add your first group by clicking the **Add Group** button now available on this page.



Users can create sensor groups and add sensors to these groups using the following criteria:

For Cb Defense sensors prior to version 3.1:

- Operating system (Any, Windows, macOS)
- Device host name
- Subnet (The subnet filtering is applied to the internal IP address of the sensor.)

For Cb Defense sensor version 3.1 (in addition to all of the above):

- Active Directory organizational unit (Windows only)
- Active Directory domain (Windows only)
- Active Directory distinguished name (Windows only)

All the sensors in the sensor group receive an automatic assignment to a policy group based on the metadata that is associated with the sensor, and the criteria that you define. This can save you time in managing large numbers of sensors.

For full details on configuring sensor groups please refer to the Cb Defense User Guide.

Controlled Uninstall

For Windows 3.1+ sensors, you can protect the action of uninstalling the sensor at the endpoint by requiring a unique, randomly generated code. Admins can use this feature to enhance their security posture and increase tamper protection from end users.

The controlled uninstall setting can be enabled per policy group by selecting the “Require Code to Uninstall Sensor” checkbox. After the setting is enabled, there are two uninstall code options--a device-level Uninstall Code, which is used to uninstall individual devices via the command line:

and an org-level Company Deregistration Code, which can be used to uninstall the sensor on multiple devices simultaneously using .bat files or SCCM.

Sensors that have been uninstalled will be tracked in the audit log.

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 January

ID	Description
DSER-4691	Deleted devices should no longer show up in the UI.
EA-10361	Resolved an issue that prevented **Unsupported OS** from appearing as a Sensor Bypass reason.
EA-10913, EA-10797	Resolved an issue that caused irrelevant events to appear alongside alert events when selecting an alert on the Alerts page and drilling into

	the details of that alert on the investigate page.
EA-10818	Resolved an issue that prevented the **Clear All** button from properly functioning when selecting an alert on the Alerts page and drilling into the details of that alert on the investigate page.
EA-10440	Resolved an issue that caused the cursor to jump up the Investigate page when expanding a row to view the full event details.
EA-9376	Reintroduced the ability to delete pending devices from the Enrollment page.
EA-10490	URL Verification tools in email clients no longer result in user inadvertent user registration.
EA-10440	Resolved an issue resulting in inadvertent scrolling behavior when expanding a row on the Investigate page.
EA-9509	Resolved an issue where Adobe Installer would trigger a level 7 alert when attempting to modify the next instruction to execute.

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.