General notes

Starting the third week in May 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 May release.

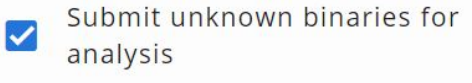
Features

Cloud Analysis

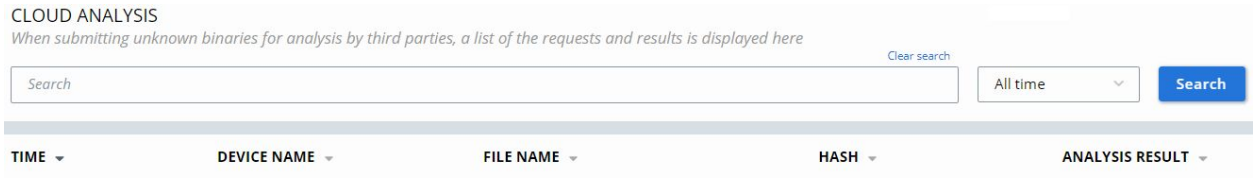
Upon updating to the 3.2 Windows Cb Defense sensor and enabling the local scanner feature on the **Policies** page, you can use this new feature, which provides additional cloud analysis of unknown binaries. The Cloud Analysis feature is disabled by default and can be enabled on a per-policy basis. To enable the cloud analysis feature, click the **Submit Unknown Binaries for analysis** checkbox on the **Policies** page, and click **OK** to confirm that you consent to share data with Carbon Black and our third-party partner detailed below.

DATA COLLECTION NOTICE: If you opt in to this functionality, the binary files (including the content of the files) are uploaded to Carbon Black for analysis. Carbon Black uses a third-party vendor, Avira Operations GmbH & Co. KG ("Avira"), as a sub-processor to assist with the threat analysis. The binary files are sent to Avira's network. Avira only processes the data to meet Carbon Black's obligations under the applicable agreement and for no other purpose. Avira has implemented appropriate security and operational methods that are designed to secure the data, and will comply with all applicable data privacy laws when processing the data. The information will be processed by Avira in their US or EU data centers.

In the course of using the services, you shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use and transfer to Carbon Black all such data. You can view Carbon Black's privacy policy at https://www.carbonblack.com/privacy-policy/ (which is modified by Carbon Black from time to time).



After you enable this feature, you can visit the **Cloud Analysis** page to view unknown binaries that have been sent for analysis, the device they came from, timestamps, and the results of the analysis.



Notifications service

A new in-product notifications service displays messages about new releases, maintenance windows, and expected downtime. A red circle indicates unread messages. Click on the Notifications header to view unread announcements. Click on the "X" next to an announcement to permanently delete it.

Feedback button

A new megaphone icon is added to the left navigation panel, which allows you to submit feedback directly to our product team. Click the icon to open a pop-up modal, which allows you to leave comments and categorize your feedback by these subjects: alerts/events, search/filter, sensors, policies, in-product help, other. By selecting the checkbox, you can also opt-in to becoming a design partner to help us with future product improvements.

Usability improvements

New Look

The Cb Defense platform has a new look in the coming release. You will find information and buttons in the same places, but the product color theme is updated to provide a modern new look that reflects the Carbon Black brand. Fonts have also changed for easier readability, and some icons have been redesigned. Table-row colors now support more states, making them easier to use. Many pages have a single button that's colored orange; this design improvement should help users identify the main function of a page.

These changes provide current customers with a better experience and convey to prospective customers that Cb Defense is a modern, cutting-edge NGAV solution.

Email notifications performance

Major performance improvements have been made to the email notifications service.

Detection alerts

Detection alerts are now visible in the process tree so even if a malicious process doesn't execute, you will see them in the process tree.

Malware removal

The **Vector** column has been removed from the table on the Malware Removal page based on feedback from our users.

Supported browsers

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

Note that IE11 is not a supported browser.

Issues resolved in May

ID	Description
DSER-6252	The **Allow Executable Uploads for Scan** setting on the policy configuration page has been removed. We transitioned this functionality to the new Cloud Analysis feature.
EA-12041 DSER-5500	Resolved an issue where items on the **Blacklist** and **Whitelist** could not be removed from either list.
DSER-7363	Fixed an issue where if certain information in the was missing about an item on the **Triage** page, the page would fail to render.
EA-11610	Resolved an issue on the investigation page, where the devices and applications panels were not displaying data when filtering on sensors by policy.
EA-11574	Resolved a performance issue where policies with thousands of endpoints were not accurately displaying the correct number of enrolled endpoints.
EA-11944	Resolved an issue where some policies were not loading correctly in the UI.

EA-11542	Resolved an issue where some policies that had previously been in quarantine (before the feature was deprecated in October 2017) were inadvertently brought out of quarantine.
EA-11924	Investigated high false positives that resulted when Cb Defense's repmgr.exe service was blacklisted; instituted a graceful way to display these alerts.
EA-11871	Investigated delayed email notifications and implemented major performance improvements (referenced in the release notes above).
EA-12198	Investigated delayed notifications received via the API and SIEM connectors, and implemented major performance improvements referenced in the release notes above.
EA-11459	Resolved an issue where sensor uninstall codes were not consistently displaying in the UI.
DSER-7488	The time window selection slider is now functional
EA-11102	Resolved an issue where some devices were not put in bypass with bulk bypass action
EA-11368	Updated the invitation emails for new sensors so as to no longer display old information
EA-10656	Fixed an issue where SAML SSO status was not correctly displayed in the UI
EA-12049	Resolved an issue with validating a SAML response with "NotBefore" timestamp in SubjectConfirmation

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.