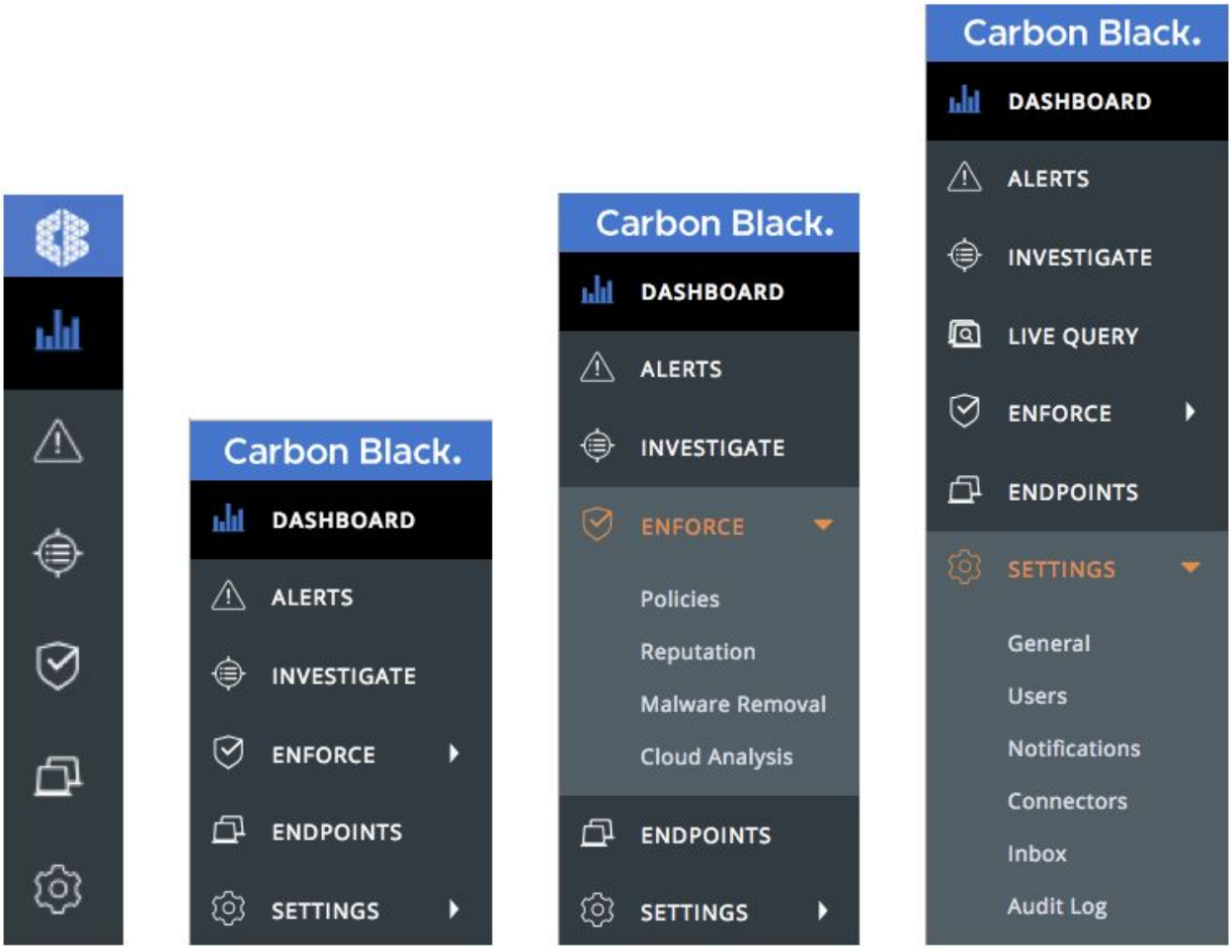
General notes

Starting the second week in July 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 July release.

Features

Improved navigation menus



The navigation menus on the left-hand side and the top-right corner are re-organized to make it easier to find the product features you're looking for.

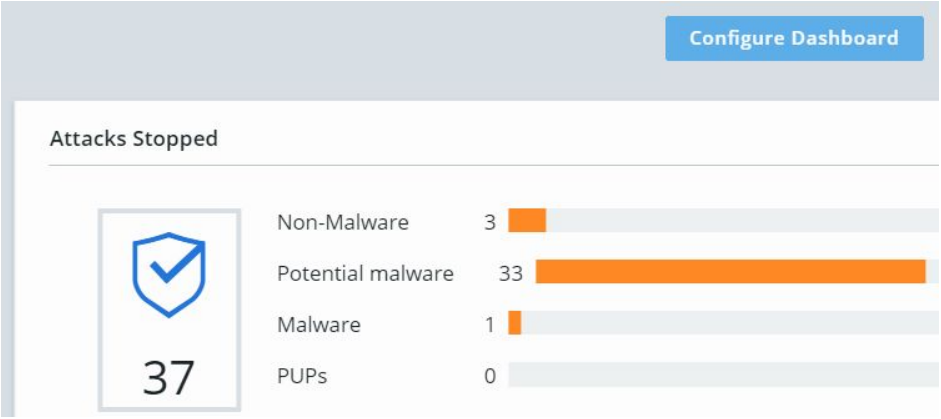
- Brings related capabilities together, such as the enforcement items under **Enforce**.
- Condenses menu options to reduce clutter, such as Alerts **Preventions** and **Detections**.
- Renames menu items to align with user expectations, such as **Sensor Management** > **Endpoints**.
- Moves **Help** content to top right nav where users expect it, and moves **Settings** to left nav where it's more visible.

Note: **VMware** and **ThreatSight** menu items are only visible to customers who have purchased those solutions and services.

Dashboard Improvements

The **Attacks Detected, No Action Taken Per Policy** widget has been renamed to **Potentially Suspicious Activity** due to feedback from many of our users.

We have added a dashboard configurability mode, which allows you to remove and add widgets so you can fully customize your dashboard and save those configurations. In the future, additional widgets will be added to the product.



Usability improvements

Table selection colors

The selection colors within the **Alerts**, **Investigate**, and **Endpoint** tables have been reversed to better emphasize what's currently showing in the detail pane above the table. Rows with checked checkboxes have a light blue background color. If a single row is selected to show more information in the detail pane, it has a dark blue background.

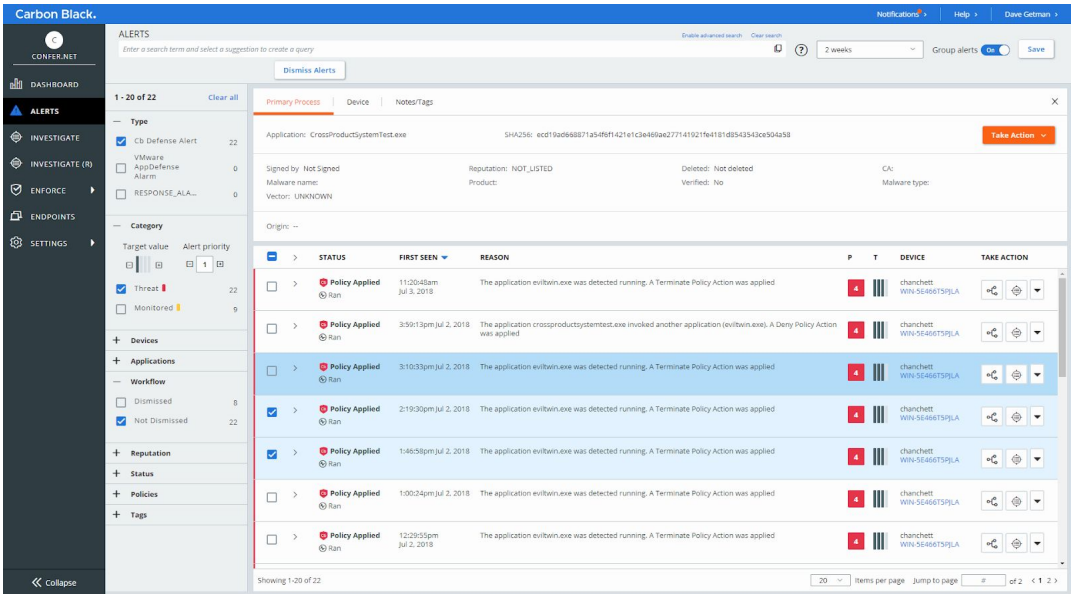


Table rows now collapse with new filters

Previously, in the **Alerts**, **Investigate**, and **Endpoints** tables, rows that were expanded to show more information stayed open when a new filter or search was applied. However, this sometimes resulted in a previously collapsed row filling an expanded row. To eliminate confusion, all rows will now collapse when any new criteria is added.

Issues resolved in July

ID	Description
DSER-6383	Fixed an issue where alert results past a certain number were no longer showing.
DSER-8456	Fixed an issue where Live Response “execfg” commands failed to return “stdout”.
DSER-8847	FIxed an issue where Mac 3.1 Sensor versions were not being properly assigned to sensor groups.
DSER-8418, DSER-8436, DSER-8608	Fixed an issue with checking whether a certificate is already whitelisted on the **Investigate** page, and fixed an issue where only some reputation and certificate overrides were being sent to the sensor.
DSER-8377	Removed an invalid device count from the delete modal.

Known issues and caveats

The following section lists known issues in this version of the Cb Defense backend/UI. The issue list is longer for this release in order to be more transparent about smaller issues.

ID	Description
DSER-8379	Bulk delete requests should not be sent to de-registered devices.
DSER-2951	Using Live Response to get or put a file that is larger than 2MB might be slow or not occur.
DSER-4585	Performing a CSV export on the Dashboard page does not follow the currently applied filter.
DSER-7977	Device count in the left navigation pane of the Inbox might show inaccurate counts.
DSER-7443	Sensor Grouping criteria "Device name" "Starts with" is not working.

DSER-8420	Reputation entries in the UI might be outdated after changing COMPANY_WHITE status.
DSER-7403	CSV exports that take longer than 1 minute fail to export any data.
DSER-6226, DSER-6228, DSER-6389	Uploading a bulk reputation file does not return an error if file processing fails.
DSER-6238	Events that have a policy applied but are not stopped don't show up on the **Dashboard**.
DSER-6038	Alerts Summary is not displayed properly when the threat actor is an IP.
DSER-4390	Some old versions of the Cb Defense sensor are not flagged as eligible for update.