PSC

CB Predictive Security Cloud

macOS 3.3.2
Release Notes

PSC sensor version 3.3.2.58 is a GA (General Availability) release for macOS only.

In these release notes:

Important

Devices that are upgrading from sensor versions **3.0** and older to **3.1**+ should have the new code signing certificate (***Team ID 7AGZNQ2S2T***) whitelisted prior to the sensor upgrade. This procedure is required because of a Team ID change in the CB Defense code signing certificate that was introduced in the 3.1 sensor release. See the Known issues section for more details. Carbon Black recommends using an MDM-compatible mass deploy solution to push the updates, pre-approve, and whitelist the KEXT code signing certificate.

Please see the following User Exchange article about granting the sensor Full Disk Access as required by macOS 10.14+: macOS 10.14+ Privacy Changes and Granting the macOS Sensor Access.

Release checksums

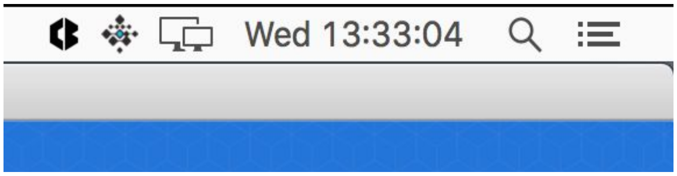
3.3.2.58 DMG SHA256 Checksum	ea3564331b4f6caa5c95d58500aee31ac99a602a418eab9441bcd928a79be1c8
3.3.2.58 PKG SHA256 Checksum	d6618a8a11de6b0b273b0bc17cb7379ead3b33b24895a09b69bcef9337ae8989

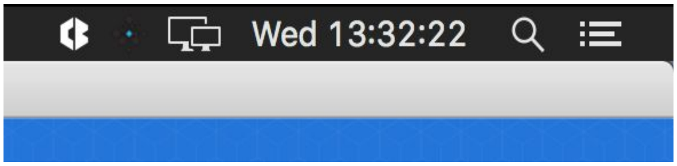
Copyright © 2011–2019 Carbon Black, Inc. All rights reserved. Carbon Black, CB Defense, and CB LiveOps are registered trademarks and/or trademarks of Carbon Black, Inc. in the United States and other countries. All other trademarks and product names may be the trademarks of their respective owners

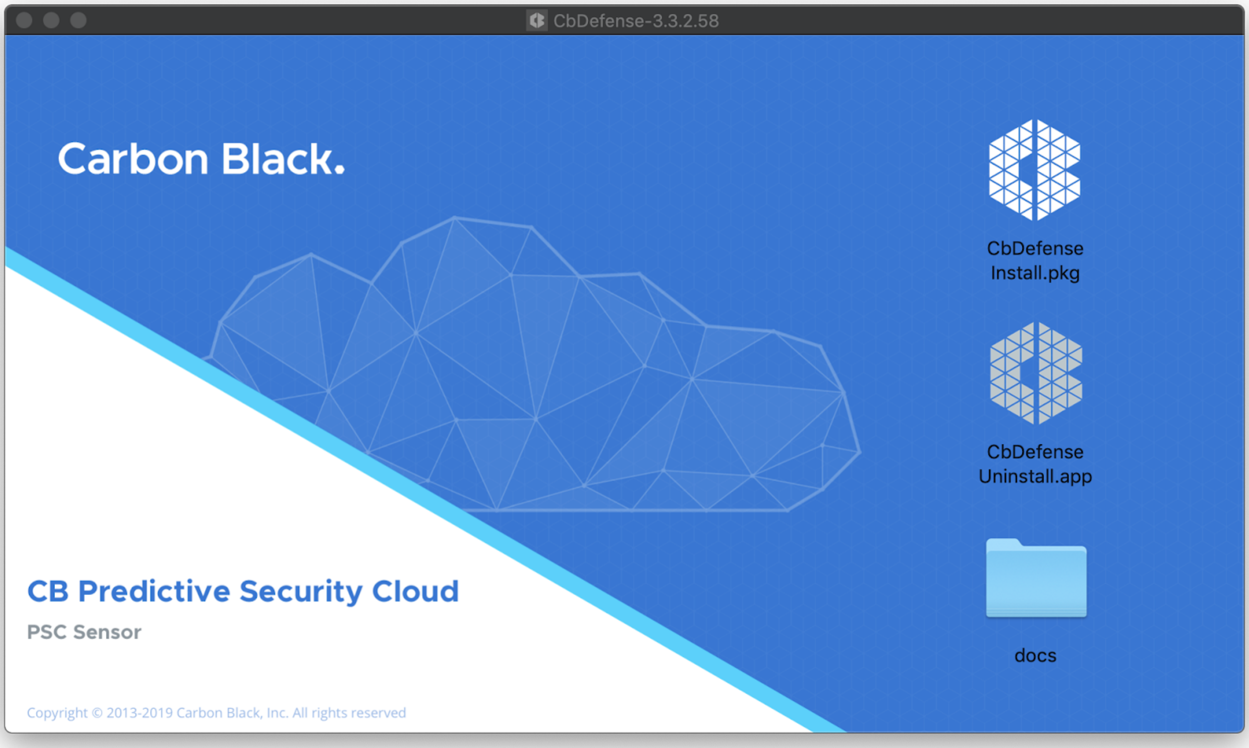
New features

Sensor UI Rebrand

As part of a company wide rebrand, the macOS sensor UI (including icons, favicons, the installer background, etc.) has been updated to match the PSC console and the rest of the company branding. Because this rebrand is focused solely on the UI, no changes were made to sensor directory structure or file names. This update has no impact on customer workflows, including installation processes. The sensor favicon in the menu bar supports both dark and light mode for Mojave 10.14. Logout and login is required for the favicon change to take effect when switching between dark and light mode.







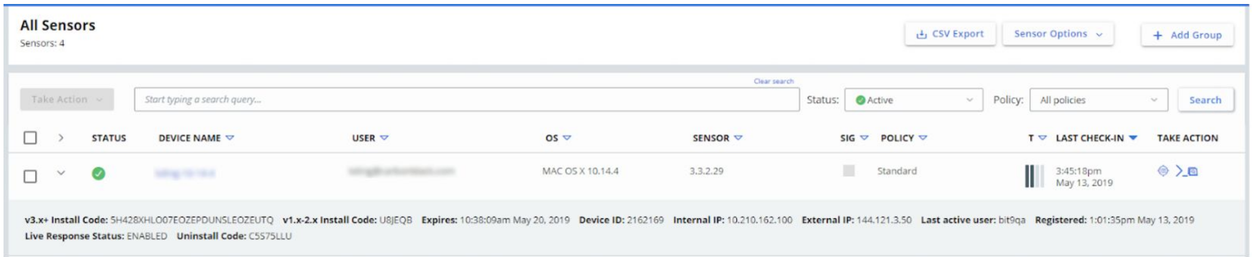
Mojave App Notarization

Starting with this release, every sensor build released will be notarized by Apple. By notarizing our builds, you can be confident that the Developer ID-signed builds that Carbon Black distributes have been checked by Apple for malicious components. “The Apple notary service is an automated system that scans [Carbon Black sensor builds] for malicious content, checks for code-signing issues… [and] tells Gatekeeper that Apple notarized the software. Gatekeeper then places descriptive information in the initial launch dialog to help the user make an informed choice about whether to launch the app.” For more information about App Notarization, please see the Apple documentation.

Last active user on Endpoint Management page

In version 3.3.2, the macOS sensor will now pass a different value for the **User** field throughout the UI. Previously (in 3.3.1 macOS sensors and below), the **User** field/column reflected the username of the account that installed the sensor on the machine on the **Endpoints**, **Investigate** and **Alerts** pages.

Across these pages, the **User** field/column will now show the **Last active user** on the endpoint in the respective location. For example, on the **Endpoints** page, the **User** column will now update with the **Last active user** on the endpoint.



All Sensors
Sensors: 4

Status: Active
Policy: All policies

□	›	STATUS	DEVICE NAME	USER	OS	SENSOR	SIG	POLICY	T	LAST CHECK-IN	TAKE ACTION
□	⌄	✓	[redacted]	[redacted]	MAC OS X 10.14.4	3.3.2.29	▨	Standard	▮▮	3:45:18pm May 13, 2019	

v3.x+ Install Code: 5H428XHLO07EOZEPDUNSLEOZEUTQ **v1.x-2.x Install Code:** U8JEQB **Expires:** 10:38:09am May 20, 2019 **Device ID:** 2162169 **Internal IP:** 10.210.162.100 **External IP:** 144.121.3.50 **Last active user:** bit9qa **Registered:** 1:01:35pm May 13, 2019
Live Response Status: ENABLED **Uninstall Code:** C5S75LLU

The **Last active user** is either an interactive/VNC user or an ssh user. The following scenarios apply:

- If an interactive user is signed in to a given endpoint, their username is reported.
- If no interactive user is currently signed in, the most recent signed-in username is reported.
- If no interactive user is currently logged on AND an ssh user is signed in, then the ssh username is reported

Obfuscation of command line inputs

Endpoint users may input sensitive data into the command line. The obfuscation of command line inputs protects against unwanted users accessing the data in plain text in the sensor .log files and the sensor databases. You can obfuscate command line inputs by using the following argument in the unattended install script: **--enable-hide-command-lines=1** during a fresh installation of the sensor (the switch is currently not supported during sensor upgrade).

The setting enables the obfuscation of command line input in sensor .log files and databases. The data in the cloud console is not obfuscated.

Fixed in this release

Efficacy enhancements and bug fixes

Issue ID	**Description**
EA-14074, DSEN-5260, DSEN-5342	Upgraded ransomware engine incorporates new detection techniques to improve efficacy of in-place encryption prevention and decrease false positives for services and GUI-like applications.
EA-14260, DSEN-5259	This change affects by path / glob matching rules under Policies->Prevention. Certain paths might need to be updated to make sure that they are correct. The following are detailed matching rules: * is used to match any character up to the next path separator ** is used to match all folder and subfolder contents ? is used to match single characters If a path such as `**/Applications/` is entered, it is treated as an alias to `**/Applications/**` and matches all subdirectories and files in Applications directory and subdirectories. The pattern `**/Applications` **is no longer** a valid way to specify the contents of the Applications directory, and will only match an extension-less file that is named *Applications*, and in any directory. **If you are using this notation in your environment, please adjust your rules**, in this example, to `**/Applications/` or its `**/Applications/**` alias. To match only the direct files of the Applications directory, the correct pattern is `**/Applications/*` `**/Applications*` matches filenames starting with *Applications* in any directory. `**/Applications*/` is treated the same as `**/Applications*/**` and matches all files and subdirectories in a directory name that begins with *Applications*.
EA-14262, DSEN-5244	This release improves detection, monitoring and reporting of incoming network connections opened by launchd super-server, such as SSH connections. `ATTEMPTED_SERVER` TTP is now applicable to such events.

EA-14323, DSEN-5353	This release provides a fix for a reporting issue when a file blocked on-access by a non-terminating process resulted in `POLICY_TERMINATE` TTP incorrectly set instead of only `POLICY_DENY` TTP. The bug, in some cases, contributed to incorrect alerts that implied that a legitimate process was terminated after accessing a blocked file.
DSEN-3132	This release resolves a lock contention issue which caused intermittent CPU spikes and other nuanced non-deterministic behavior that could affect blocking efficacy.
EA-14042, DSEN-5056	By improving the streaming detection heuristics, this release addresses a false positive issue that was associated with oversensitive buffer overflow alerts and `BUFFER_OVERFLOW_CALL` TTPs.
DSEN-4209	This release enhances VM guest detection and reporting by populating `virtualMachine(Bool)` and `virtualizationProvider(String)`. This endpoint-specific information is currently accessible through **Endpoint > CSV Export** in the Console.

Performance and stability

Issue ID	Description
DSEN-4901	This release includes resolves an issue where the sensor did not handle the case where the db_cfg database was already corrupted before the sensor started up.

Known issues

Description
Although Carbon Black officially dropped support for macOS versions 10.6 - 10.9 in the 3.1 release, 3.1 and 3.2 sensors would still install and operate on 10.8 - 10.9. In the 3.3.1 release, we dropped this unofficial capability altogether, and the 3.3+ sensor will no longer install on macOS versions 10.8 - 10.9. The last sensor version for 10.6-10.9 is 1.2.4 (EOL). The range of macOS versions covered is as follows: **3.x sensor: macOS 10.10 - 10.14.5 (official support)** **1.x sensor (EOL): 10.6 - 10.12**

The following behavior is expected when pushing a 3.3 sensor upgrade (cloud, attended, and unattended) to 1.x sensors that are running on an unsupported OS: - Devices running 10.6-10.9 will not upgrade.
There is an infrequent known issue where the Malware Removal UI inaccurately reports the actions that were or were not taken. This issue will be resolved in an upcoming backend release.

Issue ID	Description
DSEN-2735	Device name in sensor management is case sensitive.
DSEN-2700	Rare issue where repmgr service sporadically crashes on shutdown; this is more likely to occur when the network/cloud is unreachable in http proxy environments.
DSEN-2543	The unattended install script does not accept multiple long options. The workaround is to always provide a value (such as 0 or 1) next to every long option following = character; for example: `--downgrade=1 --skip-kext-approval-check=1.`
DSEN-3740	When a device is removed from an AD domain, the sensor is still reflected as being within that domain in the **Endpoints** page and remains in a sensor group. The sensor must be taken out of auto-assignment to make policy updates to that sensor. As a workaround, you can manually remove the sensor from the AD group and assign a policy (click into the device, turn off auto-assign, and change the policy).
DSEN-3752	Cloud uninstall of the sensor takes a long time due to a change in the backend.
DSEN-3669	Old canary files, specifically with variable or random files names, are not always properly cleaned up by the sensor. This can cause ransomware false positives.
DSEN-4373	Parent information is missing in the console (parent pid -1, empty parent hash) for processes that started before the sensor was installed or while the sensor is in bypass mode and still running.
DSEN-5055	Very rare issue where when "Sensor - Allow user to disable protection" policy is enabled, the protection On/Off switch does not work. As a workaround, reboot the OS.