Carbon Black.

Cb Defense Sensor 3.0 for Mac

Release Notes

November 13th, 2017

Carbon Black, Inc.

1100 Winter Street, Waltham, MA 02451 USA

Tel: 617.393.7400 Fax: 617.393.7499

Email: support@carbonblack.com

General Notes

These Cb Defense Sensor version 3.0 release notes are for the Mac operating system only.

New Features

This section lists features that are introduced in the 3.0 version of Cb Defense Sensor. For a more thorough description of the new features in this release, see the User's Guide.

Ransomware Prevention Improvements

The 3.0 Cb Defense sensor introduces a new event streaming engine that improves prevention efficacy against ransomware TTPs, especially around the new "0-day" attacks.

To take advantage of these enhancements, administrators can set policy rules in the Cb Defense Management Console to handle ransomware-like behavior. When a ransomware policy rule is applied on an endpoint, the sensor UI displays a message that "Potential Ransomware was terminated" and a high-level alert is triggered in the Dashboard.

New customers receive updated policies out of the box that enable ransomware improvements. Current customers can add the following three rules to their policies to get started with ransomware defenses in the same way.

The standard practice for macOS is to use three Blocking and Isolation Policy Rules: (1) for adware or PUPs, (2) for not listed reputations, and (3) for unknown reputations.

We encourage customers to add these policies because they provide defense against a wide range of ransomware and incur a low risk of false positives.

To read more about these improvements and how to enable these new policies, see the User's Guide.

Live Response

This release introduces Live Response to Cb Defense. Live Response offers authorized users remote access to enabled endpoints. This lets them inspect endpoints during investigations, eradicate threats, and return endpoints to normal operations after an incident. A new administrative role, "Live Response Admin", and a new policy option, "Enable Live Response," control access to this feature.

Live Response Admin supersedes the Admin role and this privilege can only be granted by another user who has Live Response Admin rights. For current customers, all users that have Admin privilege at the time of release will be promoted to the Live Response Admin role. We encourage customers to audit their users and demote any administrators that should not have Live Response access.

To help prevent abuse, Live Response includes a kill switch that lets administrators disable remote access to any endpoint. After enabling the kill switch on an endpoint, Live Response access is not possible to that endpoint, irrespective of policy settings or the user's role. To re-enable Live Response on the endpoint, the Cb Defense sensor must be reinstalled on the endpoint.

Administrators can monitor Live Response use through Cb Defense's audit log. Live Response-related messages include the token, "LiveResponse", which makes it easy to search for Live Response messages only. By default, the audit log displays connection attempts and error messages. Turn verbose logging ON to display each command that was issued during Live Response sessions.

To read more about this feature and how to enable/disable this new role, see the User's Guide.

Support for macOS 10.13 "High Sierra"

Please see "Known Issues and Caveats"

Enhanced Reputation Engine

A new reputation engine has an improved reputation processing that is reflected in better reputation accuracy, improved blocking efficacy, reduced false positives, shorter delays and improved reporting.

Reputation: Certificate Whitelisting

Binary files that are signed and locally verified on the endpoint against the Apple trust store can now be whitelisted by the publisher certificate subject and issuer name, either on the "*Reputation*" page or on the "*Selected Application*" Tab.

Certificate Whitelisting establishes an initial base trust for the signed and verified files that are new on the device by assigning *LOCAL_WHITE* reputation until more information is available from other reputation sources (such as the Cloud). If the trusted certificate becomes compromised, the sensor relies on 1) Apple certificate revocation mechanism, backed by 2) Cloud reputation override for a file signed with such a certificate.

The whitelisting feature is especially applicable when using policy configurations that have stricter prevention rules, such as with "*unknown*" and "*not listed*" target reputations. This feature is useful for common third-party/proprietary applications that upgrade frequently in a production environment.

Operating system files that are signed and verified by Apple, Inc. are certificate whitelisted by default.

Consider identifying common application publishers in your organization, especially for applications that upgrade frequently.

Please see "Known Issues and Caveats" for current limitations around PKG installers.

Reputation: IT Tools Whitelisting

New files that are introduced into a device and that are created by trusted tools acting as "code creators" can now be whitelisted on "*Reputation*" page in the "*IT Tools*" tab. After being configured, any new code files that are created by the trusted tool are initially treated as trusted. Reputation of the tool itself is checked by using standard reputation sources to verify that the tools are not malware.

Files created by the configured IT Tools are assigned initial base trust and assigned *LOCAL_WHITE* reputation, similar to the certificate whitelisting feature. As a result, the newly created files are not stalled on pre-execution and are scanned in the background, improving perceived performance (especially when frequent code drops are followed by immediate executions, as in case of code debugging). Files dropped by the trusted tools are not subject to strict prevention rules targeting "*unknown*" and "*not listed*" reputations.

Common use-cases on Mac are: software deployment tools (such as JAMF) and software development tools (such as code editors, IDEs). IT Tools helps to maintain low false positives while enabling stricter prevention rules.

When configuring IT Tools, the administrator can select recursive mode to extend the IT Tool to child processes that the tool invokes (that is, for cases when the actual drop is performed by one of the child processes; this is common with some software deployment and development tools).

Consider identifying common IT Tools that are specific to your organization (such as software deployment tools, code builders or code editors) and configure them for optimal performance and low false positives.

Enhanced Code Injection Prevention

Enhanced code injection prevention protects against additional code injection techniques on macOS by using the "code injection" rule; namely, code injection of malicious dynamic libraries (dylibs) that override symbols in the original libraries that the application linked against. Such code injections leverage OS loader/linker in the attack chain, and have no other process actor; thus Policy rule is applied against the reputation of the dylib file being injected into process. Special cases for legitimate applications utilizing this injection technique can be addressed with whitelisting (by hash or Cert) of the dylib.

Improved Sensor Installer

This release features a new sensor installer, upgrader and uninstaller with several improvements and enhanced sensor protections.

Elongated Company Registration Code

To improve deployments and scalability, this release increases the length of the company installation code. Users must update any software deployment tools or any existing installation scripts (such as those used to deploy sensors via tools like Casper/JAMF/Munki) that utilize the previous 8-digit codes.

Known Issues and Caveats

The following section lists known issues in this version of Cb Defense sensor.

Description
We are dropping official support for macOS versions 10.6 - 10.9. The last sensor version for 10.6-10.9 is 1.2.4 (eol, but available for download). The range of macOS versions covered is as follows: **3.X sensor: macOS 10.10 - 10.13 (official support)** **1.X sensor (eol): 10.6 - 10.12** **The following behavior is expected when pushing 3.0 sensor upgrade (cloud, attended, and unattended) to 1.X sensors that are running on an unsupported OS:** - **Devices running 10.6-10.7 will not upgrade. Devices running 10.8-10.9 will upgrade to 3.0 but will be running an unsupported sensor version for that OS.**

Related to the above caveat, the Enrollment Page UI currently has a few errors that reflect inaccurate supported macOS and OSX versions next to the associated sensor in the dropdown:

1) **The 3.0.x sensor: 10.10 - 10.13 currently shows 10.8-10.12 (10.8-10.9 do work, but are not officially supported by 3.0.x).**
2) **The 1.2 sensor: 10.6 - 10.12 currently shows 10.6-10.7**

Note, there is an overlap: 10.10 - 10.12 are supported by both 1.2 and 3.0.x.

These UI bugs will both be resolved with 0.33.x release of the Backend/UI slated for mid-November.

Sensor installations on macOS 10.13, High Sierra, require initial KEXT approval of the product kernel extension by administrative policy or end-user. This new requirement enforced by Apple applies to all third party products that have a driver component.

Cb Defense recommends that you preconfigure High Sierra devices with Cb Defense pre-approved drivers by using: MDM policy, netboot, or preconfigured images. This approach simplifies sensor deployment, especially in unattended mode.

If Cb Defense drivers are not pre-approved before sensor installation, the behavior is as follows:

- **Unattended installation: installation finalizes and returns success, but logs a warning to installation logs. Because CB Defense drivers cannot load, sensor enters Bypass state and reports this state to the cloud. After KEXT is approved (either by an end-user or an administrator with MDM policy), the sensor recovers within one hour and enters the full protection state.**

- **Attended installation is handled similarly to unattended, with two differences: (1) sensor installation displays a dialog message that requests the end user to approve the KEXT using system preferences; (2) installer stalls for up 10 minutes, giving a user a chance to approve the KEXT.**

To identify devices with sensors not supporting currently loaded OS, go to Enrollment page, change Status filter to *All*, and type the following search query:

sensorStates:UNSUPPORTED_OS

Use the following search query to help identify devices with sensors that do support the new OS but with sensor KEXT not approved:

sensorStates:DRIVER_INIT_ERROR

See *Apple Technical Note TN2459* for more details and recommendations for

enterprise.
Certificate Whitelisting feature introduced in 3.0 does not fully support PKG installers. Although the rule does apply to trusted, signed and verified PKG files, it currently does not extend to files that are embedded in the trusted signed PKG installers.
New installer code format: To fresh-install 3.0 sensors, use the 3.0-supported company installation and individual device installation codes. This might require a configuration update to software deployment tools.
Changed command-line interface for sensor unattended uninstallation to require a confirmation switch. The change might require an update of remote management tools. The new unattended procedure can be invoked via: ***/Applications/Confer.app/uninstall -y***
If you are using script *cbdefense_install_unattended.sh* for unattended sensor installation or upgrade, update your software deployment environment to use the script for 3.0 sensor DMG (extracted from *Volumes/CbDefense-3.0.X.X/docs/cbdefense_install_unattended.sh*). **The script for 1.X installers is not compatible with 3.0 installer PKG.**
Due to enhanced installer protections and new reputation engine, a downgrade from 3.0 to 1.2 is not supported out-of-the-box. Contact Support if this downgrade is required. **Uninstall and install is an alternative to a downgrade path; however, this process results in a new device ID and loss of linkage to the original device data.**
Live Response feature on macOS does not currently include the memory dump command.
Policy: *Use Windows Security Center*: setting has no affect on Mac. **Policy: *Delay Execute for Cloud Scan*: setting has no effect on Mac devices. Mac sensor implicitly enables delay execute for cloud scan, based on the configured policy rules. The delay is disabled when no prevention rules are present or when the only policy rules are for "Application" targets:**

- **"At path"**
- **"Company Blacklist"**

Otherwise, the delay is implicitly enabled to facilitate rules that rely on the cloud reputations and make policy enforcement decisions at pre-execution time.

Issues Resolved in 3.0

ID	Description
DSEN-207	Added sensor security log file (security.log).
DSEN-1353	Added Support for Policy options: *Scan files on network drives* and *Scan execute on network drive.* Previous behavior was to always scan. 3.0 behavior is to scan only if the options are enabled. Disabling *Scan files on network drives* can improve performance and eliminate inter-operability issues with certain network file-systems and on high latency networks, at a cost of malware detection on network-shares during on-access. Disabling *Scan execute on network drive* should be last resort.
DSEN-1364	Added Support for Policy Option: *Hash MD5.* Previous behavior was to always hash and report MD5, 3.0 behavior is to hash and report only if enabled.
EA-8975	Fixed missing file signature information from some Mac hosts.
EA-9822	Fixed sensor Bypass state taking several hours to update in the Cb Defense Management Console.
DSEN-937 EA-8098	Fixed case where an incident didn't appear on the Alerts List page; incomplete hash information in some behavioral events.
DSEN-1183	Fixed temporary loss of events after running Adobe installer or similar installers, triggering bursts in behaviors.
n/a	Fixed UDP NETFLOW events sometimes missing destination address information.

DSEN-380	**Reverse Shell Detection 2.0 (introduced in sensor 1.2.4) - reduced false positives and enhanced reporting of events (NETWORK_FLOW information and commands executed by the reverse shell)**
CIT-9596 CIT-10729 DSEN-47 DSEN-655 DSEN-745 DSEN-752	**Miscellaneous sensor installer improvements.**
DSEN-48	**Sensors uninstalled by end-users are now automatically removed (deregistered) from the backend, if the device is online at the time of uninstallation.**
DSEN-351 DSEN-555 DSEN-976 DSEN-1168 DSEN-1170	**Sensor UI: Displaying Threat name and other minor enhancements.**
DSEN-74	**Improved Keylogger (MONITOR_INPUT TTP) detection on macOS 10.11 and newer.**
DSEN-1407	**Improved cmd-line reporting in cases of process image replacement**
EA-8728 CIT-7673 CIT-10936 CIT-11010 CIT-11023 DSEN-328 DSEN-544 DSEN-746 DSEN-789 DSEN-860 DSEN-1038 DSEN-1050 DSEN-1065 DSEN-1165 DSEN-1166 DSEN-1189 DSEN-1299	**Miscellaneous detection and prevention improvements.**
EA-10170	**Certain development IDEs (PyCharm) took long time to load when exhibiting buffer overflows.**
CIT-11027	**Miscellaneous performance improvements.**

DSEN-1198	
CIT-1048	**Improved DNS request tracking with IPv6.**