Release Notes: macOS Sensor v7.2.0

June 2021

Summary

VMware Carbon Black EDR MacOS Sensor v7.2.0 reintroduces Path Exclusion functionality on Big Sur, which previously existed in kext-based versions. This functionality adds native support for Apple Silicon/M1 hardware in addition to bug fixes and performance and stability improvements. This sensor release also includes all changes and fixes from previous releases.

This document provides information for users upgrading to VMware Carbon Black EDR macOS Sensor v7.2.0 from previous versions, as well as users who are new to VMware Carbon Black EDR. The key information specific to this release is provided in the following major sections:

- **Installation Instructions** - Provides instructions for VMware Carbon Black EDR macOS sensor installation.
- **Corrective content** – Describes issues resolved by this release and general improvements in performance or behavior.
- **Known issues and limitations** – Describes known issues or anomalies in this version.

Server compatibility

VMware Carbon Black EDR sensors included with server releases are compatible with all server releases going forward. We always recommend that you use the latest server release with our latest sensors to utilize the full feature capabilities of our product; however, using earlier server versions with the latest sensor should not impact core product functionality.

Sensor operating systems

VMware Carbon Black EDR sensors interoperate with multiple operating systems. For the current list of supported operating systems for VMware Carbon Black EDR sensors (and all VMware Carbon Black products), see the following location in the VMware Carbon Black User Exchange: https://community.carbonblack.com/docs/DOC-7991

Documentation

See the full library of VMware Carbon Black EDR user documentation at https://docs.vmware.com/en/VMware-Carbon-Black-EDR/index.html.

Technical support

VMware Carbon Black EDR server and sensor update releases are covered under the Customer Maintenance Agreement. Technical Support is available to assist with any issues that develop during the installation or upgrade process. Our Professional Services organization is also available to assist to ensure a smooth and efficient upgrade or installation.

Installation Instructions

To install the new sensor, perform the following the steps. For unattended installs using an MDM solution, use the following inputs to create profiles for preventing endpoint user prompts. More information can be found at the User Exchange post here.

Plug-in ID: `com.carbonblack.es-loader`

System Extension Bundle ID: `com.carbonblack.es-loader.es-extension`

Application Bundle ID: `com.carbonblack.CbOsxSensorService`

Apple Team ID: `7AGZNQ2S2T`

To install the sensors to your server, perform the following instructions:

1. Ensure your VMware Carbon Black EDR YUM repo is set appropriately:
    a. The repository file to modify is */etc/yum.repos.d/CarbonBlack.repo*
    b. Baseurl = https://yum.distro.carbonblack.io/enterprise/stable/$releasever/$basearch/
2. On the VMware Carbon Black EDR server, clear the YUM cache by running the following command:

```
yum clean all
```

3. After the YUM cache has been cleared, download the sensor install package by running the following command:

```
yum install --downloadonly --downloaddir=<package local download
directory> <package>
```

Note: The <*package local download directory*> is a directory of your choice.

Note: <*package*> is replaced by cb-osx-sensor.

4. Install the new sensor package on the VMware Carbon Black EDR server by running the command:

```
rpm -i --force <package>
```

5. Make the new installation package available in the server console by running the command:

```
/usr/share/cb/cbcheck sensor-builds --update
```

Note: If your groups have **Automatic Update** enabled, the sensors in that group will start to automatically update.

Your new sensor versions should now be available via the console. For any issues, contact VMware Carbon Black Technical Support.

New Features

- **Path Exclusions** – Reintroducing configurable path exclusions to MacOS Big Sur using system extensions. This feature provides the capability to filter processes and activities on the sensor itself. This is very useful for processes such as Xcode, Timemachine Backups, and others that can be very noisy to the EDR agent.
- **Native M1 Support for Apple Silicon –** The EDR sensor has been rebuilt and compiled using universal binaries. This enables it to running natively when installed on an Apple computer that has an M1 chip that is using ARM binaries, and x86 binaries only when installed on non-M1 hardware.

Corrective Content

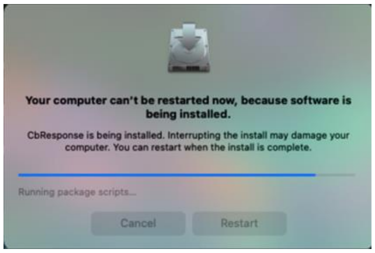
This release provides the following corrective content changes:

- Fixed an interoperability issue with other endpoint security products. [CB-34515]
- Removed unexpected characters in the command line during install/uninstall. [CB-33933]/[CB-34461]
- Fixed an issue where open processes being banned for the first time were not terminated. [CB-33583]
- Fixed an issue where subsequent processes of the same binary were not captured. [CB-34899]
- Improved process tree accuracy when fork events were attached to the incorrect parent process [CB-33217]

Known Issues and Limitations

- A limited number of features are not available in this version, but are intended for future development outside the kernel. These features include and are limited to event exclusions and proxy address reporting.

- If MDM profiles are not deployed to endpoints before installation, users are prompted to allow the `es-loader` system extension. Failure to allow the `es-loader` system extension upon installation will prevent a user from restarting the machine until the installation is complete. Attempting to restart the machine without the system extension approval will result in the following message. Manually allowing the extension in the System & Preferences pane will continue the installation. [CB-35532]:



Your computer can't be restarted now, because software is being installed.

CbResponse is being installed. Interrupting the install may damage your computer. You can restart when the install is complete.

Running package scripts...

- The System Extension can report binaries for the sensor daemon from the `/var/lib/cb` directory. [CB-32943]

- Downgrades to a 6.x series sensor, if required, should be initiated via the server console. Manual downgrades are not recommended and can fail. [CB-33288]

- Upgrading the OS from macOS 10.13.6 to 11.3.1 after installing sensor v7.2.0 will cause the system extension to crash due to an Apple bug that is related to signing of the extension. This bug has been reported to Apple. [CB-35505]

- When content filters are installed and enabled or uninstalled and disabled, existing connections are terminated. This is by design per Apple. [CB-32640]

- The Mac Response sensor does not store Live Response activity in the `sensor.log` file by default. Users can monitor Live Response activity using the `live-response.log` found under `/var/log/cb/audit` on the Carbon Black EDR server. Additionally, users can enable more verbose logging of the `sensor.log` file to capture Live Response activity on the Mac endpoint. **Note**: Enabling verbose logging can quickly consume the specified `sensor.log` size and should be used cautiously. Verbose logging can lead to shorter retention of audit information. Verbose logging can be enabled by modifying the `logging.config` file under `/var/lib/cb` to set the following parameters: `minloglevel: 0,  V:0`. [CB-8908]

- Uninstallation of the sensor should be done via the Server. Manual uninstallation via Terminal will require the user password to be entered. This is by design per Apple. [CB-32640]

Contacting Support

Use one of the following channels to request support or ask support questions:

- **Web:** User eXchange
- **Email:** support@carbonblack.com
- **Phone:** 877.248.9098
- **Fax:** 617.393.7499

Reporting Problems

When contacting VMware Carbon Black Technical Support, be sure to provide the following required information about your question or issue:

- **Contact:** Your name, company name, telephone number, and email address
- **Product version**: Product name (VMware Carbon Black EDR server and sensor version)
- **Hardware configuration:** Hardware configuration of the VMware Carbon Black EDR server (processor, memory, and RAM)
- **Document version:** For documentation issues, specify the version or date of the manual or document you are using
- **Problem:** Action causing the problem, error message returned, and event log output (as appropriate)
- **Problem severity:** Critical, serious, minor, or enhancement request