# Enterprise EDR OER

30 May 2024
VMware Carbon Black Cloud

vmware
by Broadcom

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://docs.vmware.com/

**VMware by Broadcom**
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

# Contents

# Preface

Carbon Black Enterprise EDR delivers powerful threat hunting and incident response capabilities on the Carbon Black Cloud.

# Supported Operating Systems for the Carbon Black Cloud Sensor

1

For a complete list of supported operating systems, see the following sensor OERs:

- Carbon Black Cloud Windows Sensor on Windows Desktop OER
- Carbon Black Cloud Windows Sensor on Windows Server OER
- Carbon Black Cloud Linux Sensor OER
- Carbon Black Cloud macOS Sensor OER

# Supported Browsers for the Carbon Black Cloud Console

2

- **Windows**: Firefox, Chrome, and Edge
- **macOS**: Safari, Firefox, and Chrome

# Linux 4.4+ Kernels for Linux Sensor 2.10+

3

Prior to installing the sensor, the underlying BPF implementation requires the Linux kernel headers for the active kernel to be installed.

See Linux Kernel Requirements for Linux Sensor Versions 2.10+ .

# macOS User Space Functionality

4

Beginning in macOS 11, the Carbon Black Cloud macOS sensor (v3.5.1) operates by default in user-space via System Extensions (user-space) instead of Kernel Extensions (KEXTs) that are used in prior versions of the agent. Therefore, there are some functional differences when using the sensor in System Extension mode on macOS 11 and later.

Using the sensor in KEXT mode achieves the same functionality on macOS 11 as it does on older operating systems.

Unless otherwise specified, documentation related to macOS functionality on the Carbon Black Cloud pertains to macOS 10.15 and earlier or to functionality delivered via the KEXT on macOS 11.

The following matrix outlines macOS functionality on the Carbon Black Cloud. The functionality detailed in the macOS 11+ column pertains to the sensor's functionality in user space (System Extension) in the initial macOS 11-compatible sensor release (v3.5.1+). For functionality provided via the kernel extension, refer to the macOS 10.12 - 11+ column.

Table 4-1. macOS User Space Functionality in Enterprise EDR

| Functionality | macOS10.12 - 11 (KEXT) | macOS 11+(user-space) |
|---|---|---|
| Continuous Endpoint Telemetry Data Collection: | | |
| ■ Process Start/Stop/Parent/Source binary, etc. | X | X |
| ■ In/Outbound Network Connections | X | X |
| ■ File Modifications (RWCD) | X | X |
| ■ Cross Process Memory Injection/ Scraping | X | |
| ■ Module Loads | X | |
| ■ Script Loads | X | X |
| 30 Day Data Retention (longer if associated with an alert) | X | X |
| Regex and Wildcard Search/Alert Query Language Support | X | X |

Table 4-1. macOS User Space Functionality in Enterprise EDR (continued)

| Functionality | macOS10.12 - 11 (KEXT) | macOS 11+(user-space) |
|---|---|---|
| Custom/Customer-created Alert Criteria | X | X |
| Support for Industry-standard Threat Feeds (STIX/TAXII) | X | X |

# Sensor Hardware Requirements

5

Endpoints must be in compliance with all hardware requirements for the host operating system.

Consider all processes that run on the endpoints when determining your hardware configuration. We recommend a multi-core CPU for all installations.

The following metrics represent system requirements against a minimum environment, which is defined in the context as a user level system (such as an inactive laptop).

Read the following topics next:

- Windows Sensor Hardware Requirements
- macOS Sensor Hardware Requirements
- Linux Sensor Hardware Requirements

## Windows Sensor Hardware Requirements

Table 5-1. Product: Enterprise EDR on Windows

| Metric | Enterprise EDR + Endpoint Standard | Enterprise EDR + Endpoint Standard + Audit & Remediation |
|---|---|---|
| CPU | Minimum: 1.8 GHz Recommended: 2 GHz | Minimum: 1.8 GHz Recommended: 2 GHz |
| Memory | 1 GB2 GB for Windows 10/2016+ | 1 GB2 GB for Windows 10/2016+ |
| Cores | 2 | 2 |
| Network required | Minimum: 100 Mbit Recommended: 1 Gbit | Minimum: 100 Mbit Recommended: 1 Gbit |
| Minimum network during light usage | 1k bytes/sec read/writes each | 1k bytes/sec read/writes each |
| Free disk space | Minimum: 100 MB Recommended: 500 MB | Minimum: 100 MB Recommended: 500 MB |

## macOS Sensor Hardware Requirements

Table 5-2. Product: Enterprise EDR on macOS

| Metric | Enterprise EDR | Enterprise EDR + Audit & Remediation | Endpoint Standard + Enterprise EDR | Endpoint Standard + Enterprise EDR + Audit & Remediation |
|---|---|---|---|---|
| CPU | Any supported x86-64 or arm64* | Any supported x86-64 or arm64* | Any supported x86-64 or arm64* | Any supported x86-64 or arm64* |
| Memory | 2 GB | 2 GB | 2 GB | 2 GB |
| Cores | 2 | 2 | 2 | 2 |
| Network required | Minimum: 100 Mbit<br>Recommended: 1 Gbit | Minimum: 100 Mbit<br>Recommended: 1 Gbit | Minimum: 100 Mbit<br>Recommended: 1 Gbit | Minimum: 100 Mbit<br>Recommended: 1 Gbit |
| Minimum network during light usage | 1k bytes/sec read/ writes each | 1k bytes/sec read/ writes each | 1k bytes/sec read/ writes each | 1k bytes/sec read/ writes each |
| Free disk space | Minimum: 100 MB<br>Recommended: 500 MB | Minimum: 100 MB<br>Recommended: 500 MB | Minimum: 200 MB<br>Recommended: 1 GB | Minimum: 200 MB<br>Recommended: 1 GB |

*arm64 CPU requires macOS sensor 3.6 or higher.

# Linux Sensor Hardware Requirements

Table 5-3. Product: Enterprise EDR on Linux

| Metric | Enterprise EDR | Enterprise EDR + Endpoint Standard | Enterprise EDR + Endpoint Standard + Audit & Remediation |
|---|---|---|---|
| CPU | Any 64-bit x86-64 chipset<br>No speed required | Any 64-bit x86-64 chipset<br>No speed required | Any 64-bit x86-64 chipset<br>No speed required |
| Memory | 100 MB | 250 MB | 250 MB |
| Cores | 2 | 2 | 2 |
| Network Required | Minimum: 100 Mbit<br>Recommended: 1 Gbit | Minimum: 100 Mbit<br>Recommended: 1 Gbit | Minimum: 100 Mbit<br>Recommended: 1 Gbit |
| Minimum network during light usage | 1k bytes/sec read/writes each | 1k bytes/sec read/writes each | 1k bytes/sec read/writes each |
| Free disk space | /opt: 100 MB<br>/var: 1600 MB | /opt: 100 MB<br>/var: 2600 MB | /opt: 100 MB<br>/var: 3200 MB |

# Document History

6

The following changes were made to this document:

| Date | SW Version | Topic | Change Description |
|---|---|---|---|
| 30 May 2024 | N/A | All | Updated product name |
| 31 July 2023 | N/A | Chapter 3 Linux 4.4+ Kernels for Linux Sensor 2.10+ | Updated link |
| 14 April 2022 | N/A | Chapter 1 Supported Operating Systems for the Carbon Black Cloud Sensor | Added links to new sensor OERs |
| 8 April 2022 | N/A | All | Updated document architecture |