vmware

Carbon Black
EDR

VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5

Supplemental Administrative Guidance for Common Criteria

Version: 1.1
July 27, 2021

VMware Carbon Black
1100 Winter Street
Waltham, MA 02451

Prepared By:

Booz | Allen | Hamilton
delivering results that endure

Cyber Assurance Testing Laboratory
1100 West Street
Laurel, MD 20707

Table of Contents

List of Tables

1 Introduction

The VMware Carbon Black Endpoint Detection and Response (CB EDR) Server 7.5 is a software application that is deployed on a Red Hat Enterprise Linux server platform. The VMware CB EDR Server operates as a server to perform its function of indexing and storing endpoint system event data obtained from host sensors, as well as providing any configuration and software updates for the host sensors to pull during the periodic check-ins. The Protection Profile for Application Software Version 1.3 (APP_PP) defines an application as "software that runs on a platform and performs tasks on behalf of the user or owner of the platform, as well as its supporting documentation."

As a Common Criteria evaluated product, this guidance serves to define the 'evaluated configuration' in which the evaluation was performed and to summarize how to perform the security functions that were tested as part of the evaluation.

2 Intended Audience

This document is intended for administrators responsible for installing, configuring, and/or operating VMware CB EDR Server 7.5. Guidance provided in this document allows the reader to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria (CC) testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the CC evaluation. The reader is also expected to be familiar with the VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 Security Target and the general CC terminology that is referenced in it. This document references the Security Functional Requirements (SFRs) that are defined in the Security Target document and provides instructions for how to perform the security functions that are defined by these SFRs. The VMware CB EDR Server product, as a whole, provides a great deal of security functionality but only those functions that were in the scope of the claimed PP are discussed here. Any functionality that is not described here or in the VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 Security Target was not evaluated and should be exercised at the user's risk.

3 Terminology

In reviewing this document, the reader should be aware of the terms listed below. These terms are also described in the VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 Security Target.

CC: stands for Common Criteria. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

SFR: stands for Security Functional Requirement. An SFR is a security capability that was tested as part of the CC process.

TOE: stands for Target of Evaluation. This refers to the aspects of the VMware CB EDR Server product that contain the security functions that were tested as part of the CC evaluation process.

Administration Workstation: Any general-purpose computer that is used by an enterprise administrator to manage the TOE remotely via a web browser.

Application Management: Management of the Sensors by an enterprise administrator using the operational environment's VMware Carbon Black EDR Server.

Endpoint System: A device or set of devices, such as a laptop or desktop, with a Windows operating system, that has the host sensors installed.

Endpoint User: An individual who has access to the Endpoint System but is not able to manage its behavior.

Enterprise Administrator: The administrator who has system permissions to access sensitive data and perform management functionality on the VMware Carbon Black EDR Server (TOE).

Host Sensor: Generic term for VMware Carbon Black EDR Windows Sensor.

Sensor Group: Each host sensor is associated with a sensor group that defines its configuration and security characteristics. A sensor group must contain at least one host sensor and can contain many host sensors. However, a single host sensor can only belong to one sensor group. Sensor groups can be based on the security and organizational requirements. For example, one could base sensor groups on functional groupings/departments (such as marketing, customer service, or IT) or location.

4 References

The following security-relevant documents are included with the TOE. This is part of the standard documentation set that is provided with the product. Documentation that is not related to the functionality tested as part of the CC evaluation is not listed here.

[1] VMware Carbon Black EDR User Guide, VMware Carbon Black EDR 7.5

The following document was created in support of the VMware CB EDR Server CC evaluation:

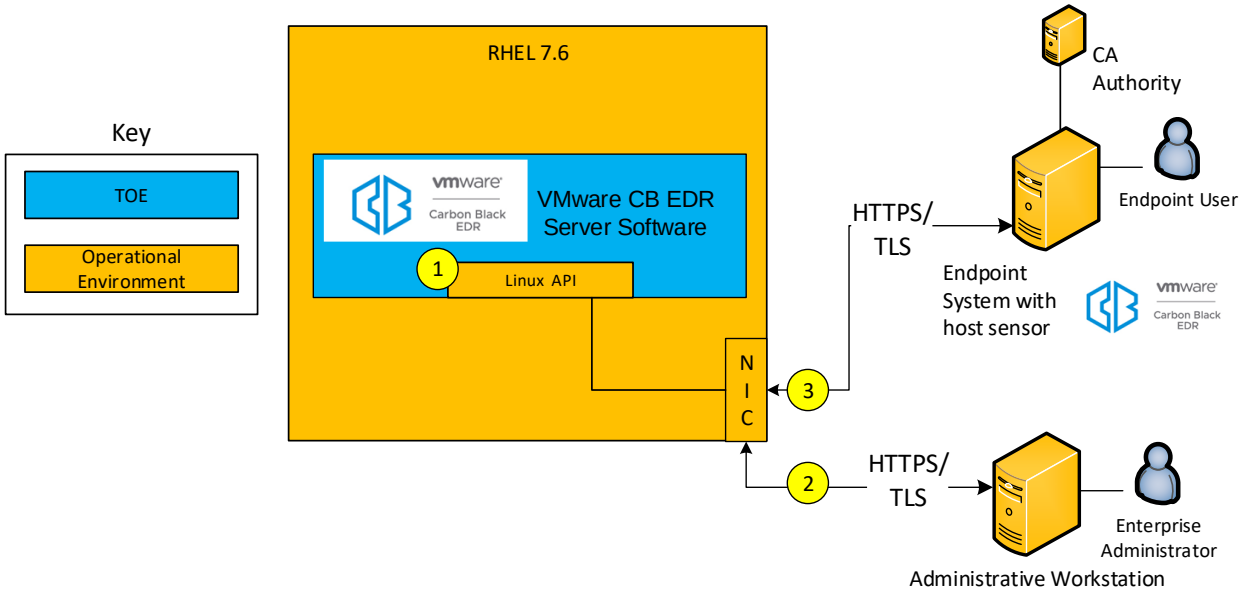
[2] VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 Security Target, v1.1

The following documents were created in support of the VMware CB EDR Windows Sensor CC evaluation:

[3] VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2 Security Target, v1.3
[4] VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2 Supplemental Administrative Guidance for Common Criteria, v1.1

5 Evaluated Configuration of the TOE

This section lists the components that have been included in the TOE's evaluated configuration, whether they are part of the TOE itself, environmental components that support the security behavior of the TOE, or non-interfering environmental components that were present during testing but are not associated with any security claims. The figure below depicts the TOE within its operational environment.



5.1 TOE Components

The TOE is the VMware Carbon Black EDR Server

7.5 application, referred to as VMware CB EDR Server or TOE. The TOE is installed on a physical server running Red Hat Enterprise Linux (RHEL) 7.6 and utilizes several functions of the operating system to perform its operations.

The following table describes the TOE components in the evaluated configuration:

Component	Definition
VMware CB EDR Server (TOE)	The TOE is a management server and central data storage for host sensors that have gathered and reported endpoint system event data to the TOE for storage and indexing.

Table 1: Evaluated Components of the TOE

5.2 Supporting Environmental Components

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

Component	Definition
Red Hat Enterprise Linux (RHEL) 7.6	The operating system environment that the TOE application is installed on.
Host Sensor (VMware CB EDR Windows Sensor)* *evaluated separately	An application that is installed on a Windows platform, which collects event data from the host endpoint system and reports the data back to the TOE.
Administration Workstation	Any general-purpose computer that is used by an enterprise administrator to manage the TOE remotely via a web browser.
Certificate Authority	The server deployed within the Operational Environment which confirms the validity and revocation status of certificates. This is only required for the

	Endpoint System with Host Sensor to validate TOE server certificate. Including for completeness.

Table 2: Evaluated Components of the Operational Environment

5.3 Resource Access Requirements

By installing the VMware CB EDR Server and agreeing to the End User Licensing Agreement (EULA), the end user agrees to allow the TOE to access the following resources:

Hardware Resources Access

- Network Connectivity: The TOE invokes the OS to establish an HTTPS session over TLSv1.2 (HTTPS/TLS) trusted channel to respond to requests from:
  - Remote administrators using a web browser to access the TOE's web UI. Port for remote administration
  - Host sensors as part of their polling cycles which includes:
    - receiving collected host platform system information
    - sending configuration updates and software updates

Sensitive Information Repositories Access

- There are no sensitive information repositories (storage locations for private user or administrator data) that the TOE requires access.

5.4 Assumptions

In order to ensure the product is capable of meeting its security requirements when deployed in its evaluated configuration, the following conditions must be satisfied by the organization, as defined in the claimed Protection Profile:

- **Platform:** The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- **Proper administrator:** The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.
- **Proper user:** The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.

6 Secure Installation and Configuration

Documentation for how to order and acquire the TOE is described under the Contact Us link on the Carbon Black website www.carbonblack.com. Section 5.1 of this document lists the properties that are associated with the TOE. When downloading the TOE, this documentation should be checked as part of the acceptance procedures so that the correctness of the software application can be verified.

6.1 Initial Out-Of-The-Box Setup

Before the VMware Carbon Black EDR Server is installed, there are a several pre-requisite configurations that need to be performed by the administrator on the underlying platform.

6.1.1 Pre-requisites on the VMware CB EDR Server System:

The VMware CB EDR Server should be installed on a clean official RHEL 7.6 distribution. The instructions set should be the same whether it is installed on a bare metal box (as required for CC certification) or in a virtual environment.

1. From the official Red Hat download site, download the full ISO for the RHEL 7.6.

   NOTE: You must have a valid RHEL user account.

2. Click on software selection early so the system does not go through the regular automated install and select "**Server with GUI**" with the following Add-Ons:
   a. Security Tools
   b. System Administration Tools

3. Ensure that LUKS Encryption is specified and configured on the OS installation destination.
   a. Enable block device encryption by checking "**Encrypt System**" during the partitioning selection.
   b. Specify the encryption passphrase required to decrypt the encrypted device(s).
   c. Ensure the "**United States Government Configuration Baseline**" profile is selected for the OS Security Policy, which enables FIPS and SELinux mode for the OS during installation time.
   d. Configure the remaining OS installation steps (e.g. network, hostname, etc.).
   e. After installation of the OS is completed, register with the subscription manager by following procedures here: https://access.redhat.com/solutions/253273
   f. Update security dependencies via 'yum update' as described here: https://access.redhat.com/articles/1403233 under "How can I keep my CC-configured system patched?"

```
yum install yum-plugin-security
yum updateinfo
yum update --security
```

4. Configure X.509 certificates for the TOE:
   a. Generate an appropriate signing CA certificate with an RSA 4096 bit key and SHA256 as the signing algorithm.
   b. Generate a TOE server certificate signed by the CA certificate from step (a) with an RSA 2048 bit key and SHA256 as the signing algorithm. The TOE server certificate should have the following X.509 extensions:

      subject: CN=<*hostname of the server*>
      basicConstraints, CA:FALSE
      keyUsage: digitalSignature, keyAgreement
      extendedKeyUsage: serverAuth
      subjectKeyIdentifier: hash

subjectAltName = DNS.1:<*hostname of the server*>
authorityInfoAccess = OCSP;URI:<*URI of the OCSP responder server*>

c. Place the CA signing certificate and key in the following location on the TOE host:

/etc/pki/ca-trust/source/cb-client-ca.crt

/etc/pki/ca-trust/source/cb-client-ca.key

d. Place the TOE server certificate and key in the following location on the TOE host:

/etc/pki/tls/certs/cb-server.crt

/etc/pki/tls/private/cb-server.key

6.1.2 Installing the VMware CB EDR Server

Installation and first-time setup of the TOE can be accomplished by following the steps outlined below which use procedures. The initial installation requires the enterprise administrator to download a customer specific .rpm file from the VMware CB website onto the host server platform and perform "yum install". The steps below will specify any options required for the CC evaluation.

1. Obtain the TOE application software and place it onto the TOE host as root.

2. Execute the following command as root to initialize the installation of the TOE application:

```
rpm -ivh <VMware CB EDR Server filename>.x86_64.rpm
```

3. Update /etc/yum.repos.d/CentOSBase.
repo to enable the baseurl of http://mirror.centos.org.

4. Verify the date and time settings are accurate on the TOE host.

5. Execute the following command as root:

```
yum install cb-enterprise
```

   a. If prompted, install the CentOS GPG key.
   b. If the TOE's environment requires that outbound firewall exceptions be made, ensure to follow the exceptions documented in "Firewall Configuration for Feeds" in [1].

6. When the installation completes, initialize and configure the VMware CB EDR Server:
   a. Execute the following command as root to initialize the TOE with a specific set of parameters in order to use the pre-configured X.509 certificates:

```
/usr/share/cb/cbinit --retain-orig-cert-paths --
```

```
server-cert-key=/etc/pki/tls/private/cb-server.key --
server-cert-file=/etc/pki/tls/certs/cb-server.crt --
client-ca-cert-key=/etc/pki/ca-trust/source/cb-client-
ca.key --client-ca-cert-file=/etc/pki/ca-
trust/source/cb-client-ca.crt
```

b. Press `[Return]` to open the EULA. When you are done reviewing it, if you agree to the terms, enter `q` and then enter `yes` to continue the configuration.
c. Select a storage location for your data and press `[Return]`.
d. Enter an initial Administrator account to log in and configure VMware CB EDR Server. Enter values for "**Username**", "**First Name**", "**Last Name**", "**E-Mail**", "**Password**", and "**Confirm password**".
e. Press `[Enter]` and then validate the account information by entering `y`.
f. In the Sensor Communications section, you define the address that the sensors will use to communicate back to the VMware CB EDR Server:

```
Would you like to keep the default [Y/n]: n
Use SSL [Y/n]: Y
Hostname [192.168.117.141]: cbr.company.com
Port [443]: return
```

If the Verify Account Information looks correct:

```
Is this correct [Y/n]: Y
```

NOTE: The IP address of the server will be accessed via the default SSL port 433. A best practice is to use a DNS record that points to this IP address.

g. Review all prompts and configure sharing settings in accordance with your company's security policies. The recommended settings are provided here. You can change these settings at any time by accessing the VMware CB EDR Server console and clicking Username > Sharing Settings.
    i. This enables the program to be supplemented with updated threat intelligence from CB Threat Intel and the extended network of CB Threat Intel partners.

```
Do you want to enable communication with the
Carbon Black Alliance? – Y
```

    ii. This enables the VMware CB EDR Server to submit health statistics back to Carbon Black. These are used by Carbon Black Support and Professional Services to determine how the allocated VMware CB EDR Server is performing with our application.

```
Do you want your server to submit statistics and
feedback information to Carbon Black? – Y
```

iii. See Chapter 17 – "Threat Intelligence Feeds" in [1] for more information on sharing hashes with VMware CB EDR Server.

```
Do you want the default sensor group to submit
hashes to Carbon Black Alliance? – N
```

iv. Save settings.

```
Continue with current sharing settings? – Y
```

h. The SSL Certificates section is automated and requires no user input. If you used arguments pointing to valid certificate and key files when you ran cbinit, the certificate from your organization is substituted for the default certificate created by the server. Run the following script to create an encrypt backup of your certificates. The exact certificates are critical to disaster recovery efforts.

```
/usr/share/cb/cbssl backup --out <backup filename>
```

i. In the IP Tables section, answer `Y`. This opens port 433 in the server's IP tables.
j. The POSTGRESQL Database Setup section is automated and requires no user input.
k. In the Setup Complete section, enter `Y` to start the services.

NOTE: To confirm sensor-to-server communications are functioning properly:

i. Open a web browser and launch the TOE's web UI: https://<*VMware CB EDR Server IP address*>
ii. Download a sensor and install it on an endpoint. For more information on installing and managing sensors, refer to [4].

7. Configure (as root) the allowed TLS ciphers for Common Criteria configuration on the RHEL operating system by modifying /var/cb/nginx/props/nginx.runtime.ssl_ciphers.prop to contain:

```
ssl_ciphers EECDH+AESGCM:EDH+AESGCM;
ssl_ecdh_curve prime256v1:secp384r1;
```

8. If the TOE application was already started, restart the nginx service using the following command as root:

```
/usr/share/cb/cbservice cb-nginx restart
```

6.1.3 Installing the VMware CB EDR Windows Sensor

Installation and first-time setup of a host sensor (VMware CB EDR Windows Sensor) can be

accomplished by following the steps outlined in [4]. The installation and configuration of a host sensor include administrative actions being performed via the VMware CB EDR Server's web UI.

6.2 Cryptographic Configuration

There is no TOE-required configuration for cryptography. The TOE does not perform any asymmetric key generation. The TOE invokes the underlying RHEL platform to perform all cryptographic services including DRBG functionality and HTTPS sessions over TLSv1.2 (HTTPS/TLS) trusted communications. The TOE also invokes the underlying RHEL platform's OpenSSL cryptographic module to generate RSA scheme certificates for the Sensor Group Certificate. These certificates are included as part of the Host Sensor's installation package and are used for Host Sensor identification to the TOE during their check-in cycles. The administrator installing the TOE is expected to perform all of the operations in Section 6 of this document to configure the underlying RHEL platform's cryptographic services.

NOTE: The TOE was installed on a certified RHEL OS and platform based on the "*Red Hat Enterprise Linux 7.6 Security Target Version 1.1 June 2020*" in order to have assurance of correct cryptographic implementation. Cryptographic Algorithm Verification Program (CAVP) certificate numbers are contained in the referenced RHEL evaluation documentation.

NOTE: The TOE operates as a HTTPS/TLS server for its trusted communications with host sensors and web browsers for administration. If a HTTPS/TLS connection is interrupted, the TOE will wait for the HTTPS/TLS client to attempt to re-establish the connection.

NOTE: The use of other cryptographic engines and cryptographic settings were not evaluated nor tested during the Common Criteria evaluation of the TOE.

7 Secure Management of the TOE

The following sections provide information on managing TOE functionality that is relevant to the claimed Protection Profile. Note that this information is largely derived from [1] but summarized here to discuss only actions that are required as part of the 'evaluated configuration'. The enterprise administrator is encouraged to reference this document in full in order to have in-depth awareness of the security functionality of the VMware CB EDR Server, including functions that may be beyond the scope of this evaluation.

7.1 Administrator Functionality

The TOE provides a remote web UI to allow enterprise administrators to manage the TSF. This interface provides functions that are related to the management of the server application itself. Only the functions that are relevant to the TSF and have SFR claims are discussed in this guidance document.

7.1.1 Version Verification

The enterprise administrator can verify the version of the TOE through the web UI.

1. Navigate to the TOE's web UI: https://<*VMware CB EDR Server IP address*>
2. Authenticate via the UI as an enterprise administrator.

3. In the lower right corner, click on the version number information.

The enterprise administrator can also check the TOE's version via the OS platform by executing the following command as root:

```
yum info cb-enterprise
```

7.1.2 Uninstall VMware CB EDR Server

Uninstallation of the TOE can be performed by the running the YUM utility to remove all remnants that constitute the TOE or remove packages plus all other third-party packages upon which it depends. When the TOE application is uninstalled, settings are left behind for the purposes of re-installing the TOE software while maintaining previous configuration (recovery).

1. Via the OS platform, execute the following command as root to stop VMware CB EDR Server services:

```
service cb-enterprise stop
```

2. Confirm that the /etc/yum.conf file contains the following line:

```
clean_requirements_on_remove=1
```

3. Execute the following commands:

```
yum erase cb-enterprise

yum remove carbon-black-release

rm -rf /var/www/cb/

rm -rf /var/run/cb/

rm -rf /var/log/cb/

rm -rf /var/lib/cb/

rm -rf /var/cb/

rm -rf /usr/share/cb/

rm -rf /etc/cb/
```

7.2 Secure Updates

The TOE application is packaged in an .rpm file format for the RHEL OS platform. The VMware CB

EDR Server product's individual RPMs (installations and updates) are signed using a VMware CarbonBlack certificate via GPG signing. The binary code is only modified or replaced when a manual software update is performed from the OS. The TOE does not automatically download, modify, replace, or update its own binaries or executable files.

The YUM repo file is configured to validate GPG signatures automatically. YUM uses the VMware CB public key, available from the same VMware CB EDR REPO that the .rpm was downloaded from, to validate the signatures. With signature verification enabled, YUM will refuse to install any packages not GPG-signed with the correct key for that repository.

7.2.1 Check for an Update

1. On the underlying platform that is running the TOE, execute the command (as root) to check if any updates to the TOE are available.

```
yum check-update cb-enterprise
```

2. Verify that the command does not return any errors.

7.2.2 Perform an Update:

1. On the underlying platform that is running the TOE, execute the following commands (as root):

```
service cb-enterprise stop
yum clean all
yum upgrade cb-enterprise
service cb-enterprise start
```

2. Configure (as root) the allowed TLS ciphers for Common Criteria configuration on the RHEL operating system by modifying /var/cb/nginx/props/nginx.runtime.ssl_ciphers.prop to contain:

```
ssl_ciphers EECDH+AESGCM:EDH+AESGCM;
ssl_ecdh_curve prime256v1:secp384r1;
```

3. If the TOE application was already started, restart the nginx service using the following command as root:

```
/usr/share/cb/cbservice cb-nginx restart
```

8 Operational Modes

The TOE does not have operational modes. When the TOE is first installed, it is considered to be in its evaluated operational mode provided the pre-requisites outlined in Section 6.1.1 and installation steps outlined in Section 6.1.2 of this document have been accomplished. Once these steps have been completed, the TOE will be in its normal operational mode to perform the functions as described in the Security Target.

There is no separate error mode or other degraded mode of operation. If the VMware CB EDR Server fails, the TOE's application will need to be restarted with the following command:

```
service cb-enterprise restart
```

If that does not work, reboot the entire system the TOE is installed on. If the TOE has been corrupted or the application has failed such that restarting and rebooting will not resolve the issue, an administrator will need to contact VMware Carbon Black support per the guidance in Section 9.

9 Additional Support

VMware Carbon Black provides technical support for its products, if needed, on their Support website https://www.carbonblack.com/support/. Customers can register for a User Exchange account to open a support case at by clicking on 'User Exchange' at the bottom of the Support website. Additionally, customers can open a ticket with a VMware Carbon Black representative by calling (877) 248-9098 (toll free) or (617) 393-7400 (choose option 2), or by emailing support@carbonblack.com.