National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

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

Report Number: CCEVS-VR-VID11156-2021
Version 1.0
August 02, 2021

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Linda Morrison
Clare Parran
Ted Farnsworth

The MITRE Corporation

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Laurel, Maryland

Contents

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 3 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 provided by VMware Carbon Black. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in August 2021. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the *Protection Profile for Application Software Version 1.3* (APP_PP), March 1, 2019.

The TOE is the VMware Carbon Black Endpoint Detection and Response Server 7.5 application, referred to as VMware CB EDR Server or TOE from this point forward. The VMware CB EDR Server product's primary functionality is receiving endpoint system event data from one or more host sensors for indexing, analyzing, and storing the event data. The VMware CB EDR Server also allows administrators to create and deploy sensor groups, configure host sensors, configure the data collection policy that each host sensor will enforce, update the host sensors, and uninstall host sensors.

The TOE is an application that is installed on a RHEL 7.6 system with Linux Unified Key Setup (LUKS) encrypted partitioning enabled. The TOE is administered through a web user interface (web UI) via a web browser.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5), as interpreted by the Assurance Activities contained in the APP_PP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the APP_PP Assurance Activities. The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5
Protection Profile	Protection Profile for Application Software Version 1.3 [APP_PP], including all applicable NIAP Technical Decisions and Policy Letters
Security Target	VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 Security Target v1.1 dated July 27, 2021
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5" Evaluation Technical Report v1.1 dated July 27, 2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	VMware Carbon Black
Developer	VMware Carbon Black
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Paul Bicknell Linda Morrison Clare Parran Ted Farnsworth

Table 1– Evaluation Identifiers

3 Assumptions and Clarification of Scope

3.1 Assumptions

The assumptions are drawn directly from the APP_PP.

3.2 Threats

The threats are drawn directly from the APP_PP.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the *Protection Profile for Application Software Version 1.3*, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the APP_PP are claimed by the TOE and documented in the ST.
- This evaluation covers only the specific device model and software version identified in this document, and not any earlier or later versions released or in process.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter vulnerabilities that were not "obvious" or vulnerabilities to security functionality not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. All other functionality provided by these devices, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. In particular, the VMware Carbon Black EDR Server 7.5 support of collecting, indexing, analyzing, and storing endpoint system event data as well as managing host sensors was not assessed as part of this evaluation. Further information of excluded functionality can be found in Section 2.3 of the Security Target.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

The TOE is application software that is deployed on a RHEL OS and provides enterprise-level system visibility of IT infrastructure. The [APP_PP] states the following:

"The application, which consists of the software provided by its vendor, is installed onto the platform(s) it operates on. It executes on the platform, which may be an operating system, hardware environment, a software-based execution environment, or some combination of these. Those platforms may themselves run within other environments, such as virtual machines or operating systems, that completely abstract away the underlying hardware from the application. The TOE is not accountable for security functionality that is implemented by platform layers that are abstracted away. Some evaluation activities are specific to the particular platform on which the application runs, in order to provide precision and repeatability."

The Application Software TOE type is justified because the TOE is a application software that provide enterprise-level system visibility for the IT infrastructure that is installed on standalone desktops or workstations running a platform OS that communicates back to a remote server.

4.2 Physical Boundary

VMware Carbon Black EDR Server 7.5 is a software-only TOE. All hardware that is present is part of the TOE's Operational Environment.

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 server platform	The host platform with the RHEL operating system environment that the TOE application is installed on.
Endpoint System with 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 platform 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 – IT Environment Components

NOTE: It is expected that the TOE is operating on a Common Criteria certified operating system and platform based on the Red Hat Enterprise Linux 7.6 (VID11039-2020).

5 Security Policy

The TOE enforces the following security policies as described in the ST.

5.1 Cryptographic Support

The TOE invokes the underlying platform to perform all cryptographic services including HTTPS sessions over TLSv1.2 (HTTPS/TLS) trusted communications and hashing user password credentials for storage.

5.2 User Data Protection

The TOE application restricts its access to the host system's network connectivity resources. Network activity is restricted to establishing HTTPS/TLS connections to remote management (via web UI) and sensor check-in requests. During the host sensor check-in, the TOE receives sensor-collected endpoint system data for the host sensor as well as providing any configuration and software updates for the host sensors to pull during the check-in. The TOE requires LUKS encrypted partitioning to protect local sensitive data storage.

5.3 Security Management

The TOE does not provide any default credential used for initial authentication. The TOE uses the underlying platform's recommended methods for storing and setting configuration options. The TOE provides enterprise administrators with the ability to manage the TOE and host sensor through a web UI.

5.4 Privacy

The TOE does not transmit any personally identifiable information (PII) over the network.

5.5 Protection of the TSF

The TOE is packaged as separate software that is installed on the platform and can be uninstalled/removed if needed. The enterprise administrator can verify the software version from the web UI. All updates are downloaded and installed by an enterprise administrator using the OS software package manager. The digital signature of the update is verified by the platform during installation. Otherwise, the TOE does not download, replace, or modify its own binary code. The TOE implements anti-exploitation features, such as stack-based overflow protection, is compatible with security features provided by the OS, and only uses documented APIs and libraries.

.

5.6 Trusted Path/Channels

The TOE invokes the OS platform to act as a HTTPS/TLS v1.2 non-mutual authentication server for both the host sensor check-in and the remote administrative web browser communication channels.

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 Supplemental Administrative Guidance for Common Criteria – v1.1, July 27, 2021
- VMware Carbon Black EDR User Guide VMware Carbon Black EDR 7.5

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

7 Evaluated Configuration

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 3 - Evaluated Components of the TOE

Section 4.2 describes the TOE's physical configuration as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to communicate with the following environment components:

- RHEL 7.6 platform (Server host)
- Windows Sensor (VMware CB EDR Windows Sensor)
- Administration Workstation

To use the product in the evaluated configuration, the product must be configured as specified in the *VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 Supplemental Administrative Guidance for Common Criteria Version 1.1, July 27, 2021* document.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the *Assurance Activity Report for a Target of Evaluation "VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5" Assurance Activities Report v1.1, July 27, 2021*.

8.1 Developer Testing

No evidence of developer testing is required in the Evaluation Activities for this product.

8.2 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the APP_PP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that:

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.3 Evaluation Team Vulnerability Testing

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with the APP_PP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

Keyword	Description
VMware Carbon Black	This is a generic term for searching for known vulnerabilities for the overall company that authored the TOE product.
Endpoint Detection and Response	This is a generic term for searching for known vulnerabilities for the specific TOE product.
	Third party libraries
Lucene 8.6.3	This is a generic term for searching for known vulnerabilities for the specific third-party library. Version used to filter initial results to only relevant items. Version used to filter initial results to only relevant items. VMware customized this library but is based on Apache SOLR/Lucene.
Solr 8.6.3	This is a generic term for searching for known vulnerabilities for the specific third-party library. Version used to filter initial results to only relevant items. VMware customized this library but is based on Apache SOLR.

Keyword	Description
Erlang 22.3.4.12	This is a generic term for searching for known vulnerabilities for the specific third-party library. Version used to filter initial results to only relevant items.
Google protobuf 3.15.6	This is a generic term for searching for known vulnerabilities for the specific third-party library. Version used to filter initial results to only relevant items.
Jetty 9.4.42	This is a generic term for searching for known vulnerabilities for the specific third-party library. Version used to filter initial results to only relevant items.
OpenResty 1.19.3.2	This is a generic term for searching for known vulnerabilities for the specific third-party library. Version used to filter initial results to only relevant items. This additionally covers looking for vulnerabilities in the 2 dependencies of openresty: openresty-zlib and openresty-pcre that would be displayed as part of the openresty keyword search results.
PostgreSQL 10.17	This is a generic term for searching for known vulnerabilities for the specific third-party library. Version used to filter initial results to only relevant items.
Python 3.9.5	This is a generic term for searching for known vulnerabilities for the specific third-party library. Version used to filter initial results to only relevant items.
RabbitMq 3.7.28	This is a generic term for searching for known vulnerabilities for the specific third-party library. Version used to filter initial results to only relevant items.
Redis 6.0.13	This is a generic term for searching for known vulnerabilities for the specific third-party library. Version used to filter initial results to only relevant items. This additionally covers looking for vulnerabilities in the redis: jemalloc dependency which are displayed with Redis keyword search results.
openjdk-11 11.0.11.0.9	This is a generic term for searching for known vulnerabilities for the specific third-party library. Version used to filter initial results to only relevant items. Shipped with product in case OS has not been updated.
Tzdata-java 2020a-1 –	This is a generic term for searching for known vulnerabilities for the specific third-party library. Version used to filter initial results to only relevant items. This is an openjdk dependency that is additionally shipped.

Table 4 - Keyword Vulnerability Analysis

NOTE: As a result of VMware Carbon Black's normal vulnerability monitoring process and the lab's public search for vulnerabilities, several of the third-party libraries were updated during the course of the evaluation. The final third-party package versions are what is identified in the keyword table above.

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources (updated July 27, 2021). The following public vulnerability sources were searched:

- Common Vulnerabilities and Exposures: https://www.cvedetails.com/vulnerability-search.php
- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- US-CERT: http://www.kb.cert.org/vuls/html/search
- SecurITeam Exploit Search: www.securiteam.com
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities
- Security Focus: http://www.securityfocus.com/vulnerabilities/

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration. Testing that was conducted under the functional testing that would have been duplication of a vulnerability tests were not re-run. This left one remaining exploit to further explore: malicious binary.

- Virus Scan – This test scans the TOE binaries with a virus scanner using the most current virus definitions against the application files and then the evaluator verifies that no files are flagged as malicious.

- Web Interface Vulnerability Identification (Burp Suite) – This test scans web pages to identify possible vulnerabilities with the desired tool that is specifically designed to identify OWASP vulnerabilities.

- Port Scanning – This test scans the TOE host to identify any open ports and attempt to enumerate running services information.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC Version 3.1 Rev 5 and CEM Version 3.1 Rev 5. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the APP_PP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the VMware Carbon Black EDR Server 7.5 product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the APP_PP in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the APP_PP related to the examination of the information contained in the TOE Summary Specification.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the APP_PP related to the examination of the information contained in the operational guidance documents.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit and the extended assurance requirement ALC_TSU_EXT.1 defined in the APP_PP. The evaluation team found that the TOE was identified and a method of timely updates was described.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the APP_PP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and validated that the vendor fixed all findings with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the APP_PP were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s test activities also demonstrated the accuracy of the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 Supplemental Administrative Guidance for Common Criteria Version 1.1, July 27, 2021* document.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation such as its ability to collect information from its host. All other functionality provided by the product needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 Security Target v1.1,* dated July 27, 2021.

13 List of Acronyms

Acronym	Definition
API	Application Programming Interface
CA	Certificate Authority
CB	Carbon Black
CC	Common Criteria
CLI	Command Line Interface
HTTPS	Hyper Text Transfer Protocol Secure
IT	Information Technology
NIAP	National Information Assurance Partnership
OS	Operating System
PII	Personally Identifiable Information
PP	Protection Profile
DRBG	Deterministic Random Bit Generator
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function

Table 5 – Acronym Definition

14 Terminology

Term	Definition
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.

Table 6 - Customer Specific Terminology

Term	Definition
Application (app)	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. The terms *TOE* and *application* are interchangeable in this document.
Application Programming Interface (API)	A specification of routines, data structures, object classes, and variables that allows an application to make use of services provided by another software component, such as a library. APIs are often provided for a set of libraries included with the platform.
Credential	Data that establishes the identity of a user, e.g. a cryptographic key or password.
Developer	An entity that writes application software. For the purposes of this document, vendors and developers are the same.
Operating System (OS)	Software that manages hardware resources and provides services for applications.
Personally Identifiable Information (PII)	Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.
Platform	The environment in which application software runs. The platform can be an operating system, hardware environment, a software based execution environment, or some combination of these. These types platforms may also run atop other platforms.

Security Administrator	An authorized administrator role that is authorized to manage the TOE and its data.
Sensitive Data	Sensitive data may include all user or enterprise data or may be specific application data such as emails, messaging, documents, calendar items, and contacts. Sensitive data must minimally include PII, credentials, and keys. Sensitive data shall be identified in the application's TSS by the ST author.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application an Authorized Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to manage TOE functions or data.
Vendor	An entity that sells application software. For purposes of this document, vendors and developers are the same. Vendors are responsible for maintaining and updating application software.

Table 7 - CC Specific Terminology

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Protection Profile for Application Software Version 1.3.
6. VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 Security Target v1.1, dated July 27, 2021.
7. VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5 Supplemental Administrative Guidance for Common Criteria, Version 1.1, dated July 27, 2021.
8. Assurance Activity Report for a Target of Evaluation “VMware Carbon Black Endpoint Detection and Response (EDR) Server 7.5” Assurance Activities Report v1.1, dated July 27, 2021.
9. VMware Carbon Black EDR User Guide VMWare Carbon Black EDR 7.5.