

National Information Assurance Partnership



Common Criteria Evaluation and Validation Scheme Validation Report

VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2

Report Number: CCEVS-VR-VID11155-2021

Version 1.0

July 28, 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

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

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

1	EXECUTIVE SUMMARY	5
2	IDENTIFICATION	7
3	ASSUMPTIONS AND CLARIFICATION OF SCOPE	8
3.1	ASSUMPTIONS	8
3.2	THREATS	8
3.3	CLARIFICATION OF SCOPE	8
4	ARCHITECTURAL INFORMATION	9
4.1	TOE INTRODUCTION	9
4.2	PHYSICAL BOUNDARY	9
5	SECURITY POLICY	11
5.1	CRYPTOGRAPHIC SUPPORT	11
5.2	USER DATA PROTECTION	11
5.3	IDENTIFICATION AND AUTHENTICATION	11
5.4	SECURITY MANAGEMENT	11
5.5	PRIVACY	11
5.6	PROTECTION OF THE TSF	11
5.7	TRUSTED PATH/CHANNELS	11
6	DOCUMENTATION	12
7	EVALUATED CONFIGURATION	13
8	IT PRODUCT TESTING	14
8.1	DEVELOPER TESTING	14
8.2	EVALUATION TEAM INDEPENDENT TESTING	14
8.3	EVALUATION TEAM VULNERABILITY TESTING	14
9	RESULTS OF THE EVALUATION	16
9.1	EVALUATION OF THE SECURITY TARGET (ASE)	16
9.2	EVALUATION OF THE DEVELOPMENT (ADV)	16
9.3	EVALUATION OF THE GUIDANCE DOCUMENTS (AGD)	16
9.4	EVALUATION OF THE LIFE CYCLE SUPPORT ACTIVITIES (ALC)	16
9.5	EVALUATION OF THE TEST DOCUMENTATION AND THE TEST ACTIVITY (ATE)	17
9.6	VULNERABILITY ASSESSMENT ACTIVITY (VAN)	17
9.7	SUMMARY OF EVALUATION RESULTS	17
10	VALIDATOR COMMENTS	18
11	ANNEXES	19
12	SECURITY TARGET	20
13	LIST OF ACRONYMS	21
14	TERMINOLOGY	22
15	BIBLIOGRAPHY	24

List of Tables

Table 1– Evaluation Identifiers.....	7
Table 2 – IT Environment Components.....	9
Table 3 - Evaluated Components of the TOE.....	13
Table 4 - Keyword Vulnerability Analysis.....	15

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

Table 5 – Acronym Definition	21
Table 6 - Customer Specific Terminology.....	22
Table 7 - CC Specific Terminology	23

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

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) Windows Sensor 7.2 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 July 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 (EDR) Windows Sensor 7.2 application, also referred to as the TOE from this point forward. The VMware CB EDR Windows Sensor is an enterprise software application whose primary purpose is to gather event data on the endpoints and invoke the OS to securely transmit this information to the operating environment's management server (VMware Carbon Black EDR Server) for centralized storage and indexing.

The TOE is installed on administratively defined network endpoints, such as laptops, desktops, and servers. The TOE, when installed, operates as a Windows service to perform its function of observing and reporting on system-level behavior. Changes to the TOE's data collection policy can only be initiated by the enterprise administrator using the management server in the operational environment. In the evaluated configuration, only the Windows Sensor application is inside the security boundary. The TOE operates on top of Microsoft Windows 10 and Windows Server 2019 OS with BitLocker (or equivalent) enabled.

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.

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

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.

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

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) Windows Sensor 7.2
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) Windows Sensor 7.2 Security Target v1.5 dated July 21, 2021
Evaluation Technical Report	Evaluation Technical Report For a Target of Evaluation “VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2” Evaluation Technical Report v1.3 dated July 21, 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 Windows Sensor 7.2 support for gathering event data on the endpoints and reporting it back to the operating environment’s VMware Carbon Black EDR Server (aka management server) for storage and indexing, described in Section 1.3 of the Security Target, were 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 type for VMware Carbon Black EDR Windows Sensor 7.2 is application software that is deployed on individual endpoint systems running the Windows operating system (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 application software that must be installed onto the platform it will operate on
- the TOE executes on a hardware platform that is running Windows 10 or Windows 2019 server
- the TOE is not accountable for security functionality provided by the platform layers.

4.2 Physical Boundary

VMware Carbon Black EDR Windows Sensor 7.2 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
Endpoint system with Microsoft Windows 10 (Windows)	The host platform along with the operating system installed that the TOE application is installed on.**
Management Server platform with the VMware CB EDR Server* software installed *evaluated independently	The management server is used in the evaluated configuration to deploy the TOE, collect the system data from these sensors, perform configuration updates, and deploy software updates. However, it is used to the extent that it can assist in the evaluation of the TOE software and no security claims for its functionality are made in this evaluation.
Administration Workstation	Any general-purpose computer that is used by an enterprise administrator to operate the Management Server 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 TOE to validate TOE server certificate.

Table 2 – IT Environment Components

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

****NOTE:** It is expected that the TOE is operating on a Common Criteria certified operating system and platform based on the Microsoft Windows 10 and Server 2019 version 1903 (May 2019 Update) evaluation. The TOE software that is installed on the Windows based OS, is identical (installation, executables, functionality, and features) no matter which variation of the Windows 10 (May 2019 Update) is used. For testing, the TOE was installed and fully tested on the Windows 10 Enterprise 2019 variant.

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/TLS trusted communications, and sensitive data encryption storage. As an application on an operating system, the TOE interfaces with the operating system's key storage to securely store key data related to secure communications.

5.2 User Data Protection

The application restricts its access to the endpoint system's network connectivity resources. It also restricts its sensitive data access to system logs and memory dumps stored on the endpoint system. Network activity is restricted to periodic management server polling, aka sensor check-in. During the periodic polling, the Sensor transmits sensor collected endpoint system data to the management server, retrieves configuration settings/updates and TOE software updates (if available) from the management server.

5.3 Identification and Authentication

The TOE relies on the OS to validate X.509.3 certificates for HTTPS/TLS communication.

5.4 Security Management

During installation, the TOE is automatically configured to protect itself and its data from unauthorized access and implements the recommended Windows platform security mechanisms. The TOE application provides one CLI that provides the ability for an OS administrator to verify the application version. The TSF implements changes to its configuration received during the polling cycle from the management server.

5.5 Privacy

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

5.6 Protection of the TSF

The TOE is packaged as separate software that is installed on the platform and can be uninstalled/removed if needed. In the evaluated configuration, all updates are obtained from the management server. The digital signature of the update package is verified by the host platform prior to being installed. The TOE will only initiate an update when the management server has indicated, during the periodic polling cycle, there is an authorized update available. 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.

5.7 Trusted Path/Channels

The TOE invokes the OS platform to provide a trusted communication channel (HTTPS session over TLS v1.2) to the management server.

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

6 Documentation

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

- VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2 Supplemental Administrative Guidance for Common Criteria – v1.1, June 24, 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 Windows Sensor (TOE)	An application that is installed on a Windows platform, which collects event data from this host endpoint platform and invokes the OS to securely transmit this collected information back to the management server in the Operating Environment. The TOE maintains the configuration settings in the Windows registry and on the local file system. The TOE does not provide an interactive user interface for creating or storing data on the endpoint system.

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:

- Microsoft Windows 10 (Windows Sensor host)
- Management Server (VMware CB EDR Server)

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) Windows Sensor 7.2 Supplemental Administrative Guidance for Common Criteria Version 1.1, June 24, 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) Windows Sensor 7.2” Assurance Activities Report v1.3, July 21, 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
CarbonBlack	This is a generic term for searching for known vulnerabilities produced by the company as a whole. Company has been referred to as both CarbonBlack (one word) and Carbon Black (two words). This key word will also obtain any information on the full product name. The terms: EDR, EDR Sensor, CB Sensor, Response Sensor, Windows, and version number will be used as a further delimiter on any found responses.
Carbon Black	This is a generic term for searching for known vulnerabilities produced by the company as a whole. This key word will also obtain any information on the full product name. The terms: EDR, EDR Sensor, CB Sensor, Response Sensor, Windows, and version number will be used as a further delimiter on any found responses.

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

Keyword	Description
Endpoint Detection	TOE application software technology type. The use of Response will be used as a further delimiter on any found responses.
Google protobuf 2.6.1	Third-party library that is included in the installed TOE software in order to function. Version number used as further delimiter on any found responses.
zlib 1.2.11	Third-party library that is included in the installed TOE software in order to function. Version number used as further delimiter on any found responses.

Table 4 - Keyword Vulnerability Analysis

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources (updated July 21, 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.

The team tested the following areas:

- Virus Scan
This test scans the TOE binary 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.

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 Windows Sensor 7.2 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.

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

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.

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

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) Windows Sensor 7.2 Supplemental Administrative Guidance for Common Criteria Version 1.1, June 24, 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

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

12 Security Target

The security target for this product's evaluation is *VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2 Security Target v1.5*, dated July 21, 2021.

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

13 List of Acronyms

Acronym	Definition
ASLR	Address Space Layout Randomization
CA	Certificate Authority
CB	Carbon Black
CC	Common Criteria
CLI	Command Line Interface
DEP	Data Execution Prevention
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

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

14 Terminology

Term	Definition
Local Administrator	The Windows OS administrator who has system permissions to access sensitive data and perform management functionality on the endpoint system.
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 the Windows operating system that hosts the VMware Carbon Black EDR Windows Sensor (TOE).
Endpoint User	An individual who has access to the TOE but is not able to manage its behavior.
Sensor Group	Each sensor is associated with a sensor group that defines its configuration and security characteristics. A sensor group must contain at least one sensor and can contain many sensors. However, a single 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
Address Space Layout Randomization (ASLR)	An anti-exploitation feature which loads memory mappings into unpredictable locations. ASLR makes it more difficult for an attacker to redirect control to code that they have introduced into the address space of an application process.
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 <i>TOE</i> and <i>application</i> 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.
Data Execution Prevention (DEP)	An anti-exploitation feature of modern operating systems executing on modern computer hardware, which enforces a non-execute permission on pages of memory. DEP prevents pages of memory from containing both data and instructions, which makes it more difficult for an attacker to introduce and execute code.
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

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

	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

VALIDATION REPORT
VMware Carbon Black EDR Windows Sensor 7.2

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) Windows Sensor 7.2 Security Target v1.5, dated July 21, 2021.
7. VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2 Supplemental Administrative Guidance for Common Criteria, Version 1.1, dated June 24, 2021.
8. Assurance Activity Report for a Target of Evaluation “VMware Carbon Black Endpoint Detection and Response (EDR) Windows Sensor 7.2” Assurance Activities Report v1.3, dated July 21, 2021.
9. VMware Carbon Black EDR User Guide VMware Carbon Black EDR 7.5.