National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



TM

Validation Report

for the

Carbon Black
Endpoint Detection and Response
(EDR) System

Report Number: CCEVS-VR-VID11692-2026
Dated: October 14, 2026
Version: 1.0

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

Jenn Dotson
Sheldon Durrant
Randy Heimann
Lisa Mitchell
Clare Parran
Jaemond Reyes
Lori Sarem
Charles Schmidt
Joe Walton

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Kelvert Ballantyne
Evan Seiz

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 EXECUTIVE SUMMARY 4
2 IDENTIFICATION 5
3 ARCHITECTURAL INFORMATION 6
4 SECURITY POLICY 7
4.1.1 Security Audit 7
4.1.2 Cryptographic Support 7
4.1.3 User Data Protection 7
4.1.4 Host Agent 8
4.1.5 Identification and Authentication 8
4.1.6 Security Management 8
4.1.7 Privacy 8
4.1.8 Protection of the TSF 8
4.1.9 Trusted Path/Channel 8
5 ASSUMPTIONS AND CLARIFICATION OF SCOPE 9
6 DOCUMENTATION 10
7 IT PRODUCT TESTING 11
8 EVALUATED CONFIGURATION 12
9 RESULTS OF THE EVALUATION 13
10 VALIDATOR COMMENTS 17
11 ANNEXES 18
12 SECURITY TARGET 19
13 LIST OF ACRONYMS 20
14 TERMINOLOGY 21
15 BIBLIOGRAPHY 22

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Carbon Black Endpoint Detection and Response (EDR) System provided by Broadcom. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

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 October 2026. The information in this report is largely derived from the 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 Extended and meets the assurance requirements set forth in the *PP-Configuration for Application Software, Endpoint Detection and Response, and Host Agent*, Version 1.1, 2022-04-07 which includes the base-PP: *Protection Profile for Application Software*, version 1.4, 2021-10-07 [App_PP] with the *Protection Profile Module for Endpoint Detection and Response (EDR*), Version 1.0, 2020-10-23 [EDRMOD], and the *Protection Profile Module for Host Agent*, Version 1.0, 2020-10-23 [HAMOD].

The TOE is the Carbon Black Endpoint Detection and Response System, referred to as the EDR System or the TOE from this point forward. The EDR System's primary functionality is to continuously record and store endpoint activity data to aid in incident response and threat hunting activities. The minimum configuration for this evaluation is one Carbon Black Endpoint Detection and Response Server (EDR Server) and one Carbon Black Endpoint Detection and Response Windows Sensor (Host Sensor) installed on an endpoint. Additional Endpoint Systems with a Host Sensor application installed as part of the operational configuration does not affect the validity of the functional claims made within this document and the Common Criteria certification.

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, EDRMOD, and HAMOD. This VR 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 ETR 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, EDRMOD, and HAMOD Assurance Activities. The Validation team found that the evaluation showed that the product satisfies all of 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 ETR are consistent with the evidence produced.
The technical information included in this report was obtained from the *Carbon Black Endpoint Detection and Response (EDR) System Security Target*, Version 1.0, dated June 26, 2026, and analysis performed by the Validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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 Profiles 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.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Carbon Black Endpoint Detection and Response (EDR) System comprised of the Carbon Black EDR Server application software v7.9 and the Carbon Black EDR Windows Sensor application software v7.5
Protection Profile	- *PP-Configuration for Application Software, Endpoint Detection and Response, and Host Agent*, Version 1.1, 2022-10-07 which includes o Base-PP: *Protection Profile for Application Software*, version 1.4, 2021-10-07 [App_PP] o Module*: Protection Profile Module for Endpoint Detection and Response (EDR)*, Version 1.0, 2020-10-23 [EDRMOD] o Module: *Protection Profile Module for Host Agent*, Version 1.0, 2020-10-23 [HAMOD]
Security Target	*Carbon Black Endpoint Detection and Response (EDR) System Security Target*, Version 1.0, June 26, 2026
Evaluation Technical Report	*Evaluation Technical Report for a Target of Evaluation Carbon Black Endpoint Detection and Response (EDR) System*, Version 1.0, September 30, 2026
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor & Developer	Carbon Black by Broadcom
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	The MITRE Corporation

3 Architectural Information

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

3.1 TOE Introduction

The TOE is Carbon Black Endpoint Detection and Response (EDR) System consisting of the EDR Server v7.9 and EDR Windows Sensor v7.5. The Carbon Black EDR System consists of both the EDR Server residing on a Red Hat Enterprise Linux (RHEL) 8.6 OS and the EDR Windows Sensor residing on a Microsoft Windows 11 OS Pro Edition (22H2) OS.

3.2 Physical Boundary

This 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:

Table 1: Components of the Operational Environment

Component	Definition
Red Hat Enterprise Linux (RHEL) 8.6 Server	The host platform with the RHEL operating system environment that the EDR Server application is installed on.
Endpoint System with Microsoft Windows 11 Pro Edition (22H2)	The host platform along with the operating system installed that the Host Sensor application is installed on.
Administrative Workstation	Any general-purpose computer that is used by an 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 the server X.509v3 certificate from the EDR Server's platform.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Security Audit
2. Cryptographic Support
3. User Data Protection
4. Host Agent
5. Identification and Authentication
6. Security Management
7. Privacy
8. Protection of the TSF
9. Trusted Path/Channel

4.1.1 Security Audit

The EDR Server generates and displays alerts to authorized users when potentially unauthorized activity is detected on enrolled endpoints. The EDR Server collects data from the endpoint that the Host Sensor is installed on. Both the EDR Server and the Host Sensor contain mechanisms to generate audit data for a set of predefined events. The Host Sensor relies on Windows Event Logger to store audit events.

4.1.2 Cryptographic Support

The EDR Server invokes the underlying platform OS to perform all cryptographic services including establishing HTTPS sessions over TLSv1.2 trusted communications and hashing user password credentials for storage.

The Host Sensor invokes the underlying platform OS to perform all cryptographic services including establishing HTTPS/TLS trusted communications, and sensitive data encryption storage. As an application on an operating system, the Host Sensor interfaces with the operating system's key storage to securely store key data related to secure communications.

4.1.3 User Data Protection

The TOE application restricts its access to the EDR Server platform's and Host Sensor platform's network connectivity resources. The TOE also restricts the Host Sensor's sensitive data access to system logs and memory dumps stored on the Endpoint System. Network activity is restricted to establishing HTTPS/TLS connections for remote management via Web GUI to the EDR Server, and between the Host Sensor and EDR Server for reachability events. During the Host Sensor check-in reachability event, the EDR Server receives collected Endpoint System data from the Host Sensor as well as provides any configuration and software updates for the Host Sensors to pull. The EDR Server requires LUKS encrypted partitioning to protect local sensitive data storage.

4.1.4 Host Agent

Data collected on the Host Sensor is stored locally until it is forwarded to the EDR Server over a secure HTTPS/TLS channel during Host Sensor check-in reachability event. The Host Sensor interacts only with the EDR Server and no other ESM software. There is no sensor-to-sensor communication for deployments of the TOE that contain more than one Host Sensor.

4.1.5 Identification and Authentication

The EDR Server provides username/password-based authentication to support administrative access to the TOE's Web GUI. Authentication passwords defined by the Administrator are only accepted by the TOE if the password meets the minimum password requirements. The Host Sensor enforces the use of X.509v3 certificates to support the establishment of all HTTPS/TLS connections to the EDR Server.

4.1.6 Security Management

The TOE provides Administrators with the ability to manage the EDR Server and Host Sensor (through the EDR Server) through a Web GUI. Each component of the TOE uses its underlying platform's recommended methods for storing and setting configuration options. During installation, the Host Sensor is automatically configured to protect itself and its data from unauthorized access.

4.1.7 Privacy

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

4.1.8 Protection of the TSF

Each TOE component is packaged as separate software that is installed on the platform and can be uninstalled/removed if needed. All updates are downloaded and installed by the Administrator using the OS software package manager. All updates for the Host Sensor are obtained through the EDR Server. The digital signature of the update is verified by the EDR Server platform during installation. The TOE does not download, replace, or modify its own binary code. The Administrator can verify the software version of the TOE from the Web GUI. The EDR Server invokes the OS platform to operate as the server in the HTTPS/TLS v1.2 communication channel with the Host Sensor.

The TOE implements anti-exploitation features such as stack-based overflow protection. The TOE is compatible with security features provided by the OS and only uses documented APIs and libraries.

4.1.9 Trusted Path/Channel

The EDR Server invokes the OS platform to operate as the server in the HTTPS/TLS v1.2 communication channels with the web browser on the administrative workstation.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *Protection Profile for Application Software*, version 1.4, 2021-10-07 [App_PP]
- *Protection Profile Module for Endpoint Detection and Response (EDR)*, Version 1.0, 2020-10-23 [EDRMOD]
- *Protection Profile Module for Host Agent*, Version 1.0, 2020-10-23 [HAMOD]

That information has not been reproduced here and the App_PP/EDRMOD/HAMOD should be consulted if there is interest in that material.

5.2 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 App_PP/EDRMOD/HAMOD including all relevant NIAP Technical Decisions. A subset of the "selection-based" security requirements defined in the App_PP, EDRMOD, and HAMOD are claimed by the TOE and documented in the ST.
- 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 ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about their effectiveness. In particular, the EDR system's collection, storage, and analysis of host platform data described in Section 1.3 of the ST were not assessed as part of this evaluation. Further information of excluded functionality can be found in Section 8.2.

6 Documentation

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

- *Carbon Black Endpoint Detection and Response (EDR) System Supplemental Administrative Guidance for EDR Host Sensor v7.5*, Version 1.0, December 31, 2025
- *Carbon Black Endpoint Detection and Response (EDR) System Supplemental Administrative Guidance for EDR Server v7.9*, Version 1.0, December 31, 2025
- *Carbon Black EDR 7.9.0*, 20 February 2026
- *Carbon Black EDR Sensor Documentation*, 07 July 2026, (Covers 7.5.0 version)

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.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation team. It is derived from information contained in the proprietary *Carbon Black Endpoint Detection and Response (EDR) System Test Plan*, Version 1.0, July 7, 2025, and summarized in the *Assurance Activity Report for a Target of Evaluation Carbon Black Endpoint Detection and Response (EDR) System*, Version 1.0, September 30, 2026.

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the App_PP/EDRMOD/HAMOD including the tests associated with optional requirements. The AAR, in sections 4.1.1, lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

This section briefly identifies the evaluated configuration(s) and any excluded and out of scope functionality.

8.1 Evaluated Configuration

The evaluated configuration, as defined in the ST, is Carbon Black Endpoint Detection and Response (EDR) System consisting of the EDR Server v7.9.0 and EDR Windows Sensor v7.5.0. The Carbon Black EDR System consists of both the EDR Server residing on a Red Hat Enterprise Linux (RHEL) 8.6 OS and the EDR Windows Sensor residing on a Microsoft Windows 11 Pro Edition (22H2) OS .

8.2 Excluded Functionality

The following optional products, components, and/or applications can be integrated with the TOE but are not included in the evaluated configuration. They provide no added security-related functionality for the evaluated product. They are separated into three categories: not installed; installed but requires a separate license; and installed but not part of the TSF.

8.2.1 Not Installed

There are no optional components that are omitted from the installation process.

8.2.2 Installed but Requires a Separate License

There are no excluded components that are installed and require a separate license.

8.2.3 Installed Functionality Excluded from the Evaluation

The TOE only includes the functionalities that are satisfied by the Security Functional Requirements in the claimed Protection Profile. Therefore, the following are considered out of scope of the evaluated configuration because there are no SFRs in the PP that allow this functionality to be claimed:

- The EDR System includes a number of capabilities in support of its primary function, such as the collection, storage, and analysis of host platform data, that are outside the scope of the claimed Protection Profile.
- The EDR System supports having multiple EDR servers in a cluster/minion configuration where a host sensor can communicate with multiple EDR servers. This cluster/minion configuration, along with the communications between EDR servers is not part of the evaluated configuration. Each host sensor is only communicating with one EDR server and host sensors do not talk to other host sensors.

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 team determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the Evaluation team performed the Evaluation Activities specified in the App_PP, EDRMOD, and HAMOD documents.

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 Carbon Black Endpoint Detection Response (EDR) System product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the Evaluation team performed an assessment of the Evaluation Activities specified in the App_PP, EDRMOD, and HAMOD documents to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

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 Evaluation team performed the Evaluation Activities specified in the App_PP, EDRMOD, and HAMOD documents related to the examination of the information contained in the TOE Summary Specification.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

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 Evaluation team performed the Evaluation Activities specified in the App_PP, EDRMOD, and HAMOD documents related to the examination of the information contained in the operational guidance documents.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work units. The Evaluation team found that the TOE was identified.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

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, EDRMOD, and HAMOD documents and recorded the results in a Test Report, summarized in the ETR and sanitized for non-proprietary consumption in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence was provided by the Evaluation team to show that the evaluation activities addressed the test activities in the App_PP, EDRMOD, and HAMOD documents, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability for TOE related components.

The Evaluation team performed a public search against the following sources to ensure there are no publicly known and exploitable vulnerabilities in the TOE:

a) NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
b) Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
c) Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
d) Offensive Security Exploit Database: https://www.exploit-db.com/
e) KEV database: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

The search was performed on September 30, 2026 and included the following search terms:

- CarbonBlack
- Carbon Black
- Broadcom Carbon Black
- EDR Server
- Host Agent
- Endpoint Detection and Response

- temurin-17-jre 17.0.14 (Eclipse Adoptium).
- Erlang/OTP 26.2.5.15 (erlang-26.2.5.15-1.el8) Then reduced based on applicability to (RabbitMQ Erlang RPM) package"
- lm_sensors-libs
- libjemalloc
- CPython 3.10.19
- pycryptodome 3.21.0 - PyPI (all Crypto/*)
- cryptography 43.0.1 - PyPI
- cffi 1.15.0 - PyPI (bundles libffi)
- numpy 1.22.3 - PyPI (bundles OpenBLAS 0.3.18, libgfortran, libquadmath)
- gevent 24.2.1 - PyPI (bundles libev 4.33, libuv 1.44.2, c-ares (versions per gevent 24.2.1 wheel))
- greenlet 3.1.0
- bcrypt 3.2.0
- protobuf 3.19.6
- python-ldap 3.4.0
- psycopg2 2.9.3
- SQLAlchemy 1.3.24
- netifaces 0.11.0
- wrapt 1.13.3
- libselinux 2.8 (libselinux-cb-python) - Red Hat, rebuilt by Broadcom (selinux/*.so)
- zope.interface 5.4.0
- pyrsistent 0.18.0
- python-rapidjson 1.5
- regex 2021.11.10
- simplejson 3.17.6
- MarkupSafe 2.1.1
- msgspec 0.18.6
- psutil 5.9.0
- hiredis 2.0.0
- pypl coverage 6.2
- OpenResty 1.21.4.3 - Broadcom build (luajit, lualib, nginx module .so)
- PCRE 8.44 (openresty-pcre) - libpcre.so
- zlib 1.2.12 (openresty-zlib) - libz.so
- PostgreSQL 13.23

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation addressed the vulnerability analysis requirements in the App_PP, and that the conclusion reached by the Evaluation team was justified.

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.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team performed the Evaluation Activities in the App_PP,

EDRMOD, and HAMOD documents, and correctly verified that the product meets 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 *Carbon Black Endpoint Detection and Response (EDR) System Supplemental Administrative Guidance for EDR Host Sensor v7.5*, Version 1.0, December 31, *2025* and the *Carbon Black Endpoint Detection and Response (EDR) System Supplemental Administrative Guidance for EDR Server v7.9*, Version 1.0, December 31, 2025 documents. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the Security Target. It is important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. It is important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled.

Evaluation activities are strictly bound by the assurance activities described in the App_PP/EDRMOD/HAMOD and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment. Integrators are encouraged to understand and mitigate potential vulnerabilities that may become relevant if non-evaluated features or functionality is enabled.

Per NIAP/CCEVS Publication #6, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Carbon Black Endpoint Detection and Response (EDR) System Security Target*, Version 1.0, June 26, 2026.

13 List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CA	Certificate Authority
CAVP	Cryptographic Algorithm Verification Program
CC	Common Criteria
CLI	Command-Line Interface
cPP	collaborative Protection Profile
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSP	Content Security Policy
DRBG	Deterministic Random Bit Generator
FTP	File Transfer Protocol
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
I&A	Identity and Access
IDS	Intrusion Detection System
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OS	Operating System
PP	Protection Profile
RAM	Random Access Memory
RBG	Random Bit Generator
RNG	Random Number Generator
RU	Rack Unit
SCP	Secure Copy Protocol
SFR	Security Functional Requirement
SFTP	SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SPAN	Switched Port Analyzer
SSH	Secure Shell
ST	Security Target
SVR	Server
TAP	Test Access Port
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UART	Universal Asynchronous Receiver/Transmitter
UI	User Interface

14 Terminology

Term	Definition
Administrator or 'Admin'	A user who is assigned the 'Admin' role on the TOE and has the ability to manage the TSF. Synonymous with Security Administrator.
Credential	Data that establishes the identity of a user (e.g., a cryptographic key or password).
Operating System (OS)	Software that manages hardware resources and provides services for applications.
Platform	A 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. This TOE defines three separate user roles, but only the most privileged role (Admin) is authorized to manage the TOE's security functionality and is therefore considered to be the Security Administrator for the TOE.
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 a Security Administrator uses to manage it (SSH client, terminal client, etc.).
User	In a CC context, any individual who has the ability to access the TOE functions or data.

15 Bibliography

1. *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-001
2. *Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components*, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-002
3. *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components*, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-003
4. *Common Methodology for Information Technology Security Evaluation – Evaluation Methodology*, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-004
5. *Protection Profile for Application Software*, Version 1.4 [App_PP], 2021-10-07
6. *Protection Profile Module for Endpoint Detection and Response (EDR)*, Version 1.0, 2020-10-23 [EDRMOD]
7. *Protection Profile Module for Host Agent*, Version 1.0, 2020-10-23 [HAMOD]
8. *Carbon Black Endpoint Detection and Response (EDR) System Security Target*, Version 1.0, June 26, 2026 (ST)
9. *Carbon Black Endpoint Detection and Response (EDR) System Supplemental Administrative Guidance for EDR Host Sensor v7.5*, Version 1.0, December 31, 2025
10. *Carbon Black Endpoint Detection and Response (EDR) System Supplemental Administrative Guidance for EDR Server v7.9*, Version 1.0, December 31, 2025
11. *Carbon Black EDR 7.9.0*, 20 February 2026
12. *Carbon Black EDR Sensor Documentation*, 07 July 2026, (Covers 7.5.0 version)
13. *Evaluation Technical Report for a Target of Evaluation Carbon Black Endpoint Detection Response (EDR) System*, Version 1.0, 09/30/2026
14. *Assurance Activities Report for a Target of Evaluation Carbon Black Endpoint Detection Response (EDR) System*, Version 1.0, 07/28/2026
15. *Carbon Black Endpoint Detection and Response (EDR) System Test Plan*, Version 1.0, July 7, 2025
16. *Carbon Black Endpoint Detection and Response (EDR) System Vulnerability Analysis*, Version 1.0, September 30, 2025