National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

VMware Carbon Black App Control v8.8.2

Report Number: CCEVS-VR-VID11158-2022
Version 1.0
March 03 2022

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

Daniel Faigin
Jerome Myers
Swapna Katikaneni
Dale Schroeder
The Aerospace Corporation

Common Criteria Testing Laboratory

Herbert Markle
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of VMware Carbon Black App Control, provided by VMware Inc. 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.

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 March 2022. 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 Conformant and meets the assurance requirements set forth in the *Standard Protection Profile for Enterprise Security Management-Access Control, version 2.1* [ESM_AC_PP] and the *Standard Protection Profile for Enterprise Security Management-Policy Management, version 2.1* [ESM_PM_PP].

The Target of Evaluation (TOE) is VMware Carbon Black App Control v8.8.2. App Control is an Enterprise Security Management (ESM) product that provides host-based access control meaning it controls client user access to objects including files, processes, and system configuration settings on an endpoint system based on an enterprise-level access control policy. The TOE includes a policy management component that is used to configure the access control policies and an agent component which will enforce its policy to allow or prevent client users from performing read, modify, delete, execute, and other operations on objects.

The Target of Evaluation (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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the [ESM_AC_PP] and [ESM_PM_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 [ESM_AC_PP] and [ESM_PM_PP]. 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the VMware Carbon Black App Control v8.8.2 Security Target, Version 1.0, February 27, 2022, and analysis performed by the Validation Team.

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 that 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 Compliance 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 results 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	VMware Carbon Black App Control v8.8.2
Protection Profile	• Standard Protection Profile for Enterprise Security Management-Access Control, version 2.1 (ESM_AC_PP) • Standard Protection Profile for Enterprise Security Management-Policy Management, version 2.1 (ESM_PM_PP)
Security Target	VMware Carbon Black App Control v8.8.2 Security Target, v1.0, February 27, 2022
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "VMware Carbon Black App Control v8.8.2" Evaluation Technical Report v1.0 February 27, 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	VMware, Inc.
Developer	Booz Allen Hamilton, Laurel, Maryland
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Daniel Faigin, The Aerospace Corporation Jerome Myers, The Aerospace Corporation Swapna Katikaneni, The Aerospace Corporation Dale Schroeder, The Aerospace Corporation

3. Assumptions and Clarification of Scope

- **Assumptions**

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.
- There will be one or more competent individuals assigned to install, configure, and operate the TOE.
- The TOE will be able to establish connectivity to other ESM products in order to share security data.
- The TOE will receive reliable time data from the Operational Environment.
- The TOE will receive identity data from the Operational Environment.
- The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
- The TOE will receive policy data from the Operational Environment.

- **Threats**

The following lists the threats addressed by the TOE. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

- T.ADMIN_ERROR [PM] - An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- T.CONDTRADICT [PM] - A careless administrator may create a policy that contains contradictory rules for access control enforcement.
- T.DISABLE [AC] - A malicious user or careless user may suspend or terminate the TOE's operation, thus making it unable to enforce its access controls upon the environment or TOE-protected data.
- T.EAVES [AC, PM] - A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
- T.FALSIFY [AC] - A malicious user can falsify the TOE's identity, giving the Policy Management product false assurance that the TOE is enforcing a policy.
- T.FORGE [AC] - A malicious user may create a false policy and send it to the TOE to consume, adversely altering its behavior.
- T.FORGE [PM] - A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.
- T.MASK [AC, PM] - A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
- T.NOROUTE [AC] - A malicious or careless user may cause the TOE to lose connection to the source of its enforcement policies, adversely affecting access control behaviors.

- T.OFLOWS [AC] - A malicious user may attempt to provide incorrect policy data to the TOE in order to alter its access control policy enforcement behavior.
- T.UNAUTH [AC] - A malicious or careless user may access an object in the Operational Environment that causes disclosure of sensitive data or adversely affects the behavior of a system.
- T.UNAUTH [PM] - A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.
- T.WEAKIA [PM] - A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.
- T.WEAKPOL [PM] - A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.

- **Objectives**

The following identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

- O.ACCESSID [PM] - The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.
- O.AUDIT [PM] - The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
- O.AUTH [PM] - The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
- O.BANNER [PM] - The TOE will display an advisory warning regarding use of the TOE.
- O.CONSISTENT [PM] - The TSF will provide a mechanism to identify and rectify contradictory policy data.
- O.DATAPROT [AC] - The TOE will protect data from unauthorized modification by enforcing an access control policy produced by a Policy Management product.
- O.DISTRIB [PM] - The TOE will provide the ability to distribute policies to trusted IT products using secure channels.
- O.INTEGRITY [AC] - The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components.
- O.INTEGRITY [PM] - The TOE will contain the ability to assert the integrity of policy data.
- O.MAINTAIN [AC] - The TOE will be capable of maintaining access control policy enforcement if it is unable to communicate with the Policy Management product which provided it the policy.
- O.MANAGE [PM] - The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.
- O.MNGRID [AC] - The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.

- O.MONITOR [AC] - The TOE will monitor the behavior of itself for anomalous activity (e.g., provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users).
- O.OFLOWS [AC] - The TOE will be able to recognize and discard invalid or malicious input provided by users.
- O.POLICY [PM] - The TOE will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control.
- O.PROTCOMMS [AC,PM] - The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
- O.RESILIENT [AC] - If the TOE mediates actions performed by a user against resources on an operating system, the system administrator or user shall not be allowed to perform an operation in the Operational Environment that would disable or otherwise modify the behavior of the TOE.
- O.ROBUST [PM] - The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
- O.SELFID [AC] - The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.
- O.SELFID [PM] - The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.

- **Clarification of Scope**

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 Standard Protection Profile for Enterprise Security Management-Access Control, version 2.1 (ESM_AC_PP) and the Standard Protection Profile for Enterprise Security Management-Policy Management, version 2.1 (ESM_PM_PP)
- 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 objectives 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 Section 6 of the Security Target and their operation with respect to the TOE is described in Section 8 of the Security Target. Any other functionality provided by VMware Carbon Black App Control needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

- The evaluated configuration of the TOE is the VMware Carbon Black App Control v8.8.2 software product and not any earlier or later versions released or in process. The TOE includes all the code that enforces the policies identified (see Section 5).
- 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.

    - Server database encryption – The key used to encrypt the SQL Server database is protected by the OS; App Control has no role in this.
    - Firewall/IIS configuration – The console/server is installed on Microsoft IIS, which is assumed to be hardened in an appropriate manner for the customer's environment. Similar, Windows Defender or another firewall can be assumed to be in place to limit network exposure of the server. The TOE cannot exert any control over the configuration of the underlying server.
    - SAML - Support for SAML to facilitate single sign-on from another application in the organization's environment.
    - REST API - This is an alternate method of remote management using a custom build management program. This evaluation did not evaluate the REST API or a custom build management console.
    - Timed override to endpoint – The Console can be used to generate a one-time token that can be used to locally administer an endpoint for set period of time, known as timed override. This is provided for cases where an endpoint system must have new policy rules applied to it but it is currently deployed in a situation where a persistent connection to the server is not feasible (e.g., submarine or other location with sharply constrained bandwidth).
    - App Control Connector – Allows the integration of the App Control Server with one or more network security devices or services. Integration with other network security devices or services is not included in the evaluation boundary.
    - Unified Management – Centralized management of multiple App Control Servers. Multiple App Control Servers and centralized management are not included in the evaluation boundary.
    - MacOS Agent – Agents can be installed on MacOS endpoints; however, this was not included in the evaluation boundary.
    - Two-tier Deployment Architecture – The App Control Server and SQL Server Database could be installed on separate machines in the Two-tier Deployment Architecture. This was not part of the evaluation boundary. The evaluation boundary only includes both the App Control Server and SQL Server Database on the same machine.
    - Visibility and Disabled Modes – Policies have different Modes of operation that can be configured. To enforce the functionality described by the ST, all policies must be in Control Mode. Visibility Mode and Disabled Mode are not included within the evaluation.

- Rule Types – The product has multiple types of rules that can be generated by administrative users. The only rules covered by this evaluation are Custom Software Rules, Memory Rules, Registry Rules, and Rapid Configs. Rules of any other name are not included within the evaluation.
- The broad set of vendor documentation covers a large number of product features. However, only those features and capabilities discussed in the specific sections of the 'VMware Carbon Black App Control v8.8.2 Supplemental Administrative Guidance v1.0' document was evaluated as part of this evaluation. Product functionality discussed within the broader vendor documents and not directly referenced by the 'VMware Carbon Black App Control v8.8.2 Supplemental Administrative Guidance v1.0' document was not evaluated as part of this evaluation.

4. Architectural Information

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

- **TOE Introduction**

App Control (also referred to as the TOE) is an Enterprise Security Management (ESM) product that provides host-based access control meaning it controls client user access to objects including files, processes, and system configuration settings on an endpoint system based on an enterprise-level access control policy.

- **Physical Boundaries**

The physical boundary of the TOE includes the following App Control Server software and Agent software:

- The App Control Server and App Control Console are software version 8.8.2.
- The App Control Agent for Windows operating systems is software version 8.7.2.
- The App Control Agent for Linux operating systems is software version 8.7.6.

The TOE does not include the hardware or operating systems of the systems on which it is installed. It also does not include the third-party software that is required for the TOE to run.

The following table lists the TOE software components and the operating environment in the evaluated configuration.

TOE Component Definition	Operational Environment	
	Operating System	CPU
App Control Server and Console System	Microsoft Windows Server 2019 Datacenter (1809)	Intel Xeon Gold 6230 (Cascade Lake)
App Control Agent - Linux Endpoint System(s)	Red Hat Enterprise Linux 7.6	Intel E5-2620 v4 (Broadwell)
App Control Agent - Windows Endpoint System(s)	Windows 10 Professional (1903)	Intel Core i5-8365U (Whiskey Lake)

Table 4-1: Host Platform Environment Components

These Operational Environment components are expected to be patched to include the latest security fixes for each component.

Component	Definition
Active Directory (AD)	This is an enterprise authentication server. In the evaluated configuration, TOE administrative users can be authenticated against an AD user account. AD is also used for client user identity data on endpoint systems. For endpoint systems running Linux a LDAP client, which is part of the operational environment, is used to map local system account information to network accounts defined in AD (since it is not natively supported on the Linux platforms) o Examples of this include realmd or SSSD. o The TOE's Agent has no awareness of how the user is authenticated by the environment, it just knows the user's claimed identity on the system (e.g.,

Component	Definition
	username, UID)
Endpoint System(s)	Any general-purpose computer that has the TOE Agent software installed and that supports TLS/HTTPS communications. Supported operating systems for the evaluation include Windows and Linux. These operating systems provide all cryptography for the TOE Agents to communicate with the TOE's App Control Server. Users of the endpoint systems are considered 'client users'. 'Client users' are users that are considered the subjects to which the access control policies are applied and are not considered TOE users. Refer to Section 2.4.1 for these machines' specifications.
Management Workstation	Any general-purpose computer that is used by an administrative user to remotely manage the TOE via the Console. The management workstation requires a web browser which supports HTTPS (Google Chrome 36 or higher supported, recommend latest version) to access the Console.
SQL Server Database	The TOE requires a pre-installed instance of Microsoft SQL Server (2012 or higher supported, recommend latest version) on the same machine where App Control Server is installed. Microsoft SQL Server must be configured to use AES-256 encryption method. All TOE configuration data, audit data, and local user data is stored in the database.
Windows Server	A Windows Server that has the TOE App Control Server and App Control Console software installed. The SQL Server Database is also installed on this machine. The Windows Server supports TLS/HTTPS communications. The Windows operating system installed on this machine provides all cryptography required by the TOE's App Control Server and App Control Console components. Refer to Section 2.4.1 for this machine's specifications.

Table 4-2: IT Environment Components

5. Security Policy

Enterprise Security Management

The TOE provides the ability to define access control policies for consumption by Agents for enforcement. The TOE maintains security attributes that belong to an individual object as well as individual subjects. Through the TOE's Console interface, administrative users create policies and configuration lists of rules which define whether or not a subject is allowed or denied the ability to perform an operation on an object based upon the attributes defined within the rule applied to the authorization request. The Server is responsible for deploying the new policies and configuration lists to the Agents for enforcement. The Agents will immediately enforce any new policies and configuration lists it receives.

The Agents rely on their underlying operating system and its communication with an Active Directory for the identification of client user subjects and the operating system for the identification of process subjects. The Console requires identification and authentication of the TOE's administrative user which is accomplished via a local username/password mechanism or the AD server.

Security Audit

The Agent generates records of auditable events and either transmits the audit events to the Server over TLS provided by the TOE's underlying operating systems or stores the audit events in local audit logs. The Server generates audit records and stores them in local audit logs or an SQL Server Database that resides on the Server's host platform. Additionally, the Server will store all audit events received from the Agent in the SQL Server Database. The ability to select

the set of events to be audited can be configured by administrative users defining rules that require or do not require audit events to be generated. Generated audit data is stored in a manner that prevents unauthorized modification or deletion.

Communications

The TOE provides a mechanism that requires the Agent to send a proof of receipt to the Server upon receiving a policy or configuration list. This receipt contains information that relates to the hostname of the Agent's endpoint server and the policy name or configuration list version that was received. This feedback is then verified by the Server.

User Data Protection

The Agent enforces the access control policy received from the Server and the rules applicable to its policy from the configuration lists received from the Server. The TOE's access control Security Function Policy (SFP) defines whether or not a subject is allowed or denied the ability to perform an operation on an object based upon the attributes defined within the rule applied against the authorization request. Each Agent will process rules assigned to their policy in a hierarchical manner, ensuring the lowest numbered rule (i.e. highest ranked hierarchically) is always enforced. By default, the TOE also enforces a self-protection SFP on its Agent's binaries and configuration data.

Identification and Authentication

The TOE requires each administrative user to be successfully identified before allowing any TSF-mediated actions on behalf of that subject. The TOE binds administrative users to their assigned role for restrictive security management enforcement.

Security Management

The TOE's Server maintains the administrative user roles: Read-Only, Power User, Admin, and custom role. Each of these roles has varying levels of privileges which determine what management functions the administrative users are able to perform via the TOE's Console interface which is a web based GUI. Administrative users are able to manage the TOE's own security functions, administrative users, audit events, and the Access Control SFP to include modifying its default configuration.
The TOE has only a single role when the Server is managing one of its Agents called administrator. The Server assumes this role every time an Agent polls the Server and during this connection the Server will send policy and configuration list updates.

Protection of the TSF

The TOE preserves a secure state when an Agent is terminated by immediately restarting the Agent. Agents will maintain policy enforcement by enforcing the last policy received when it is unable to communicate with the Server and can be configured to enforce a different Enforcement Level when this occurs. The Agent relies on its operating system's implementation of TLS to discard traffic in case a replay is detected. The client users' and administrative users' credentials which are needed for TOE operation are stored hashed and encrypted. The TOE also prevents the reading of symmetric keys.

Resource Utilization

In the event of a communication outage between the TOE's Agent and Server, the Agent will enforce the last known policy and configuration list it consumed. Once communications are restored, the Agent will immediately query the Server for the most up-to-date policy and configuration list data, and immediately enforce them.

TOE Access

The TOE displays a customizable warning banner on the Console login page. The TOE will terminate inactive sessions to the Console after an administratively configured amount of time and allows administrative users to terminate their own Console sessions. The TOE also allows the creation of rules which will allow or deny client users the ability to login to endpoint systems.

Trusted Path/Channels

The TOE's evaluated configuration enforces secure communication using TLS and HTTPS from the Agent to the Server, the Server to Active Directory, and administrative users via web browser to Console. The TLS and HTTPS protocols are implemented by the underlying TOE components' operating systems.

6. Documentation

The vendor provides a standard set of guidance documents that covers the core functionality of the product. These documents were used during the evaluation of the TOE:

- VMware Carbon Black App Control v8.8.2 Supplemental Administrative Guidance v1.0, dated February 27, 2022
- Server Installation Guide VMware Carbon Black App Control 8.8, dated 8 December 2021
- Operating Environment Requirements VMware Carbon Black App Control 8.8, dated 8 December 2021
- SQL Server Configuration Guide VMware Carbon Black App Control 8.8, dated 8 December 2021
- VMware Carbon Black App Control User Guide Product Version 8.8, Document Version 1.0, dated 6 December 2021

These guidance documents contain the security-related guidance material for this evaluation and must be referenced to place the product within the Common Criteria evaluated configuration. The guidance documents are applicable for the version of App Control claimed by this evaluation.

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

7. Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is the VMware Carbon Black App Control 8.8.2 software installed upon a general-purpose server platform.

Section 4.2 describes the TOE's physical boundary 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:

- Web Browser used for remote administration of the TOE.
- Database for storage of configuration, operation and audit data for the TOE.
- Authentication Store provide enterprise authentication and user data.
- Underlying endpoint system for hosting the App Control Agent software is installed.
- Underlying Server on which the App Control Server software is installed.

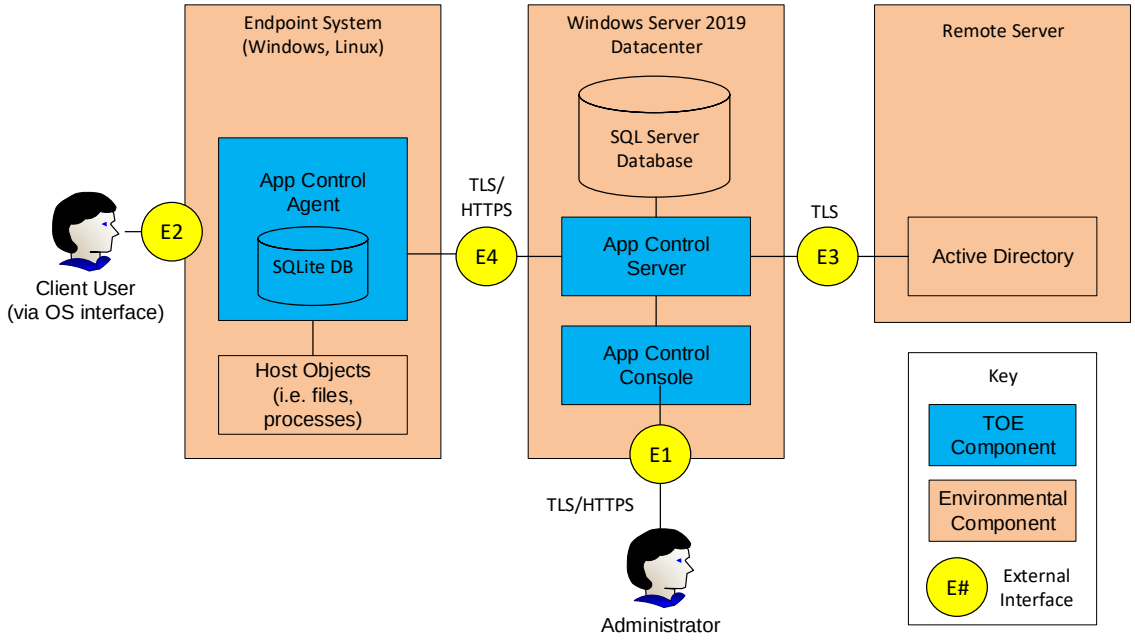
To use the product in the evaluated configuration, the product must be configured as specified in the *VMware Carbon Black App Control v8.8.2 Supplemental Administrative Guidance v1.0* document. Refer to Section 6 for the full list of documents needed for instructions on how to place the TOE in its evaluated configuration.

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 *Evaluation Technical Report for a Target of Evaluation "VMware Carbon Black App Control v8.8.2" Evaluation Technical Report v1.0 dated February 27, 2022*, which is not publically available.

- **Test Configuration**

The evaluation team installed and configured the TOE according to *VMware Carbon Black App Control v8.8.2 Supplemental Administrative Guidance v1.0* document for testing.



The TOE was installed on the following host operational environment.

TOE Component Definition	Host Operational Environment Operating System	CPU	
App Control Server and Console System	Microsoft Windows Server 2019 Datacenter (1809)	Intel Xeon Gold 6230 (Cascade Lake)	Server System SQL Database
App Control Agent - Linux Endpoint System(s)	Red Hat Enterprise Linux 7.6	Intel E5-2620 v4 (Broadwell)	Endpoint system
App Control Agent - Windows Endpoint System(s)	Windows 10 Professional (1903)	Intel Core i5-8365U (Whiskey Lake)	Endpoint system

The TOE was configured to communicate with the following external environment components:

- Windows 2019 Server Active Directory
- Management Workstation HP EliteBook Laptop with Windows 10

- Wireshark version 2.4.10
- Google Chrome version 76

- **Developer Testing**

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

- **Evaluation Team Independent Testing**

The test team's approach was to test the security mechanisms of the VMware Carbon Black App Control software by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. Each TOE external interface was described in the relevant design documentation (e.g., ST and AGD) in terms of the claims on the TOE that can be tested through the external interface.

The "VMware Carbon Black App Control v8.8.2 Security Target v1.0" (ST), "VMware Carbon Black App Control v8.8 Test Plan" were used to demonstrate test coverage of all SFR testing assurance activities as defined by the ESM_PM_PP and ESM_AC_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.

- **Evaluation Team Vulnerability Testing**

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The Evaluation Team conducted searches for public vulnerabilities related to the TOE. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

Keyword	Description
Carbon Black	This is a vendor specific term for searching for known vulnerabilities produced by the company, overall. *The term VMware is too broad and returns over 1300 findings. The term was refined to VMware Carbon Black which returned the same results as just Carbon Black.
Carbon Black App Control (8.8.2)	This is a vendor specific term for searching for known vulnerabilities for the specific product. This covers Server and Agents.
VMware App Control (8.8.2)	This is a vendor specific term for searching for known vulnerabilities for the specific product. This covers Server and Agents.

Keyword	Description
Host Based Access Control	This is a generic technology term for searching for known vulnerabilities for the specific technology.
Server/Console Libraries	**The following terms are libraries contained in the TOE server/console**
ASP.NET AJAX (2020.2.617.45 Telerik)	Name of library with applied version used to filter results.
BOOST (1.74)	Name of library with applied version used to filter results.
jQuery (3.5.1)	Name of library with applied version used to filter results.
jQuery_ui (1.13.0)	Name of library with applied version used to filter results.
nghttp2 (1.43)	Name of library with applied version used to filter results.
PHP (7.4.27)	Name of library with applied version used to filter results.
PEAR (1.10.12)	Name of library with applied version used to filter results.
SimpleSAML.php (1.18.7)	Name of library with applied version used to filter results.
Yara (4.1.1)	Name of library with applied version used to filter results.
Zlib (1.2.11)	Name of library with applied version used to filter results.
Agent Library	**The following terms are libraries contained in the TOE agents**
BOOST (1.69 Linux, 1.59 Windows)	Name of library with applied version used to filter results.
wxWidget (3.1.3 Linux, 3.0.2 Windows)	Name of library with applied version used to filter results.
Minizip (1.1-5 Linux)	Name of library with applied version used to filter results.
Zlib (1.2.11 Windows)	Name of library with applied version used to filter results.
7-zip (19.0 Windows)	Name of library with applied version used to filter results.
SQLite (3.35 Linux, 3.30.1 Windows)	Name of library with applied version used to filter results.

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources was updated on February 7, 2022. The following public vulnerability sources were searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- 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

All search activities were conducted prior to the execution of the vulnerability testing activities. 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.

The team tested the following areas:

- **Port Scanning**

Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test enumerates network port and service information to determine if any ports were open and running services outside of the TOE standard configuration.

- **Virus scan (ClamAV)**

The test is to ensure that there is no malicious code included in the software for any of the TOE's server or agent components.

- **Web Interface Vulnerability Identification (Burp Suite Pro)**

The test is to identify possibly vulnerabilities by scanning the web application with the desired tool that is specifically designed to identify OWASP vulnerabilities. The results provide an exploitability factor (easy, average, and difficult). Further testing is dependent on findings.

The TOE successfully prevented any attempts of subverting its security.

The results from the penetration testing showed that there were no vulnerabilities that could be leveraged by a malicious user when installed according to the *VMware Carbon Black App Control v8.8.2 Supplemental Administrative Guidance v1.0* [AGD]. There are currently no known discovered issues that could affect the security posture of a deployed system.

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 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Evaluation Activities specified in the [ESM_AC_PP] and [ESM_PM_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.

- **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 TOE that are 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 [ESM_AC_PP] and [ESM_PM_PP] in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validator 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.

- **Evaluation of the Development (ADV)**

The evaluation team applied each ADV CEM work unit specified in the [ESM_AC_PP] and [ESM_PM_PP]. 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.

The validator 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.

- **Evaluation of the Guidance Documents (AGD)**

The evaluation team applied each AGD CEM work unit specified in the [ESM_AC_PP] and [ESM_PM_PP]. 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 ICMPP related to the examination of the information contained in the operational guidance documents.

The validator 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.

- **Evaluation of the Life Cycle Support Activities (ALC)**

The evaluation team applied each ALC CEM work unit specified in the [ESM_AC_PP] and [ESM_PM_PP], as well as the Assurance Activities specified for ALC_CMC.1 and ALC_CMS.1. The evaluation team found that the TOE was identified.

The validator 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.

- **Evaluation of the Test Documentation and the Test Activity (ATE)**

The evaluation team applied each ATE CEM work unit specified in the [ESM_AC_PP] and [ESM_PM_PP]. The evaluation team ran the set of tests specified by the Assurance Activities in the ICMPP 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.

The validator 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 [ESM_AC_PP] and [ESM_PM_PP], and that the conclusion reached by the evaluation team was justified.

- **Vulnerability Assessment Activity (VAN)**

The evaluation team applied each AVA CEM work unit specified in the [ESM_AC_PP] and [ESM_PM_PP]. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator 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 Assurance Activities in the [ESM_AC_PP] and [ESM_PM_PP], and that the conclusion reached by the evaluation team was justified.

- **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 Assurance Activities in the [ESM_AC_PP] and [ESM_PM_PP], 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 *VMware Carbon Black App Control v8.8.2 Supplemental Administrative Guidance v1.0* document. No versions of the TOE and software, either earlier or later were evaluated.

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. All other functionality provided by devices in the operational environment need 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 App Control v8.8.2 Security Target, v1.0, February 27, 2022.

13. List of Acronyms

Acronym	Definition
AC	Access Control
AD	Active Directory
CC	Common Criteria
CL	Configuration List
CLI	Command-Line Interface
ESM	Enterprise Security Management
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IIS	Internet Information Services (Microsoft)
NIAP	National Information Assurance Partnership
OS	Operating System
PM	Policy Management
PP	Protection Profile
RBG	Random Bit Generator
SCM	Service Control Manager
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
ST	Security Target
TLS	Transport Layer Security
UI	User Interface

14. Terminology

Term	Definition
Access Control product	The TOE component related to the Security Functional Requirements defined in the Standard Protection Profile for Enterprise Security Management-Access Control, version 2.1. In terms of the TOE, this is the Agent component.
Admin	An administrative user who is assigned the 'Administrator' role on the TOE and has the ability to manage the TSF. An Admin using the Console is considered a TOE administrative user.
Administrative User	Administrative users access the TOE via the Console and are authorized to manage the TOE and its data. The TOE defines the out of the box administrative roles called Read-Only, Power User, and Admin but the TOE also allows the ability to create custom roles.
Client User	An endpoint system user that is considered to be the subject to which the access control policies are applied. Client users are not considered TOE users.
Configuration list	A hierarchal bundle of rules which is consumed by an Agent for making access control decisions.
Policy	The set of access control decisions which govern how the TOE will respond to an access request. In terms of the TOE, an Agent's policy and configuration list together determine the access control decisions for the TOE on that Agent's endpoint system.
Policy Management product	The TOE component related to the Security Functional Requirements defined in the Standard Protection Profile for Enterprise Security Management-Policy Management, version 2.1. In terms of the TOE, this is the Server and Console components.
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 administrative user uses to manage it (web browser, terminal client, etc.).
User or TOE 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, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. VMware Carbon Black App Control v8.8.2 Security Target, dated February 27, 2022
6. VMware Carbon Black App Control v8.8.2 Evaluation Technical Report v1.0 February 27, 2022
7. VMware Carbon Black App Control v8.8.2 Assurance Activities Report v1.0 February 27, 2022
8. VMware Carbon Black App Control v8.8.2 Test Procedures February 27, 2022
9. VMware Carbon Black App Control v8.8.2 Supplemental Administrative Guidance for Common Criteria, dated February 27, 2022
10. Server Installation Guide VMware Carbon Black App Control 8.8, dated 8 December 2021
11. Operating Environment Requirements VMware Carbon Black App Control 8.8, dated 8 December 2021
12. SQL Server Configuration Guide VMware Carbon Black App Control 8.8, dated 8 December 2021
13. VMware Carbon Black App Control User Guide Product Version 8.8, Document Version 1.0, dated 6 December 2021