National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Trellix Endpoint Security (HX) Agent, Version 35.31.31

Report Number: CCEVS-VR-VID11415-2024

Dated: 29 May 2024

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

Daniel Faigin: Senior Validator

Patrick Mallett: Lead Validator

Viet Hung Le: ECR Team

Common Criteria Testing Laboratory

Evaluator Listing

Ruban Abinesh

Akshay Jain

Jonathan Anglin

Fathi Nasraoui

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) 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 for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 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 evaluation of the Trellix Endpoint Security (HX) Agent Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in May 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 extended conformant and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for Protection Profile for Application Software, Version 1.4, October 7th, 2021, with Functional Package for Transport Layer Security Version 1.1, March 1st, 2019.

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. 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 Protection Profile for Application Software, Version 1.4, October 7th 2021 with Functional Package for Transport Layer Security Version 1.1, March 1st 2019. 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 are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). 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). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

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

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product 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(s) 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	Trellix Endpoint Security (HX) Agent
Protection Profile	Protection Profile for Application Software 1.4, 2021-10-07 with Functional Package for Transport Layer Security 1.1, 2019-03-01
Security Target	Trellix Endpoint Security (HX) Agent v35.31.31 Security Target version 2.3, May 21, 2024
Evaluation Technical Report	Evaluation Technical Report for Trellix Endpoint Security (HX) Agent v35.31.31, Version 0.8, May 29, 2024
CC Version	Version 3.1, Revision 5
Conformance Results	CC Part 2 Extended and CC Part 3 Extended Conformant
Sponsor	Trellix US LLC.
Developer	Trellix US LLC,
Common Criteria Testing Lab (CCTL)	Acumen Security Montgomery Village, MD
CCEVS Validators	Daniel Faigin: Senior Validator Patrick Mallett: Lead Validator Viet Hung Le: ECR Team

3 Architectural Information

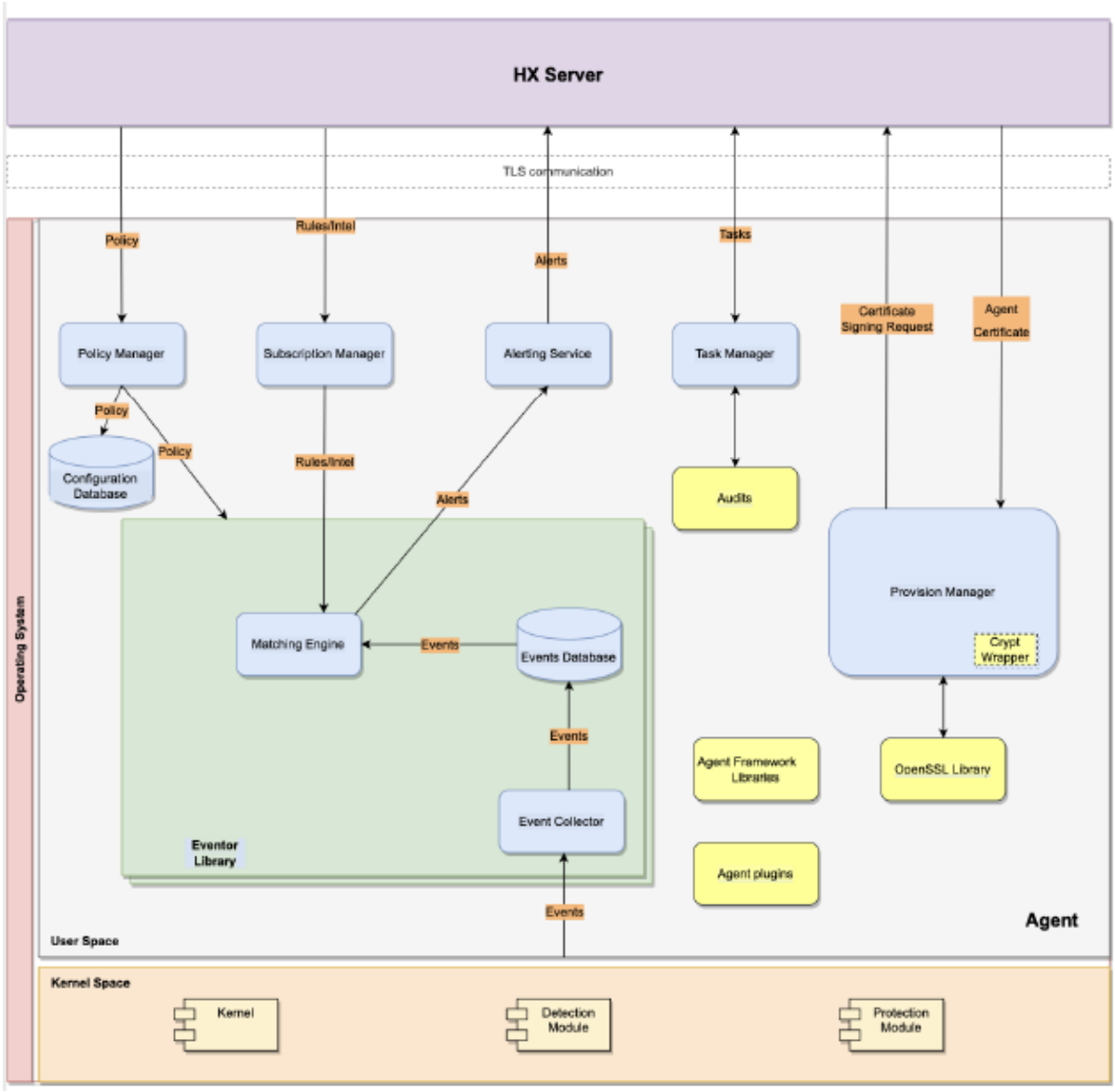
The TOE is the Trellix Endpoint Security (HX) Agent, Version 35.31.31 software application residing on a host platform and interacting exclusively with a Trellix Endpoint Security (HX) Series appliance. The TOE is an enterprise-managed agent that runs in the background of the host platform of an endpoint to provide protection against common malware as well as advanced attack. Based on a defense in depth model, the TOE uses a modular architecture with default engines and downloadable modules to protect, detect and respond to security events. There are no users interacting with the TOE or being informed of any communication between the TOE and the HX Series appliance.

3.1 TOE Description

This section provides an overview of the TOE, including physical boundary, the security functions implemented by the TOE, and any relevant TOE documentation and references.

A representative deployment of the TOE is illustrated in **Error! Reference source not found.**. TOE is a software agent executing on a host platform and interacting with the Trellix Endpoint Security (HX) Server. The TOE operates predominantly in the user space with the exception of some event sources requiring interaction with the kernel space of the host platform. The communication between the TOE and the HX Series Appliance (i.e., HX Server) is protected with TLS.

Figure 1: TOE Structure and Deployment



4 Security Policy

4.1.1 Security Functions Provided by the TOE

The TOE implements all security functions and mechanisms required for conformance with [PP_APP_v1.4] and [PKG_TLS_V1.1][1].

4.1.1.1 Cryptographic Support

The TOE implements cryptographic support for the following:

- TLS connectivity between itself and a Trellix Endpoint Security (HX) Series Appliance, including generation of 2048-bit RSA keys for a certificate signing request and implementation of all required cryptographic algorithms, and
- Digital certificate validation.

The cryptographic algorithms the TOE implements and the CAVP certificate numbers are given in Table 1. Each algorithm is implemented using the OpenSSL Cryptographic Library version 3.0.1 which is part of the TOE.

Table 1 TOE Cryptographic Algorithms and CAVP Certificate References

Algorithm	Standard	Mode/Key size	CAVP Cert. #
AES	FIPS 197, SP 800-38A	CBC 128, CBC 256	A5228
SHA	FIPS 180-4	SHA-1, SHA-256	A5228
RSA	FIPS 186-4, Appendix B.3	n = 2048 SHA-256	A5228
HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256	A5228
DRBG	SP 800-90A	CTR_DRBG(AES-256)	A5228

4.1.1.2 Identification and Authentication

The TOE uses X.509v3 certificates as defined by RFC 5280 to authenticate the TLS connection to the Trellix Endpoint Security (HX) Series appliance. The TOE validates the X.509 certificates using the certificate path validation algorithm defined in RFC 5280.

4.1.1.3 User Data Protection

The TOE is distributed as an installer package in Microsoft Installer (MSI) format. As well as the initial installation package, all updates to the TOE are also distributed as MSI packages. Each TOE installation and update package is digitally signed by Trellix in the production environment of the TOE. There are several methods to acquire the TOE's installation images. These include downloading them from the HX server, manually obtaining them from the vendor's cloud servers, or accessing them from the vendor's offline portal. Subsequent updates for the TOE can

either be distributed from the HX server or downloaded and installed manually on the host machine.

4.1.1.4 Privacy

The TOE does not transmit Personally Identifiable Information (PII) over the network. This protects the privacy of the users of the host platform.

4.1.1.5 Protection of the TSF

The TOE implements several security mechanisms to protect itself when installed on the host platform. Protection of the installation and update packages when stored on the Trellix Endpoint Security (HX) Series appliance or on the TOE is using digital signatures as described in Sect. 4.1.1.3.

The TOE never allocates memory with both write and execute permissions. Furthermore, the TOE operates in an environment in which the following security mechanisms are in effect:

- Data execution prevention,
- Mandatory address space layout randomization (no memory map to an explicit address),
- Structured exception handler overwrite protection,
- Export address table access filtering, and
- Anti-Return Oriented Programming.

Protection of the TOE and parts of it when stored within the production environment is not in the scope of the evaluation. Nevertheless, during compilation, the TOE is built with several flags enabled to check for engineering flaws. The flags and the protection mechanisms include the following:

- The TOE is built with the /GS flag enabled. This reduces the possibilities of stack-based buffer overflows in the product.
- The compiler enables Address Space Layout Randomization (ASLR) by default.
- The TOE is not built with the /DYNAMICBASE:NO which would disable ASLR.

4.1.1.6 Trusted Path/Channels

The TOE receives scanning policies from the associated Trellix Endpoint Security (HX) Series appliance over a network connection. The TOE uses the scanning policies for scanning the host platform and returns the results of the scanning to the appliance. The connection between the TOE and the Trellix Endpoint Security (HX) Series appliance is always secured with TLS. The TLS is implemented in full conformance with [PKG_TLS_V1.1].

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

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

5.2 Threats

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

ID	Threat
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes.

ID	Threat
	Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

5.3 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 Protection Profile for Application Software, Version 1.4, 2021-10-07.
- 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Trellix Endpoint Security (HX) Agent v35.31.31 Common Criteria Guidance Supplement, version 1.4, May 21, 2024.
- Endpoint Security xAgent Deployment Guide Release 35.31.0

Only the Administrator Guides listed above, and the specific sections of the other documents referenced by those guides should be trusted for the installation, administration, and use of this product in its evaluated configuration."

7 Conformance Claims

This section identifies the TOE conformance claims, conformance rationale, and relevant Technical Decisions (TDs).

7.1 CC Conformance Claims

The ST and the TOE are Common Criteria conformant to the following:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017,
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017, and
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision 5, April 2017.

This ST is Common Criteria Part 2 Extended conformant and Common Criteria Part 3 extended conformant.

This ST is package-conformant to the following package: [PKG_TLS_V1.1] Functional Package for Transport Layer Security, Version 1.1, March 1, 2019.

The TOE implements all security functions and mechanisms required for conformance with [PP_APP_v1.4] and [PKG_TLS_V1.1].

7.2 Protection Profile Conformance

This ST also claims exact conformation to the following protection profile:

[PP_APP_v1.4] Protection Profile for Application Software, Version 1.4, 2021-10-07

7.3 Conformance Rationale

This ST claims exact conformance to [PP_APP_v1.4] and [PKG_TLS_V1.1]. The security problem definition and the statement of security objectives are taken from them unmodified.

The statement of security requirements is taken from [PP_APP_v1.4] and [PKG_TLS_V1.1]. Only operations permitted therein are implemented. Selection-based and optional requirements (if any) are in conformance with [PP_APP_v1.4] and [PKG_TLS_V1.1].

7.3.1 Technical Decisions

All NIAP Technical Decisions (TDs) issued to date and applicable to [PP_APP_v1.4] and [PKG_TLS_V1.1] have been considered. Table 1 identifies all applicable TDs and states their applicability to the ST. Any exclusion is justified in the exclusion rationale.

Table 1 – Relevant Technical Decisions applicable to the ST

Technical Decision	Applicable	Exclusion Rationale (where applicable)
PP_APP_v1.4: Active Related Technical Decisions		
0823 – Update to Microsoft Windows Exploit Protection link in FPT_AEX_EXT.1.3	Yes	
0822 – Correction to Windows Manifest File for FDP_DEC_EXT.1	Yes	
TD0815: Addition of Conditional TSS Activity for FPT_AEX_EXT.1.5	Yes	
TD0798: Static Memory Mapping Exceptions	Yes	
TD0780: FIA_X509_EXT.1 Test 4 Clarification	Yes	
T**D**0756 – Update for platform-provided full disk encryption	Yes	
TD0747: Configuration Storage Option for Android	No	TOE is based on Windows platform
TD0743: FTP_DIT_EXT.1.1 Selection exclusivity	Yes	
TD0736: Number of elements for iterations of FCS_HTTPS_EXT.1	No	Toe does not claim FCS_HTTPS_EXT.1/Server
TD0719: ECD for PP APP V1.3 and 1.4	Yes	
TD0717: Format changes for PP_APP_V1.4	Yes	
TD0664: Testing activity for FPT_TUD_EXT.2.2	Yes	
TD0650: Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	No	ST does not claim PP-Module for VPN Clients, Version 2.4
TD0628: Addition of Container Image to Package Format	Yes	
PKG_TLS_v1.1: Active Related Technical Decisions		
TD0779: Updated Session Resumption Support in TLS package V1.1	No	ST does not claim TLS server
TD0770: TLSS.2 connection with no client cert	No	ST does not claim TLS server

Technical Decision	Applicable	Exclusion Rationale (where applicable)
PP_APP_v1.4: Active Related Technical Decisions		
0823 – Update to Microsoft Windows Exploit Protection link in FPT_AEX_EXT.1.3	Yes	
0822 – Correction to Windows Manifest File for FDP_DEC_EXT.1	Yes	
TD0815: Addition of Conditional TSS Activity for FPT_AEX_EXT.1.5	Yes	
TD0798: Static Memory Mapping Exceptions	Yes	
TD0780: FIA_X509_EXT.1 Test 4 Clarification	Yes	
T**D**0756 – Update for platform-provided full disk encryption	Yes	
TD0747: Configuration Storage Option for Android	No	TOE is based on Windows platform
TD0743: FTP_DIT_EXT.1.1 Selection exclusivity	Yes	
TD0736: Number of elements for iterations of FCS_HTTPS_EXT.1	No	Toe does not claim FCS_HTTPS_EXT.1/Server
TD0719: ECD for PP APP V1.3 and 1.4	Yes	
TD0717: Format changes for PP_APP_V1.4	Yes	
TD0739: PKG_TLS_V1.1 has 2 different publication dates	No	ST does not claim TLS server
TD0726: Corrections to (D)TLSS SFRs in TLS 1.1 FP	No	ST does not claim TLS server
TD0513: CA Certificate loading	Yes	
TD0499: Testing with pinned certificates	Yes	
TD0469: Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1	No	The TOE does not implement TLS Server
TD0442: Updated TLS Ciphersuites for TLS Package	Yes	

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration consists of the software application: Trellix Endpoint Security (HX) Agent, Version 35.31.31 when configured in accordance with the documentation specified in section 6. The TOE is packaged with 32-bit libraries and some 64-bit versions of libraries, making the TOE platform-agnostic application software that can be executed on all the claimed TOE's platforms. When deployed, the TOE is pushed to the host platform from a Trellix Endpoint Security (HX) Series appliance. It installs natively as a kernel and user space application.

The TOE runs on the following Microsoft Windows Operating Systems which are running on VMware hypervisor 7.0 on an Intel Xeon E5-4620 V4 processor (Broadwell microarchitecture), which are the only allowed host platforms:

- Windows 10 Version 21H2 32-bits running on ESXi Hypervisor v7.0 on an Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 1803 32-bits running on ESXi Hypervisor v7.0 on an Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 1903 32-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 1909 LTSC 32-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 2004 32-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 21H2 64-bits running on ESXi Hypervisor v7.0 on an Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 1803 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 1903 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 1909 LTSC 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 10 Version 2004 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
- Windows 11 Version 21H2 64-bits running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).

– Windows Server 2016 running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
– Windows Server 2019 running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
– Windows Server 2012 R2 running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
– Windows Server 2008 R2 (SP1) running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).
– Windows Server 2022 running on ESXi Hypervisor v7.0 on Intel Xeon E5-4620 V4 processor (Broadwell).

8.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- SHA-1 is used only in the provisioning of the TOE, not in the digital signature and session authentication functions implemented by the TOE.
- The TOE only implements TLS as a sender.
- xAgent to HX server communication using fast-pooling check on TCP port 80.
- Real-Time Indicator Detection.
- Trellix Exploit Guard Protection.
- Malware Protection.
- The scanning functions, or the specifics of the scanning policies and how they are managed.

9 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 Test Report for the Trellix Endpoint Security (HX) Agent, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

9.1 Developer Testing

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

9.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for Application Software, Version 1.4, October 7th, 2021, with Functional Package for Transport Layer Security Version 1.1, March 1st, 2019.

All testing was carried out on the TOE running on Microsoft operating systems Windows Server 2012 R2, Windows Server 2019, Windows 10 32-bits, Windows 10 64-bits and Windows 11 hosted on a VMWare hypervisor v7.0 with Intel Xeon E5-4620 V4 processor (Broadwell), processor, at the Acumen Security office located at 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from June 2023 to April 2024.

The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was always kept in a secure repository.

The AAR, in section 4, lists the test tools, and has diagrams of the test environment. The Independent Testing activity is documented in Section 7.4 of the Assurance Activities Report, which is publicly available, and is not duplicated here.

10 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that 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 Trellix Endpoint Security (HX) Agent to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the PP_APP_v1.4 and PKG_TLS_V.1.1.

10.1 Evaluation of Security Target

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 Trellix Endpoint Security (HX) Agent that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the PP_APP_v1.4 and PKG_TLS_V1.1.

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.

10.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 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 Assurance Activities specified in the PP_APP_v1.4 and PKG_TLS_V1.1 related to the examination of the information contained in the 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.

10.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 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 Assurance Activities specified in the PP_APP_v1.4 and PKG_TLS_V1.1 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.

10.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. 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.

10.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the PP_APP_v1.4 and PKG_TLS_V1.1 and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities 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 PP_APP_v1.4 and PKG_TLS_V1.1, and that the conclusion reached by the evaluation team was justified.

10.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit and conducted a public search for vulnerabilities, as well as vulnerability testing, but did not uncover any issues with the TOE. In accordance with AVA_VAN.1, the evaluator scrutinized publicly available information sources to detect potential vulnerabilities in the TOE. The sources examined include:

a. https://nvd.nist.gov/vuln/search

b. https://www.cvedetails.com/vulnerability-search.php

The evaluator conducted public domain vulnerability searches through keyword searches, utilizing terms derived from the vendor's name, product name, and key platform features. As a result, the evaluator performed searches using the following keywords:

:

- Trellix
- fireeye
- Libuv
- Openssl version 3.0.8
- fips.dll
- legacy.dll
- libcrypto-3-64.dll
- libcrypto-3.dll
- libssl-3-64.dll
- libssl-3.dll
- zlib 1.2.13
- CryptAcquireContextW, CryptGenRandom, CryptReleaseContext, CryptProtectData, CryptUnprotectData
- vcruntime140.dll, vccorlib140.dll, msvcp140.dll, concrt140.dll, ucrtbase.dll, api-ms-win-core-console-l1-1-0.dll, api-ms-win-core-console-l1-2-0.dll, api-ms-win-core-datetime-l1-1-0.dll, api-ms-win-core-debug-l1-1-0.dll, api-ms-win-core-errorhandling-l1-1-0.dll, api-ms-win-core-fibers-l1-1-0.dll, api-ms-win-core-file-l1-1-0.dll, api-ms-win-core-file-l1-2-0.dll, api-ms-win-core-file-l2-1-0.dll, api-ms-win-core-handle-l1-1-0.dll, api-ms-win-core-heap-l1-1-0.dll, api-ms-win-core-interlocked-l1-1-0.dll, api-ms-win-core-libraryloader-l1-1-0.dll, api-ms-win-core-localization-l1-2-0.dll, api-ms-win-core-memory-l1-1-0.dll, api-ms-win-core-namedpipe-l1-1-0.dll, api-ms-win-core-processenvironment-l1-1-0.dll, api-ms-win-core-processthreads-l1-1-0.dll, api-ms-win-core-processthreads-l1-1-1.dll, api-ms-win-core-profile-l1-1-0.dll, api-ms-win-core-rtlsupport-l1-1-0.dll, api-ms-win-core-string-l1-1-0.dll, api-ms-win-core-synch-l1-1-0.dll, api-ms-win-core-synch-l1-2-0.dll, api-ms-win-core-sysinfo-l1-1-0.dll, api-ms-win-core-timezone-l1-1-0.dll, api-ms-win-core-util-l1-1-0.dll, api-ms-win-crt-conio-l1-1-0.dll, api-ms-win-crt-convert-l1-1-0.dll, api-ms-win-crt-environment-l1-1-0.dll, api-ms-win-crt-filesystem-l1-1-0.dll, api-ms-win-crt-heap-l1-1-0.dll, api-ms-win-crt-locale-l1-1-0.dll, api-ms-win-crt-math-l1-1-0.dll, api-ms-win-crt-multibyte-l1-1-0.dll, api-ms-win-crt-private-l1-1-0.dll, api-ms-win-crt-process-l1-1-0.dll, api-ms-win-crt-runtime-l1-1-0.dll, api-ms-win-crt-stdio-l1-1-0.dll, api-ms-win-crt-string-l1-1-0.dll, api-ms-win-crt-time-l1-1-0.dll, api-ms-win-crt-utility-l1-1-0.dll, msvcp140_1.dll, msvcp140_2.dll, msvcp140_atomic_wait.dll, msvcp140_codecvt_ids.dll, vcruntime140_1.dll

Two vulnerability searches were conducted: the first on March 20, 2024, and the second on May 29, 2024. No open vulnerabilities relevant to the TOE were found.

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 PP_APP_v1.4 and PKG_TLS_V1.1, and that the conclusion reached by the evaluation team was justified.

10.7 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 Assurance Activities in the PP_APP_v1.4 and PKG_TLS_V1.1, and correctly verified that the product meets the claims in the ST.

11 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Administrator Guides documents listed in Section 6. 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. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

Some administrative parameters in this system are modified through editing JSON configuration files. There is no real input validation for such files, and there is real risk of user error. Adjustments of parameters through JSON file editing should be only used when absolutely necessary (often as part of troubleshooting processes), and ideally under the guidance of vendor support representatives. Administrators should also double check both syntax and semantics of any change before saving the JSON file and directing the system to ingest the change.

12 Annexes

Not applicable.

13 Security Target

Trellix Endpoint Security (HX) Agent Security Target, version 2.2, May 21, 2024.

14 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

15 Bibliography

The Validation Team used the following documents to produce this Validation Report:

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 1.4, October 7th, 2021.
6. Functional Package for Transport Layer Security Version 1.1, March 1st, 2019.
7. Trellix Endpoint Security (HX) Agent Security Target, Version 2.2, May 21, 2024.
8. Trellix Endpoint Security (HX) Agent Common Criteria Supplement, Version 1.3