National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Symantec Endpoint Protection Client, Version 1.0

Report Number:	**CCEVS-VR-VID10926-2018**
Dated:	**December 10, 2018**
Version:	**0.1**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers: Senior Validator

Marybeth Panock: Lead Validator

Common Criteria Testing Laboratory

Tony Busciglio

Thibaut Marconnet

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 Symantec Endpoint Protection Client Series 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 November 2018. 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 Conformant, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for Protection Profile for Application Software, version 1.2, dated, 25 April 2016 [ASPP].

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 (CEM), 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 Protection Profile for Application Software, version 1.2, dated, 25 April 2016 [PP_APP_v1.2]. 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 result 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	Symantec Endpoint Protection Client
Protection Profile	Protection Profile for Application Software, version 1.2, dated, 25 April 2016 [PP_APP_v1.2]
Security Target	Symantec Endpoint Protection Security Target
Evaluation Technical Report	Symantec Endpoint Protection ETR
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Symantec Corporation
Developer	Symantec Corporation
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Jerome Myers: Senior Validator Marybeth Panock: Lead Validator

3 Architectural Information

The Symantec Endpoint Protection client (hereafter referred to as the TOE or SEP) is a multifaceted endpoint threat control agent blending features of traditional antivirus, HIDS, host-based firewalls, etc., into a single software package.

The SEP comprises a set of applications (.exe) and libraries (.dll), written in C++, running as native code on the operating system. It is composed of components which run in user space (the traditional "application"), as well as service providers which run in privileged mode in kernel space, essentially as drivers, to allow the software to control security-relevant functionality on the host operating system, such as blocking network traffic to malicious hosts, and shutting down host access to removable media.

The platform for this evaluation will be the Windows Operating System.

4 Security Policy

Cryptographic Support

The TOE leverages the Windows built-in TLS v1.2 implementation. When establishing a session over TLS, the Windows built-in TLS v1.2 ensures the identifier presented in the exchange matches the correct reference identifier before proceeding with the connection. The Windows built-in TLS v1.2 also performs validation of TLS server certificates. If for any reason during session establishment the validity of a certificate cannot be performed successfully, the Windows built-in TLS v1.2 will not accept the certificate or establish the session.

User Data Protection

In the evaluated configuration, the TOE does not store sensitive data on the drive. In addition, the TOE is restricted to use of only the underlying platforms network connectivity for client/server communications and content updates. These are triggered either by user action or via response to a SEP Manager request. While the TOE writes to the Windows event logs, it does not provide functionality to read the generated events.

Identification and Authentication

The TOE supports use of X.509 certificates for TLS communication between the TOE and SEP Manager. This is performed via the X509TrustManager.

Security Management

The TOE does not install with any default credentials and does not store any credentials on the system. The authentication mechanisms of the underlying platform are used to ensure only authorized users of that platform can gain access to the application and underlying platform functionality.

Configuration options are stored via native mechanisms (Windows Registry) and proprietary secure storage. Protection of these configuration options is provided using Access Control Lists (ACLs) and SymProtect (Symantec Tamper Protection). By default, the application is configured with file permissions which protect it and its data from unauthorized access

Privacy

In the evaluated configuration, the TOE does not transmit any Personally Identifiable Information (PII) over the network.

Protection of the TSF

In the evaluated configuration, the TOE does not request memory mapping to any explicit address. However, the TOE does request allocation of memory regions for write and execute permissions. This allocation is performed using PAGE_EXECUTE_READWRITE. It is important to note that the application does not provide the user with the ability to write modifiable files to directories containing executable files.

The TOE is compiled with use of the GS flag to provide protection against stack-based buffer overflow. This provides buffer security checks during compilation of code by checking for risks such as buffer overruns on return addresses and potentially vulnerable parameters.

For updates to the TOE, SEP client implements its own functionality (LiveUpdate) to check for updates which are distributed as MSI files on the Windows platform. TOE updates are digitally signed for image validation. Checking of the software version can be performed through the TOE's GUI as well as using the SWID tags provided with the application. Additional updates to the MSI include content updates and security updates which can be used to update the binary code to ensure up-to-date protection. If the application is uninstalled from the platform, all traces of the application will be purged from the platform.

For the TOE to function as defined within the protection profile, Windows Defender should be disabled on the underlying platform.

Trusted Path/Channels

During operation of the TOE, transmitted data is encrypted via HTTPS and TLSv1.2. TLS communication is provided via the Windows built-in TLS v1.2. LiveUpdate, the service used for transmission of security definitions, are sent via HTTPS.

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 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 within compliance of 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	Assumption
A.PLATFORM	The TOE relies upon a trustworthy computing platform 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 within compliance of the applied enterprise security policy.

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 1.2, dated, 25 April 2016 [ASPP].
- 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. In particular, this evaluation does not make any statements about the effectiveness of the actual Anti-Virus and Host-based Intrusion capabilities of the product.

6 Documentation

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

- [ST] Symantec Endpoint Protection Security Target, TOE Software Version 14.2
- [AGD] Symantec Endpoint Protection (SEP) Client, Version 14.2 Common Criteria Addendum
- [IAG] Symantec Endpoint Protection 14 Installation and Administration Guide

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

Hardware

The TOE is a software-only evaluation running on a Windows OS platform. The following minimum requirements are needed for the underlying platform to ensure the TOE functions as required, when configured in accordance with the documents identified in Section 6:

- Operating System
  - Windows 10
- Processor
  - 32-bit processor: 1 GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended)
  - 64-bit processor: 2 GHz Pentium 4 with x86-64 support or equivalent minimum
- Physical RAM
  - 512MB (1GB recommended)
- Hard Drive
  - 395 MB (Additional 135MB required during installation)

Software

The software boundary of the TOE incudes the Symantec Endpoint Protection Client application as well as the Graphical User Interface (GUI). For cryptographic operations, the TOE uses the Windows built-in TLS v1.2 implementation in support of HTTPS/TLS communications.

Operational Environment

In support of the TOE, the following components are present within the Operational Environment:

Component	Usage/Purpose
Symantec Endpoint Protection (SEP) Manager	SEP Manager maintains the authenticated user accounts and information regarding how it itself authenticates to databases. The SEPM provides management over the Endpoint client configuration.
LiveUpdate Server	LiveUpdate provides administrators a method in which to download definitions, signatures, and other content and distributes the updates to client computers. The connection is secured via TLS.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Symantec Endpoint Protection client, which is not publicly available. The Assurance Activities Report (AAR) provides an overview of testing and the prescribed assurance activities. Section 3 of the AAR, Test Infrastructure, provides the test configuration and the tools used.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

- The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for Application Software, version 1.2, dated, 25 April 2016 [ASPP].

The Independent Testing activity is documented in the Assurance Activities Report, which is publically available, and is not duplicated here.

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 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 4 and CEM version 3.1 rev 4. The evaluation determined the Symantec Endpoint Protection Client to be Part 2 extended, and meets the SARs contained in the PP.

9.1 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 Symantec Endpoint Protection Client 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_v1.2].

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.

9.2 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_v1.2] 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.

9.3 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_v1.2] 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.

9.4 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.

9.5 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_v1.2] 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_v1.2], and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. 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 [PP_APP_v1.2], 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 Assurance Activities in the [PP_APP_v1.2], and correctly verified that the product meets the claims in the ST.

10 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 Symantec Endpoint Protection (SEP) Client, Version 14.2 Common Criteria Addendum. 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 routers and switches network infrastructure, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

All of the Validators concerns are adequately addressed elsewhere in this document.

11 Annexes

Not applicable.

12 Security Target

[ST] Symantec Endpoint Protection, Version 14.2 Security Target, version 1.2, November 2018

13 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.

14 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 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. Symantec Endpoint Protection, Version 14.2 Security Target, version 1.2, November 2018
6. Common Criteria SWAPP Assurance Activity Report Symantec Endpoint Protection, Version 1.2, November 2018
7. Symantec Endpoint Protection (SEP) Client, Version 14.2 Common Criteria Addendum, Version 1.0
8. Symantec™ Endpoint Protection 14 Installation and Administration Guide Product Version 14 Documentation version: 2, November 07, 2016
9. Symantec Endpoint Protection (SEP) Evaluation Technical Report (TOE ETR), Version 1.2, November 2018 <Evaluation Sensitive>
10. Symantec Endpoint Protection Security Target Evaluation Technical Report Template (ASE ETR), Version 1.2, November 2018 <Evaluation Sensitive>
11. Vulnerability Assessment for Symantec Endpoint Protection, Version 1.0, September 2018
12. Test Plan for Symantec Endpoint Protection Client, Version 1.3, November 2018 <Evaluation Sensitive>