National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

FireEye X-Agent version 28.8.3

Report Number:	**CCEVS-VR-VID10957-2019**
Dated:	**July 29, 2019**
Version:	**1.0**

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

Daniel Faigin

Meredith Hennan

The Aerospace Corporation

Common Criteria Testing Laboratory

Kenji Yoshino

Thibaut Marconnet

Danielle F Canoles

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 FireEye X-Agent Application 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 July 2019. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test report, as summarized in the publicly available FireEye X-Agent Assurance Activity Report (AAR), 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 Protection Profile for Application Software, version 1.2, dated, 22 April 2016 [SWAPP] and applicable Technical Decisions. The following table identifies the Technical Decisions associated with the SWAPP Protection Profile at time of evaluation, whether they are applicable to the TOE in the evaluated configuration, and rationale for exclusion, if warranted:

Table 1 - Technical Decisions

Identifier	Applicable	Exclusion Rationale (if applicable)
0434 – Windows Desktop Applications Test	Yes	
0427 – Reliable Time Source	Yes	
0392 – FCS_TLSC_EXT.1.2 Wildcard Checking	Yes	
0390 – Cryptographically Secure RNG	Yes	
0389 – Handling of SSH EP claim for platform	Yes	
0385 – FTP_DIT_EXT.1 Assurance Activity Clarification	No	This TD applies to the VPN Client Module.
0382 – Configuration Storage Options for Apps	Yes	
0380 – Linux Keyring Requirement in FCS_STO_EXT.1	No	This TD applies to the Linux platform. The TOE operations on Windows platforms.

Identifier	Applicable	Exclusion Rationale (if applicable)
0364 – Android mmap testing for FPT_AEX_EXT.1.1	No	This TD applies to the Android platform. The TOE operations on Windows platforms.
0359 – Buffer Protection	Yes	
0358 – Cipher Suites for TLS in SWApp v1.2	Yes	
0327 – Default file permissions for FMT_CFG_EXT.1.2	Yes	
0326 – RSA-based key establishment schemes	Yes	
0305 – Handling of TLS connections with and without mutual authentication	No	The TOE does not claim conformance to FCS_TLSC_EXT.2
0304 – Update to FCS_TLSC_EXT.1.2	Yes	
0300 – Sensitive Data in FDP_DAR_EXT.1	Yes	
0296 – Update to FCS_HTTPS_EXT.1.3	No	The TOE does not claim conformance to FCS_HTTPS_EXT.1
0295 – Update to FPT_AEX_EXT.1.3 Assurance Activities	Yes	
0293 – Update to FCS_CKM.1(1)	No	This TD has been archived
0283 – Cipher Suites for TLS in SWApp v1.2	No	This TD has been archived
0269 – Update to FPT_AEX_EXT.1.3 Assurance Activity	No	This TD has been archived
0268 – FMT_MEC_EXT.1 Clarification	Yes	
0267 – TLSS testing - Empty Certificate Authorities list	No	The TOE does not claim conformance to FCS_TLSS_EXT.1
0244 – FCS_TLSC_EXT - TLS Client Curves Allowed	No	The TOE does not claim conformance to FCS_TLSC_EXT.4
0241 – Removal of Test 4.1 in FCS_TLSS_EXT.1.1	No	The TOE does not claim conformance to FCS_TLSS_EXT.1
0238 – User-modifiable files FPT_AEX_EXT.1.4	Yes	
0221 – FMT_SMF.1.1 - Assignments moved to Selections	No	This TD only applies to the SWFE EP.
0218 – Update to FPT_AEX_EXT.1.3 Assurance Activity	No	This TD has been archived
0217 – Compliance to RFC5759 and RFC5280 for using CRLs	Yes	
0215 – Update to FCS_HTTPS_EXT.1.2	No	The TOE does not claim conformance to FCS_HTTPS_EXT.1
0192 – Update to FCS_STO_EXT.1 Application Note	No	This TD has been archived
0178 – Integrity for installation tests in AppSW PP	Yes	
0177 – FCS_TLSS_EXT.1 Application Note Update	No	Superseded by TD0389
0174 – Optional Ciphersuites for TLS	Yes	

Identifier	Applicable	Exclusion Rationale (if applicable)
0172 – Additional APIs added to FCS_RBG_EXT.1.1	No	Replaced by TD0390
0163 – Update to FCS_TLSC_EXT.1.1 Test 5.4 and FCS_TLSS_EXT.1.1 Test	Yes	
0131 – Update to FCS_TLSS_EXT.1.1 Test 4.5	No	The TOE does not claim conformance to FCS_TLSS_EXT.1
0122 – FMT_SMF.1.1 Assignments moved to Selections	No	This TD has been archived
0121 – FMT_MEC_EXT.1.1 Configuration Options	No	This TD only applies to the SWFE EP.
0119 – FCS_STO_EXT.1.1 in PP_APP_v1.2	Yes	
0107 – FCS_CKM - ANSI X9.31-1998, Section 4.1.for Cryptographic Key Generation	No	Superseded by TD0326

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 Protection Profile for Application Software, version 1.2, dated, 22 April 2016 [SWAPP] and all applicable NIAP technical decisions for the technology. 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.

The target of evaluation is the FireEye X-Agent Application and the associated TOE guidance documentation.

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 2 - Identification

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	FireEye X-Agent Application version 28.8.3
Protection Profile	Protection Profile for Application Software, version 1.2, dated, 22 April 2016
Security Target	FireEye X-Agent Application Security Target, Version 1.8
Evaluation Technical Report	FireEye X-Agent SWAPP Assurance Activity Report, version 1.5
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor	FireEye, Inc.
Developer	FireEye, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security, LLC
CCEVS Validators	Daniel Faigin Meredith Hennan *The Aerospace Corporation*

3 Architectural Information

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

The TOE is a software agent that resides on a host platform. The software exclusively interacts with the NIAP validated FireEye HX Series Appliances (NIAP VID 10892). This interaction consists of the TOE receiving policies from an external HX series appliance (validated separately) and sending any alerts that are found as a result of these scans. This is done via polling. The TOE is an enterprise managed agent that runs in the background of an endpoint platform. It is intended that the user will have no interaction with the software and will not be alerted of communications with the external HX appliance.

The frequency at which the agent communicates with the HX appliance is set by the enterprise. By default, each agent polls the HX appliance every 600 seconds (10 minutes) to obtain information and task requests and polls the appliance every 30 minutes to obtain the latest indicators. When new policies are received, they are used to identify potential intrusions on the host platform.

3.1 Physical Boundaries

The TOE boundary is the application software which runs on the host platform. The software is pushed to the host platform from a FireEye HX series and installs natively as a kernel and user space application. The software runs on Microsoft Operating Systems. The following Operating Systems are included in this evaluation:

- Windows Server 2012R2 x64 running on an Intel Xeon E5 processor
- Windows Server 2008R2 (SP1) x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1507 x86 and x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1511 x86 and x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1607 x86 and x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1703 x86 and x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1709 x86 and x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1803 x86 and x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1809 x86 and x64 running on an Intel Xeon E5 processor
- Windows Server 2016 Version 1607 on an Intel Xeon E5 processor

4 Security Policy

The TOE is comprised of several security features, as identified below.

The TOE provides the security functionality required by [SWAPP].

4.1 Cryptographic Support

The TOE provides cryptographic support for the following features,

- TLS connectivity with the following entities:
  - HX Series Appliance (NIAP VID 10892)
- Digital certificate validation

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified below. Each of these algorithms are implemented as part of the OpenSSL Cryptographic Library.

Table 3 - CAVP Certificate References

Algorithm	Standard	Mode/Keysize	CAVP Cert. #
AES	FIPS 197 SP 800-38A	CBC 128, CBC 256	C779 (AES)
SHA	FIPS 180-4	SHA-1, SHA-256	C779 (SHS)
RSA	FIPS 186-4	n = 2048 SHA-256	C779 (RSA)
HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256	C779 (HMAC)
DRBG	SP 800-90A	CTR_DRBG(AES-256)	C779 (DRBG)

4.2 Identification and Authentication

The TOE uses X.509v3 certificates as defined by RFC 5280 to authentication the TLS connection to the HX Series appliance. The TOE validates the X.509 certificates using the certificate path validation algorithm defined in RFC 5280.

4.3 Secure Software Update

The TOE is distributed as a Microsoft .MSI file providing a consistent and reliable versioning. After initial installation, all updates to the X-Agent are distributed as .MSI. Each TOE installation and update is signed by FireEye and can only come from the HX Series appliance associated with the TOE.

4.4 Privacy

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

4.5 Protection of the TSF

The TOE employs several mechanisms to ensure that it is secure on the host platform. The TOE never allocates memory with both write and execute permission. The TOE is designed to operate in an environment in which the following security techniques 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. This allows the TOE to operate in an environment in which the Enhanced Mitigation Experience Toolkit is also running. During compilation the TOE is built with several flags enabled that check for engineering flaws. The TOE is built with the /GS flag enabled. This reduces the possibilities of stack-based buffer overflows in the product. The compiler enables ASLR by default. The TOE is not built with the /DYNAMICBASE:NO which would disable ASLR.

4.6 Trusted Path/Channels

The TOE receives scanning policies from the associated HX Series appliance over the network which it uses on the host platform. This connection is always secured using TLS.

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.

Table 4 – Assumptions

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 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.

Table 5 - Threats

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. 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 1.2, dated, 22 April 2016 [SWAPP], and performed by the evaluation team.
- 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 PP and applicable Technical Decisions. Any additional security related functional capabilities that may be included in the product were not covered by this evaluation.
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.

6 Documentation

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

- FireEye X-Agent Security Target, Version 1.8, July 2019 [ST]
- Common Criteria FireEye X-Endpoint Agent Addendum, Release 28 Revision 2 [AGD]

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.

To use the product in the evaluated configuration, the product must be configured as specified in the Common Criteria FireEye X-Endpoint Agent Addendum, Release 28 Revision 2.

Consumers are encouraged to download this guidance document from the NIAP website to ensure the device is configured using the same instructions used by the evaluation team.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration of the TOE is the FireEye X-Agent version 28.8.3 running on one of the following Operating Systems:

- Windows Server 2012R2 x64 running on an Intel Xeon E5 processor
- Windows Server 2008R2 (SP1) x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1507 x86 and x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1511 x86 and x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1607 x86 and x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1703 x86 and x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1709 x86 and x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1803 x86 and x64 running on an Intel Xeon E5 processor
- Windows 10 Version 1809 x86 and x64 running on an Intel Xeon E5 processor
- Windows Server 2016 Version 1607 on an Intel Xeon E5 processor

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 the FireEye X-Agent, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

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 purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the Protection Profile for Application Software, version 1.2, dated, 22 April 2016 [SWAPP] and applicable NIAP Technical Decisions referenced in section 1 of this VR.

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, 22 April 2016 [SWAPP]. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

8.3 Test Configuration

Multiple test beds were were constructed to exercise Application Software capabilities and claimed security functionality. Testbed configuration diagrams and descriptions can be found in Section 4 of the AAR.

8.3.1 Testbed Tools

The following tooling was used as part of the test activities:

- Windows Server 2016 x64
- Windows 10 x86
- FireEye HX v4.6
- Kali Linux 2018.4
- Acumen-TLSC
- OpenSSL
- TCPView
- ProcMon
- AccessCheck
- VMMap
- BinScope

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) and as summarized in the FireEye X-Agent Assurance Activity Report, Version 1.2. 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 FireEye X-Agent to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the [SWAPP].

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 FireEye X-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 Protection Profile for Application Software, version 1.2, dated, 22 April 2016 [SWAPP].

The validators 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 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 SWAPP related to the examination of the information contained in the TOE Summary Specification.

The validators 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 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 SWAPP related to the examination of the information contained in the operational guidance documents.

The validators 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 found that the TOE was identified. Additionally, the team verified that both the TOE and its supporting documentation are consistently reference the same version and use the same nomenclature. The evaluation team also verified that the vendor website identified the TOE version accurately.

The validators 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 ran the set of tests specified by the Assurance Activities in the SWAPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validators 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 SWAPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The following sources of public vulnerability information were searched on July 25, 2019:

- https://www.cvedetails.com/
- https://www.exploit-db.com/
- https://www.google.com/

The search terms used included:

- FireEye X-Agent 28.8.3
- xagt vulnerabilities
- OpenSSL 2.0.10
- FireEye Audits 11.12.39
- zlib 1.2.8

The validators 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 SWAPP, 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 SWAPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

All validator comments have been addressed in the Clarification of Scope section.

11 Annexes

Not applicable.

12 Security Target

Please see the FireEye X-Agent Security Target, Version 1.8 [ST].

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. Protection Profile for Application Software, version 1.2, dated, 22 April 2016 [SWAPP]
6. FireEye X-Agent Security Target, Version 1.8 [ST]
7. FireEye X-Agent Assurance Activity Report, Version 1.5 [AAR]
8. Common Criteria FireEye Endpoint Agent Addendum, Release 28 Revision 2 [AGD]
9. FireEye X-Agent SWAPP Evaluation Technical Report, Version 1.4, July 2019 [ETR]