National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Trellix Security Enterprise Security Manager v11.6.12

Report Number: CCEVS-VR-VID11470-2025

Dated: 03/18/2025

Version: 0.4

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

Jerome Myers

Meredith Martinez

The Aerospace Corporation

Farid Ahmed

Anne Gugel

Russell Fink

The Johns Hopkins Applied Physics Laboratory

Common Criteria Testing Laboratory

Siddhant Kasley

Snehal Gaonkar

Rahul Joshi

Joan Marshall

Intertek Acumen Security

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 Security Enterprise Security Manager Target of Evaluation v11.6.12 (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 Intertek Acumen Security in March 2025. 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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e].

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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e].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	Trellix Security Enterprise Security Manager v11.6.12
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e]
Security Target	Trellix Security Enterprise Security Manager Security Target
Evaluation Technical Report	Evaluation Technical Report for Trellix Security Enterprise Security Manager v1.8
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Trellix, Inc.
Developer	Trellix, Inc.
Common Criteria Testing Lab (CCTL)	Intertek Acumen Security Rockville, MD
CCEVS Validators	Jerome Myers Farid Ahmed Meredith Martinez Anne Gugel

	Russell Fink

3 Architectural Information

The Trellix Security Enterprise Security Manager v11.6.12 brings event, threat, and risk data together to provide strong security intelligence, rapid incident response, seamless log management, and extensible compliance reporting. The TOE is distributed amongst six devices as follows: Enterprise Security Manager (ESM), Event Receiver (ERC), Application Data Monitor (ADM), Advanced Correlation Engine (ACE), Enterprise Log Manager (ELM), and Enterprise Log Search (ELS). The six TOE components are divided into three categories as follows:

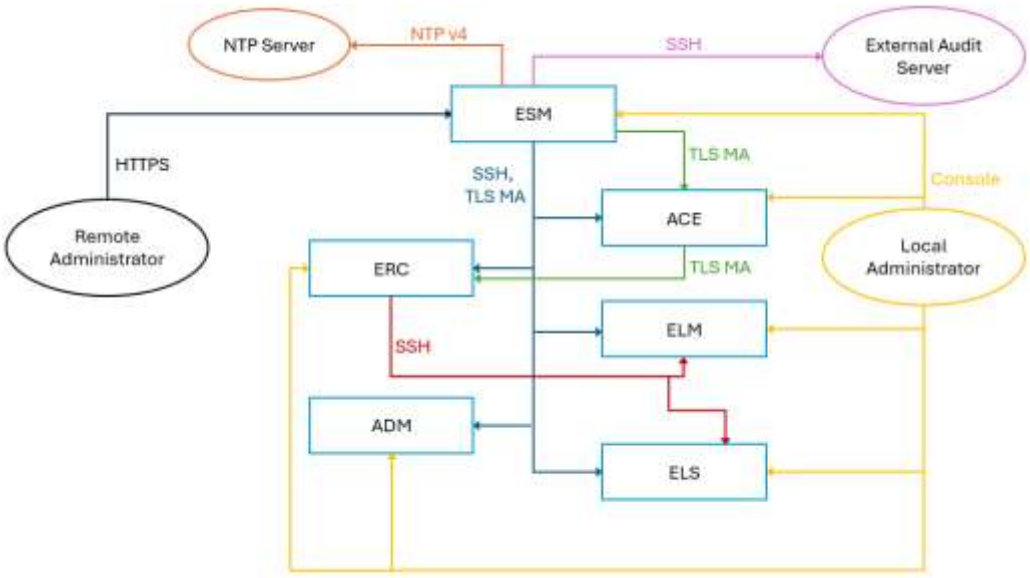
- Management Component: ESM
- Data Components: ERC, ADM
- Auxiliary Components: ACE, ELM, ELS

3.1 TOE Description

The TOE includes the hardware and software of the six Trellix Security Enterprise Security Manager v11.6.12 components. boundary encompasses all the devices of the Trellix Enterprise solution. The ESM is the central management entity responsible for managing all the other devices (colloquially called child devices) in the solution. All Data (ERC, ADM) and Auxiliary (ACE, ELM, ELS) are considered as child devices. Each of the child devices communicates with the ESM over TLS with mutual-authentication and SSH. The management-plane traffic between the ESM and child devices uses SSH; whereas the data-plane traffic uses X.509v3 mutually authenticated TLS. To manage the ESM (and the child devices via ESM), an administrator logs into the Web GUI of the ESM using HTTPS over TLS. Alternatively, an administrator may log into the local console of any of the TOE six components for local administration. Additionally, some of the child devices can communicate with each other over SSH and/or TLS trusted channels. The ESM communicates with a remote audit Syslog server over SSH to store the TOE-generated audit records. The Figure 1 below depicts a representative TOE deployment and interaction between the TOE components and external entities.

Note: The different color coding is only used to easily distinguish communication between the endpoints and it has no other significance.

Figure 1: Representative TOE Deployment



The TOE components communicate with each other over TLS or SSH as identified in the following table. The colored lines correspond to the Figure above.

Table 1: TOE Components Communication

TOE Component	Client	Server	Protocol	Purpose / Data Exchanged
ESM	ESM	All other components	SSH	Control Plane. All configuration and control data. ESM acts as an SSH client, and other TOE components are SSH servers.
	ESM	All other components	TLS MA	Data Plane. Correlation Data for analysis. ESM acts as a TLS client. All other components act as TLS servers. The TLS channel is Mutually Authenticated.
	ESM	ACE	TLS MA	Data Plane. Parsed event log data. ESM acts as a TLS client. ACE acts as a TLS Server. The TLS channel is Mutually Authenticated.
ACE	ESM	ACE	SSH	Control Plane. All configuration and control data. ESM acts as an SSH client, and other TOE components are SSH servers.
	ESM	ACE	TLS MA	Data Plane. Correlation Data for analysis. ESM acts as a TLS client. All other components act as TLS

TOE Component	Client	Server	Protocol	Purpose / Data Exchanged
				servers. The TLS channel is Mutually Authenticated.
	ESM	ACE	TLS MA	Data Plane. Parsed event log data. ESM acts as a TLS client. ACE acts as a TLS Server. The TLS channel is Mutually Authenticated.
	ACE	ECR	TLS MA	Data Plane. Parsed event log data. ACE acts as a TLS Client. ERC acts as a TLS Server. The TLS channel is Mutually Authenticated.
ERC	ERC	ELM	SSH	Data Plane. Raw event log data. ERC acts as an SSH client. ELM and ELS act as an SSH server
	ERC	ELS	SSH	Data Plane. Raw event log data. ERC acts as an SSH client. ELM and ELS act as an SSH server
	ESM	ERC	SSH	Control Plane. All configuration and control data. ESM acts as an SSH client, and other TOE components are SSH servers.
	ESM	ERC	TLS MA	Data Plane. Parsed event log data. ESM acts as a TLS client. ERC acts as a TLS Server. The TLS channel is Mutually Authenticated.
	ACE	ERC	TLS MA	Data Plane. Parsed event log data. ACE acts as a TLS Client. ERC acts as a TLS Server. The TLS channel is Mutually Authenticated.
ELM	ESM	ELM	SSH	Control Plane. All configuration and control data. ESM acts as an SSH client, and other TOE components are SSH servers.
	ESM	ELM	TLS MA	Data Plane. Correlation Data for analysis. ESM acts as a TLS client. All other components act as TLS servers. The TLS channel is Mutually Authenticated.

TOE Component	Client	Server	Protocol	Purpose / Data Exchanged
	ERC	ELM	SSH	Data Plane. Raw event log data. ERC acts as an SSH client. ELM and ELS act as an SSH server
ADM	ESM	ADM	SSH	Control Plane. All configuration and control data. ESM acts as an SSH client, and other TOE components are SSH servers.
	ESM	ADM	TLS MA	Data Plane. Parsed event log data. ESM acts as a TLS client. ADM acts as a TLS Server. The TLS channel is Mutually Authenticated.
ELS	ESM	ELS	SSH	Control Plane. All configuration and control data. ESM acts as an SSH client, and other TOE components are SSH servers.
	ESM	ELS	TLS MA	Data Plane. Parsed event log data. ESM acts as a TLS client. ELS acts as a TLS Server. The TLS channel is Mutually Authenticated.
	ERC	ELS	SSH	Data Plane. Raw event log data. ERC acts as an SSH client. ELM and ELS act as an SSH server

The following table describes the Operational Environment.

Table 2: TOE OE Components Communication

IT Entity	TOE Component	Protocol	Purpose / Data Exchanged
Remote Administrator	ESM	HTTPS	Control Plane. Administrator's remote GUI session. ESM acts as a non-MA TLS server.
NTP server	ESM	NTP v4	Time synchronization. ESM acts as an NTP client. The communication is unencrypted.
External Audit Server	ESM	SSH	Export audit logs. ESM acts as an SSH client.
Local Administrator	All TOE components	Console	Control Plane. Administrator's local console session. The interface supports the CLI.

3.1.1 Component Descriptions

3.1.1.1 Management Component

Enterprise Security Manager (ESM)

The central point of administration for data, settings, and configuration. Using ESM allows you to keep all configuration settings, user and access group profiles, and event and flow data in a single location. It communicates with devices over an encrypted control channel. Central management for all devices.

3.1.1.2 Data Components

Event Receiver (ERC)

The ERC collects security events and network flow data from multi-vendor sources including firewalls, virtual private networks (VPNs), routers, and other network devices. The Receiver gathers and analyzes data from third-party network and security solutions, allowing for the collection and normalization of this data, which provides a single view across devices from multiple vendors. This allows event and flow data collection from devices that send data feeds to the Receiver.

Application Data Monitor (ADM)

The ADM passively monitors traffic, which it then decodes to detect anomalies in application protocols. The ADM accepts rule expressions and tests them against monitored traffic, inserting records into the event table of the database for each triggered rule. It stores the packet that triggered the rule in the event table's packet field. It also adds application-level metadata to the dB session and query tables of the database for every triggered rule. It stores a text representation of the protocol stack in the query table's packet field.

3.1.1.3 Auxiliary Components:

Advanced Correlation Engine (ACE)

Provides dedicated correlation logic to supplement existing ESM event correlation capabilities. It can be deployed in real-time or historical modes. When operating in real-time mode, events are analyzed as they are collected for immediate threat and risk detection. In historical mode, any available data collected by the ESM can be “replayed” through either or both correlation engines, for historical threat and risk detection. So, when new zero-day attacks are discovered, the ESM can look back to determine whether the organization was exposed to that attack in the past, for “sub-zero day” threat detection. It provides two dedicated correlation engines:

- Risk correlation — A risk detection engine that generates a risk score using rule-less correlation.
- Rule correlation — A threat detection engine that detects threats using a traditional rule-based event correlation.

Enterprise Log Manager (ELM)

Supports the storage and management of, access to, and reporting of log data. You can define data sources as well as store and manage data from these data sources. You can also set up jobs that search, export, and check the data for integrity, allowing you to view the results and save the information. Log data from a given source may be associated with an ELS component or an ELM component, but not both.

Enterprise Log Search (ELS)

The ELS component provides high-speed access to the raw security events in an uncompressed form and is used to perform forensic analysis of events and quickly search through large amounts of log data. This component is optional in Trellix Enterprise installations. Log data from a given source may be associated with an ELS component or an ELM component, but not both.

3.1.2 Evaluated Configuration

The minimum configuration required for a Trellix TOE deployment consists of at least one management component, one data component, and one auxiliary component. In addition to the minimum configuration, additional instances of the data components or auxiliary components can be added to expand upon the minimum configuration in order to address larger enterprise deployments.

All six TOE components are part of the evaluation. However, a minimum configuration of the TOE that was tested is identified below.

1. Management Component:
   a. Enterprise Security Manager (ESM)
2. Data Components:
   a. Event Receiver (ERC)
3. Auxiliary Components:
   - Advanced Correlation Engine (ACE)

3.1.3 Physical Boundary

The physical boundary of the TOE is illustrated by the solid Blue rectangular boxes in Figure 1 above. The TOE boundary includes the hardware, operating system, and Trellix application software of each of the six TOE components. The following table describes the hardware details and Table 4 describes the software details of the six TOE components.

Table 3: TOE Component Descriptions

Component	Required	Network ports	Processors	Memory
ESM	Yes (1)	One (1) IPMI port Two (2) Ethernet Management ports One (1) VGA to connect Monitor One (1) Ethernet port not used	2x Intel Xeon Gold 5218 (Cascade Lake)	16x 16GB DDR4 2933MHz
			2x Intel Xeon Gold 6230 (Cascade Lake)	16x 32GB DDR4 2933MHz
ERC	Yes (At least 1)	One (1) IPMI port Two (2) Ethernet Management ports One (1) Ethernet Additional Management port One (1) Ethernet port not used Two (2) Ethernet ports for HA	1 x Intel Xeon E-2224 (Coffee Lake); or 2x Intel Xeon Gold 5218 (Cascade Lake)	2 x 16GB DDR4 2666MHz
				16x 16GB DDR4 2933MHz
ADM			2x Intel Xeon Gold 5218 (Cascade Lake)	16x 32GB DDR4 2933MHz
ACE ELM ELS	Yes (At least 1)	One (1) IPMI port Two (2) Ethernet Management ports One (1) Ethernet Additional Management port One (1) Ethernet port not used Two (2) Ethernet ports for HA	2x Intel Xeon Gold 5218 (Cascade Lake)	16x 16GB DDR4 2933MHz
				16x 32GB DDR4 2933MHz

Table 4: TOE Software Component Descriptions

Component	Operating System	Software Build	Cryptographic Library
ESM	Trellix Nitro OS v11.6.12	ESS_update_11.6.12.signed.tgz	BC-FJA (Bouncy Castle FIPS Java API) v 1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3
ERC		RECIEVER_Update_11.6.12.signed.tgz	
ADM			

Component	Operating System	Software Build	Cryptographic Library
ACE			
ELM			
ELS			

4 Security Policy

4.1 Security Functions Provided by the TOE

The TOE provides the security functions required by NDcPP v2.2e.

4.1.1 Security Audit

The TOE keeps local and remote audit records of security relevant events. The TOE internally maintains the date and time which can either be set manually or synchronized with an NTP server.

4.1.2 Cryptographic Support

The TOE provides cryptographic support for the services described in Table 5. The related FIPS140-2 validation details are provided in Table 21 of the ST.

Table 5: TOE Provided Cryptography

Cryptographic Method	Use within the TOE	Library Implementation
TLS Establishment	For inter-TOE-components communication (mutually authenticated TLS) For remote administrative sessions over HTTPS – non mutually authenticated TLS (ESM only)	BC-FJA (Bouncy Castle FIPS Java API) v 1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3
SSH Establishment	For inter-TOE-components communication	Trellix OpenSSL FIPS Object module v1.0.3
ECDSA Signature Services	Used in SSH session establishment.	Trellix OpenSSL FIPS Object module v1.0.3
RSA Signature Services	Used in TLS session establishment. Used in SSH session establishment. Used in secure software update	BC-FJA (Bouncy Castle FIPS Java API) v 1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3
DRBG	Used in TLS session establishment. Used in SSH session establishment	BC-FJA (Bouncy Castle FIPS Java API) v 1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3
SHS	Used in secure software update, as well as in computing hash values for TLS and SSH cryptographic operations.	BC-FJA (Bouncy Castle FIPS Java API) v 1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3
HMAC-SHS	Used to provide TLS traffic integrity verification. Used to provide SSH traffic integrity verification	BC-FJA (Bouncy Castle FIPS Java API) v 1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3

Cryptographic Method	Use within the TOE	Library Implementation
AES	Used to encrypt TLS traffic Used to encrypt SSH traffic	BC-FJA (Bouncy Castle FIPS Java API) v 1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3

4.1.3 Identification and Authentication

Administrators connecting to the TOE are required to enter an administrator username and password to authenticate the administrative connection prior to access being granted.

The TOE components authenticate to one another through X.509 certificates configured during the initial installation and setup process of the TOE (for data planes over TLS) or via public key authentication (for data planes over SSH). Administrators using the SSH remote CLI authenticate to the TOE using usernames and passwords.

4.1.4 Security Management

The TOE enables secure local and remote management of its security functions, including:

- Local console CLI administration.
- Remote GUI administration via HTTPS/TLS.
- Intra-TOE communication via SSHv2.
- Timed user lockout after multiple failed authentication attempts.
- Password complexity enforcement.
- Configurable banners to be displayed at login.
- Timeouts to terminate administrative sessions after a set period of inactivity.
- Protection of secret keys and passwords.

4.1.5 Protection of the TSF

The TOE ensures the authenticity and integrity of software updates through digital signatures and requires administrative intervention prior to the software updates being installed.

The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.

4.1.6 TOE Access

The TOE monitors local and remote administrative sessions for inactivity and terminates the session when a threshold time is reached. An advisory notice is displayed at the start of each session.

4.1.7 Trusted Path/Channels

The TSF provides the following trusted communication channels:

- SSH for an audit server

- TLS/HTTPS for remote administrators
- SSH for communication between TOE components

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.

The assumptions included in Table 6 are drawn directly from the PP and any relevant EPs/Modules/Packages.

Table 6 : Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

ID	Assumption
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.

ID	Assumption
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

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.

The threats included in Table 7 are drawn directly from the PP and any EPs/Modules/Packages specified in Section **Error! Reference source not found.**.

Table 7 :Threats

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

ID	Threat
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised. The use of appropriate secure protocols to provide authentication of endpoints (as in the SFRs addressing T.UNTRUSTED_COMMUNICATION_CHANNELS) are ensured by the requirements in FTP_ITC.1 and FTP_TRP.1/Admin; for distributed TOEs the authentication requirements for endpoints in inter-component communications are addressed by the requirements in FPT_ITT.1.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

ID	Threat
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

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 collaborative Protection Profiles for Network Devices, Version 2.2e [NDcPP v2.2e].

- Consistent with the expectations of the PP, 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. See section 7.2 of this report for additional information on product functionality that is not included in the scope of evaluation.

6 Documentation

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

- Trellix Security Enterprise Security Manager Common Criteria Configuration Guide version 0.8 [AGD]
- Trellix Security Enterprise Security Manager v11.6.12 Security Target 2.0
- Trellix Enterprise Security Manager 11.6.x Installation Guide
- Trellix Enterprise Security Manager 11.6.x Product Guide

These are the only documents that should be trusted for the installation, administration, and use of the TOE in its evaluated configuration.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The minimum configuration required for a Trellix TOE deployment consists of at least one management component, one data component, and one auxiliary component when the components are configured in accordance with the documentation listed in Section 6 of this report. In addition to the minimum configuration, additional instances of the data components or auxiliary components can be added to expand upon the minimum configuration in order to address larger enterprise deployments.

All six TOE components are part of the evaluation. However, a minimum configuration of the TOE that was tested is identified below.

4. Management Component:
   a. Enterprise Security Manager (ESM)
5. Data Components:
   a. Event Receiver (ERC)
6. Auxiliary Components:
   - Advanced Correlation Engine (ACE)

7.2 Excluded Functionality

The TOE provides enterprise security and threat monitoring information to network administrators. All TOE features related to information monitoring, analytics, and threat evaluation are out of scope for this evaluation.

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 Trellix Security Enterprise Security Manager v1.8, 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 evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e]. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here. In particular, a description of the test configurations may be found is Section 4.1-4.2 of the AAR and a list of the test tools may be found in the table in section 4.2 of the AAR.

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 5 and CEM version 3.1 rev 5. The evaluation determined the Trellix Security Enterprise Security Manager v11.6.12 to be Part 2 extended and Part 3 conformant, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

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 Trellix Security Enterprise Security Manager v11.6.12 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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e].

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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e] 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's 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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e] 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 were 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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e] 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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e] 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 most recent vulnerability search was conducted on March 4, 2025. A list of search terms, databases searched, and evaluation findings may be found in section 6.3 of the AAR.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification were provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network

Devices, Version 2.2e [NDcPP v2.2e] 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 collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e] 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 configuration guide document listed in Section 6. No other versions of the TOE, either earlier or later, were evaluated. 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. See Section 7.2 of this report for product functionality that is not included in the scope of evaluation. Additional functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Annexes

Not applicable.

12 Security Target

Trellix Security Enterprise Security Manager Security Target version 2.0

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 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. Collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP v2.2e]
6. Assurance Activity Report for Trellix Security Enterprise Security Manager version 1.6 [AAR]
7. Evaluation Technical Report for Trellix Security Enterprise Security Manager version 1.8 [ETR]
8. Trellix Security Enterprise Security Manager v11.6.12 Security Target version 2.0 [ST]
9. Trellix Security Enterprise Security Manager v11.6.12 Common Criteria Configuration Guide version 0.8 [AGD]