Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Trend Micro Deep Security 20

31 May 2022

561-LSS

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Program, and the conclusions of the testing laboratory in the evaluation report are consistent with the evidence adduced.

This report, and its associated certificate, are not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Program provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCTL.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Trend Micro Deep Security 20 (hereafter referred to as the Target of Evaluation, or TOE), from **Trend Micro Inc.** , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

Lightship Security is the CCTL that conducted the evaluation. This evaluation was completed on 31 May 2022 and was carried out in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	Trend Micro Deep Security 20
Developer	Trend Micro Inc.

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

EAL 2+ (ALC_FLR.1)

1.2 TOE DESCRIPTION

Trend Micro Deep Security is a software intrusion detection and prevention software system that protects customers' IT system servers and applications. This solution can identify suspicious activity and behavior and take proactive or preventive measures to ensure the security of the machines on which it is deployed. The TOE boundary includes the Deep Security Manager, Deep Security Agent(s) with or without Relay enabled and the Deep Security Virtual Appliance.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

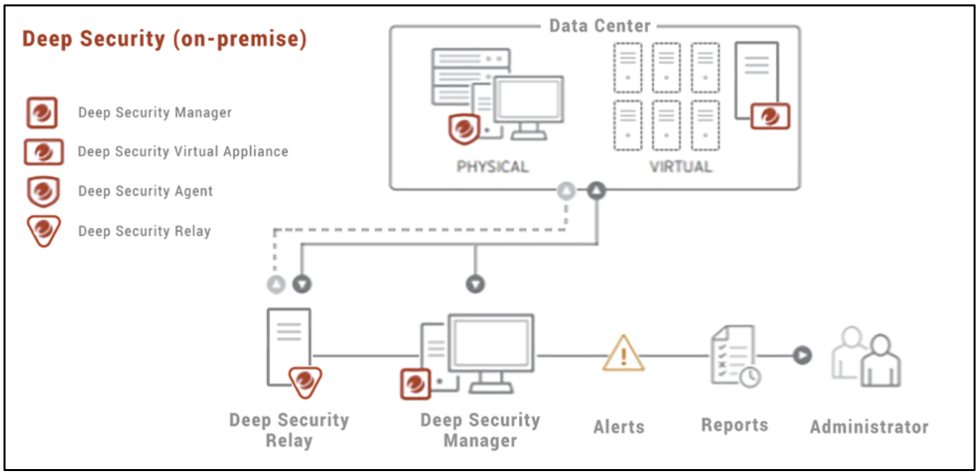

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of TSF
- Cryptographic Support
- Intrusion Detection
- Anti-Virus
- Application Control Actions
- Trusted Path/Channels

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementations have been evaluated by the CAVP and are used by the TOE:

Table 2: Cryptographic Implementation(s)

Cryptographic Algorithms/Implementations	Certificate Number
Trend Micro Java Crypto Module Engine v1.0	A1983
Trend Micro Cryptographic Module Engine v1.0	A1987
CryptoComply Server Engine v2.1	AES 5650, SHS 4531, RSA 3040, ECDSA 1524, HMAC 3764
CryptoComply Server Engine v2.2	AES 4750, SHS 3893, RSA 2594, ECDSA 1185, HMAC 3164

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product’s installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE has access to all the IT System data it needs to perform its functions.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- The TOE is appropriately scalable to the IT System the TOE monitors.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. Physical access to the Deep Security Manager component of the TOE is typically restricted on the premises of the company that owns and administers that component. For IT System computers being protected by the TOE, it is assumed that they are physically protected in a manner appropriate to the security risk and defined usage of each computer.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE can only be accessed by authorized users.

3.2 CLARIFICATION OF SCOPE

The following features of the TOE are excluded in the Common Criteria Evaluated Configuration of the TOE:

- Command Line Interface to Deep Security Agent (for installation and troubleshooting). Administrators can configure Agent self-protection using the Deep Security Manager that prevents unauthorized use of the dsa_control command.
- Legacy SOAP Application Programming Interface to the Deep Security Manager (disabled by default) and Status Monitoring APIs (disabled by default). This interface has been deprecated and no new features will be added to it.
- Command Line Interface to Deep Security Manager (for installation, initial configuration, and troubleshooting). Use of this interface in a Common Criteria environment is described in the Common Criteria Configuration Guide.
- Console Access to Deep Security Virtual Appliance (for installation and troubleshooting only)
- Shift-jis encoding is not supported on agent servers.
- MFA and SAML authentication services are provided by the IT environment, their service providers are outside the scope of this evaluation.
- The Multi-Tenancy feature allows the administrator to create independent instances of Deep Security within their enterprise for individual departments or lines of business within their organization. Multi-tenancy is not tested in this Common Criteria evaluation.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Software/Firmware	• Deep Security Manager version 20.0.344 • Deep Security Windows Agent version 20.0.0-3288 • Deep Security RHEL Agent version 20.0.0-3288 • Deep Security Virtual Appliance installed software version 20.0.0-3288
Environmental Support	Deep Security Manager • Windows Server 2019 • Microsoft SQL Server 2019 Deep Security Agent • Windows Server 2019 or • Linux Red Hat Enterprise Edition 7 Deep Security Virtual Appliance • VMware vCenter 7.0 with ESXi 7.0 • VMware Tools 10.0.6 (or newer) • VMware vShield Endpoint Security Build 15817270

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) The Deep Security 20 Common Criteria Configuration Guide, Document Number APEM209012/200622, 4/11/2021
b) The Deep Security 20 On-premise Administration Guide
c) Deep Security Agent 20 Linux Kernel Support
d) Deep Security 20 Supported features by Platform Guide

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all the procedures required to maintain the integrity of the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer’s test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT TESTING

During this evaluation, the evaluator developed independent functional & penetration tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests

b. Verification of Cryptographic Implementation: The evaluator verified the presence of the claimed cryptographic implementations

c. Anti-virus Engine: The evaluator verified that the anti-virus engine will detect a test anti-virus file; and

d. Trusted Path/Channel: The evaluator verified the SSL cipher suites used for the communication path/channels.

6.3.1 INDEPENDENT TESTING RESULTS

The developer’s tests and the independent tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 VULNERABILITY ANALYSIS

The vulnerability analysis focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their vulnerability analysis.

Type 1 & 2 searches were conducted on **21 March 2022** and included the following search terms:

Deep Security 20.0	Nginx 1.21.0	OpenSSL 1.0.2za-fips
Bouncy Castle Java Fips 1.1.0	Apache Tomcat 8.5.61	Apache Derby 10.14.2.0
Apache HTTP Client 4.5.10	Curl 7.79.0	Zlib 1.2.11

Vulnerability searches were conducted using the following sources:

National Vulnerability Database	Nginx Security Blog
Trend Micro Threat Encyclopedia	OpenSSL Vulnerabilities
Bouncycastle Release notes	Apache Tomcat 8.x vulnerabilities
Google Web search	

6.4.1 VULNERABILITY ANALYSIS RESULTS

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (CCCS). This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CM	Configuration Management
CSE	Communications Security Establishment
CCCS	Canadian Centre for Cyber Security
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Trend Micro Deep Security 20 Security Target v12.0, 30 May 2022.
Trend Micro Deep Security Evaluation Technical Report, v0.13, 31 May 2022.