Certification Report

Trend Micro Deep Security 9.5 SP1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-274-CR
Version:	1.0
Date:	27 March 2015
Pagination:	i to iii, 1 to 9

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. 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 CCS, and the conclusions of the evaluation facility 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 the Communications Security Establishment, 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 Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FORWARD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CSC Security Testing/Certification Laboratories.

By awarding a Common Criteria certificate, the CCS 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 CCEF.

This certification report is associated with the certificate of product evaluation dated 27 March 2015, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarks or registered trademarks:

- Trend Micro is a registered trademark of Trend Micro Inc.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

Trend Micro Deep Security 9.5 SP1 (hereafter referred to as Deep Security 9.5 SP1), from Trend Micro, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that Deep Security 9.5 SP1 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

Deep Security 9.5 SP1 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. Several protection features are combined in centrally managed software agents, adding a suite of protection functionality to the intrusion detection and prevention system.

Deep Security provides the ability to protect itself and associated data from unauthorized access or modification and provides an audit trail to ensure accountability for authorized actions.

CSC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 27 March 2015 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Deep Security 9.5 SP1, 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.

Communications Security Establishment, as the CCS Certification Body, declares that the Deep Security 9.5 SP1 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

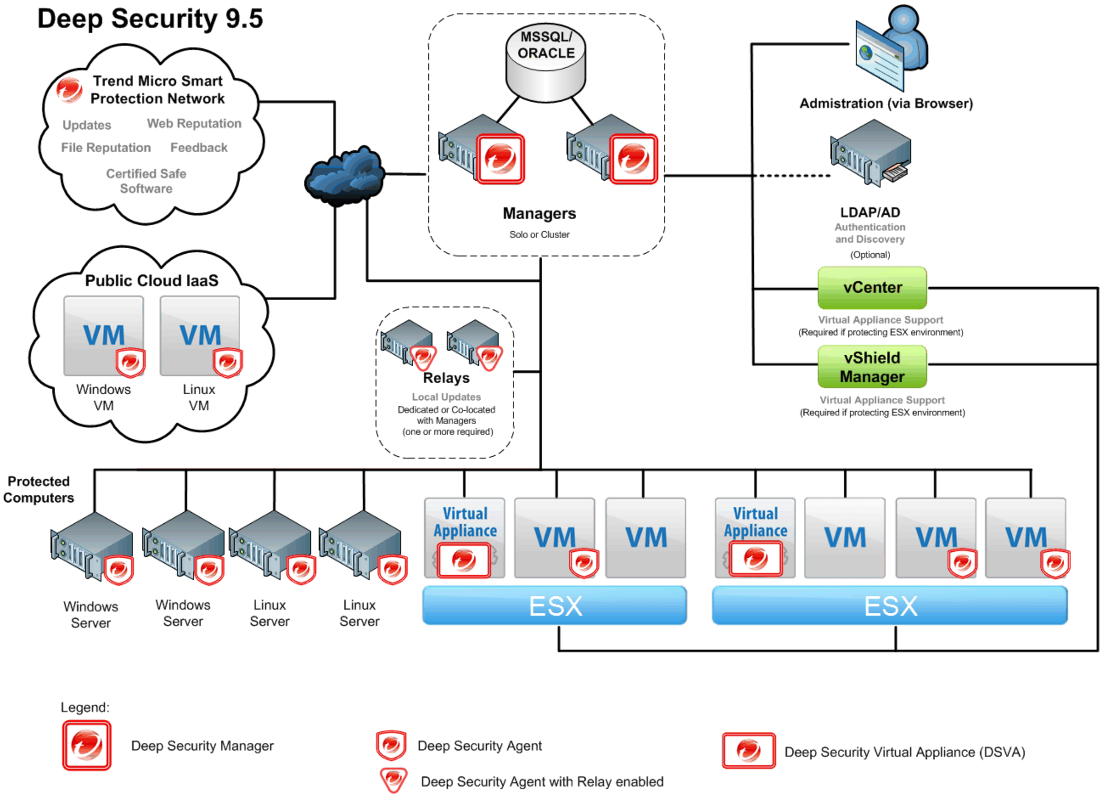
The Target of Evaluation (TOE) for this EAL 2+ evaluation is Trend Micro Deep Security 9.5 SP1 (hereafter referred to as Deep Security 9.5 SP1), from Trend Micro, Inc.

2 TOE Description

Deep Security 9.5 SP1 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. Several protection features are combined in centrally managed software agents, adding a suite of protection functionality to the intrusion detection and prevention system.

Deep Security provides the ability to protect itself and associated data from unauthorized access or modification and provides an audit trail to ensure accountability for authorized actions.

A diagram of the Deep Security 9.5 SP1 architecture is as follows:



3 Security Policy

Deep Security 9.5 SP1 implements a role-based access control policy to control administrative access to the system. In addition, Deep Security 9.5 SP1 implements policies pertaining to the following security functional classes:

Security Audit;

Cryptographic Support;

Security Management;

Identification and Authentication;

Protection of the TSF;

Intrusion Detection and Prevention; and

Anti-virus.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Deep Security 9.5 SP1:

Cryptographic Algorithm	Standard	Certificate #
Advanced Encryption Standard (AES)	FIPS 197	3159, 3004, 3005
Rivest Shamir Adleman (RSA)	FIPS 186-3	873, 828, 872
Secure Hash Algorithm (SHA-1)	FIPS 180-3	2615, 2515, 2516

4 Security Target

The ST associated with this Certification Report is identified below:

Trend Micro Deep Security 9.5 Security Target Version 21.0, 13 March 2015

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

Deep Security 9.5 SP1 is:

a. *EAL 2 augmented, containing all security assurance requirements listed, as well as the following:*
   - *ALC_FLR.1 Basic Flaw Remediation.*

b. *Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:*
   - IDS_SDC.1 System Data Collection;
   - IDS_ANL.1 Analyser Analysis;
   - IDS_RCT.1 Analyser React;
   - IDS_RDR.1 Restricted Data Review;

- IDS_STG.1 Guarantee of System Data Availability;
- IDS_STG.2 Prevention of System Data Loss;
- FAV_ACT.1 Anti-Virus Actions;
- FAV_ALR.1 Anti-Virus Alerts; and
- FAV_SCN.1 Anti-virus Scanning.

c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of Deep Security 9.5 SP1 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.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- One or more authorised administrators will be assigned to install, configure and manage the TOE and the security of the information it contains;
- The TOE can only be assessed by authorized users;
- Administrators and Users of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the guidance documentation; and
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE has access to all the IT System data it needs to perform its functions;
- The TOE is appropriately scalable to the IT systems the TOE monitors; and
- The processing resources of the TOE will be located within facilities providing controlled access.

6.3 Clarification of Scope

Deep Security 9.5 SP1 incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

7 Evaluated Configuration

The evaluated configuration for Deep Security 9.5 SP1 comprises the following components:

Deep Security Manager version 9.5.5600 installed on Windows Server 2012;

Deep Security Agent version 9.5.3-2754 running on one of the following operating systems:

- *Windows Server 2001; or*
- *Linux Red Hat Enterprise Edition 6.*

Or

Deep Security Virtual Appliance Agent version 9.5.3-2754 and Deep Security Filter Driver version 9.5.3-2750 on a VMWare ESX5.5 virtual machine.

The publications entitled

- *Deep_Security_95_SP1_Install_Guide_basic_EN: Basic installation of DSM and DSA;*
- *Deep_Security_95_SP1_Install_Guide_nsx_EN;*
- *Deep_Security_95_SP1_Install_Guide_vmsafe_EN: Installation for DSVA ; and*
- *Deep Security 95 Common Criteria Addendum to Install Guide: Special instructions for CC evaluated configuration.*

describe the procedures necessary to install and operate Deep Security 9.5 SP1 in its evaluated configuration.

8 Documentation

The Trend Micro, Inc. documents provided to the consumer are as follows:

a. Deep_Security_95_SP1_Install_Guide_basic_EN: Basic installation of DSM and DSA;
b. Deep_Security_95_SP1_Install_Guide_nsx_En;
c. Deep_Security_95_SP1_Install_Guide_vmsafe_EN: Installation for DSVA; and
d. Deep Security 95 Common Criteria Addendum to Install Guide: Special instructions for CC evaluated configuration.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Deep Security 9.5 SP1, including the following areas:

Development: The evaluators analyzed the Deep Security 9.5 SP1 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Deep Security 9.5 SP1 security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Deep Security 9.5 SP1 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.

Life-cycle support: An analysis of the Deep Security 9.5 SP1 configuration management system and associated documentation was performed. The evaluators found that the Deep Security 9.5 SP1 configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Deep Security 9.5 SP1 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Deep Security 9.5 SP1. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

10.1 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 ETR[1].

The evaluators analyzed the developer’s test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification was complete.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional 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. Resulting from this test coverage approach is the following list of test goals:

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Assign a policy to a computer; The objective of this test goal is to verify that a policy can be assigned to a computer;

c. Password policies: The objective of this test goal is to verify that the TOE is exercising the password rules properly;

d. Authentication: The objective of this test goal is to validate rules on authentication;

e. Access Control: The objective of this test goal is to test role based access control;

f. Retrieval of anti-malware events: The objective of this test goal is to demonstrate the retrieval of events specified by ID;

g. Identification of Deep Security Manager: The objective of this test goal is to retrieve information on Deep Security Manager that will verify its identity; and

h. Usage Monitoring: The objective of this test goal is to verify the TOE`s ability to return data on usage.

10.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;

b. Search the Public Domain to discover potential vulnerabilities with the TOE;

c. Monitor Network Traffic: The objective of this test goal is to capture traffic between parts of the TOE using Wireshark and to verify that such communication is secured by TLS;

d. TLS Strength: The objective of this test goal is to demonstrate that the TOE is not using weak ciphers; and

e. Heartbleed, Poodle and Shellshock: The objective of this test goal is to examine if the TOE is susceptible to any of those vulnerabilities.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

10.4 Conduct of Testing

Deep Security 9.5 SP1 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place onsite at the developer’s location at Trend Micro, Inc, 40 Hines Road, Suite 200, Ottawa, Ontario, Canada, K2K 2M5. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that Deep Security 9.5 SP1 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Evaluator Comments, Observations and Recommendations76

The users shall follow the user guidance documentation, installation guides, the addendum to the installation guides, and the assumptions specified in the Security Target to install and operate the TOE as specified.

The Deep Security Relay (a separate Trend Micro product) is excluded in the CC evaluation (see Section 1.5 of ST). The TOE's operational environment includes Deep Security Relay. This recommendation serves as a reminder to the user of the TOE that Deep Security Relay has not been evaluated.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

14 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Trend Micro Deep Security 9.5 Security Target Version 21.0, 13 March 2015

e. Trend Micro Deep Security 9.5 Evaluation Technical Report, version 3, 27 March2015.