Certification Report

EAL 4 Evaluation of Deep Security 7.5 SP2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-152
Version: 1.0
Date: 2 September 2011
Pagination: i to iii, 1 to 10

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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply 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 Canada, 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 Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

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 Canada.

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 DOMUS IT Security Lab located in Ottawa, Canada.

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, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 2 September 2011, 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 trademark of Trend Micro, Inc.;
- Linux is a registered trademark of Linus Torvalds Inc.;
- HP-UX is a trademark of Hewlett Packard Company in the United States;
- VMware is a registered trademark of VMware Incorporated; and
- Oracle is a registered trademark of Oracle Corporation.

TABLE OF CONTENTS

Executive Summary

Deep Security 7.5 SP2 (hereafter referred to as Deep Security 7.5), from Trend Micro, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 *augmented* evaluation.

Deep Security 7.5 is an intrusion detection and prevention system that provides anti-malware, stateful firewall, deep packet inspection, file and system integrity monitoring, and log inspection and collection capability. Deep Security 7.5 protects itself and its associated data from unauthorized access and modification, and provides an audit trail to ensure accountability for authorized actions.

DOMUS IT Security Lab is the CCEF that conducted the evaluation. This evaluation was completed on 23 August 2011 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 7.5, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security 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 results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.* The following augmentation is claimed: ALC_FLR.1 – Basic Flaw Remediation.

Deep Security 7.5 is conformant with the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness, Version 1.7, July 25, 2007.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Deep Security 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] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 *augmented* evaluation is Deep Security 7.5 SP2 (hereafter referred to as Deep Security 7.5), from Trend Micro, Inc..

2 TOE Description

Deep Security 7.5 comprises the applications management console *Deep Security Manager* and traffic filtering engines called *Deep Security Agents*. Deep Security Manager is deployed by downloading and installing the application to a designated management computer. Deep Security Agents are deployed by downloading and installing the applications to the physical or virtual machines to be protected.

Deep Security 7.5 provides anti-malware, stateful firewall, deep packet inspection, file and system integrity monitoring, and log inspection and collection capability. Deep Security 7.5 protects itself and its associated data from unauthorized access and modification, and provides an audit trail to ensure accountability for authorized actions.

A detailed description of the Deep Security 7.5 architecture and functionality is found in Section 1.3 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Deep Security 7.5 is identified in Section 1.5.2 of the Security Target (ST).

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

Cryptographic Algorithm	**Standard**	**Certificate #**
Advanced Encryption Standard (AES)	FIPS 197	1754, 1667, 1753
Secure Hash Algorithm (SHA-1, SHA-256)	FIPS 180-3	1541, 1460, 1540
Rivest, Shamir and Adleman (RSA)	FIPS 186-3	873, 828, 872

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Trend Micro Deep Security 7.5 Security Target
Version: 1.18
Date: 2 August 2011

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

Deep Security 7.5 is:

a. *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_(EXT).1 - Anti Virus actions;
    - FAV_ALR_(EXT).1 - Anti-Virus Alerts; and
    - FAV_SCN_(EXT).1 - Anti-Virus Scanning.
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3;
c. *Common Criteria EAL 4 augmented, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.1 – Basic Flaw Remediation;* and
d. Deep Security 7.5 is conformant with the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness, Version 1.7, July 25, 2007.

6 Security Policy

Deep Security 7.5 implements a role-based access control policy to control user access to the system; details of this security policy can be found in Section 6.1 of the ST.

In addition, Deep Security 7.5 implements policies pertaining to audit, identification and authentication, secure intra-TOE communication, intrusion detection and prevention, and anti-virus. Further details on these security policies may be found in Section 6.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Deep Security 7.5 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.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- 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, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation; and
- The TOE can only be accessed by authorized users.

7.2 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 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; and
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

7.3 Clarification of Scope

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

8 Evaluated Configuration

The evaluated configuration for Deep Security 7.5 comprises:

- Deep Security Manager v7.5.6333 that runs on Windows Server 2008 R2 (64 bit) with Oracle 10g or 11g Express Edition;
- Deep Security Agent v7.5.0.5535 that runs on Windows Server 2008 R2;
- Deep Security Agent v7.5.0.5531 that runs on Solaris 10, Linux Red Hat Enterprise Edition 5, Linux SUSE 11, and HP-UX 11i;
- Deep Security Agent v7.5.0.5533 that runs on AIX 6.1; and
- Deep Security Virtual Appliance v7.5.0.34 with Deep Security Filter Driver v7.5.0.5434 that runs on VMware ESX 4.1.

The publication entitled *Trend Micro Deep Security 7.5 Common Criteria Addendum to the Installation Guide* describes the procedures necessary to install Deep Security 7.5 in its evaluated configuration.

9 Documentation

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

- Trend Micro Deep Security 7.5 User's Guide, v1.1, September 2011;
- Trend Micro Deep Security 7.5 Installation Guide, v1.1RC, January 2011; and
- Trend Micro Deep Security 7.5 Common Criteria Addendum to the Installation Guide, v1.0, January 2011.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Deep Security 7.5, including the following areas:

Development: The evaluators analyzed the Deep Security 7.5 functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Deep Security 7.5 architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Deep Security 7.5 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 7.5 configuration management system and associated documentation was performed. The evaluators found that the Deep Security 7.5 configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Deep Security 7.5 during distribution to the consumer.

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Deep Security 7.5 design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Trend Micro, Inc. for Deep Security 7.5. 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.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of Deep Security 7.5. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the Deep Security 7.5 in its operational environment.

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

11 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 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[2].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification, TOE design and security architecture description was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

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 DOMUS IT Security Lab test goals:

a. Repeat of Developer's Tests: The evaluators repeated a subset of the developer's test to gain assurance of the developer's overall testing effort. The evaluator chose a subset of tests that exercised all of the TOE's security related interfaces and functions;

b. Security Management: The evaluators confirmed that the security parameters are able to be securely managed by repeating a subset of the developer's tests as well as a number of independent tests that exercised the security management interfaces;

c. User Data Protection: The evaluators confirmed the TOE's ability to protect user data by performing a number of tests against the Role Based Access Control enforcement functions;

d. Audit: The evaluators ensured that event logging requirements have been met by confirming the capture of logs and the presence of event details as specified in the ST;

e. Identification and Authentication: The evaluators ensured that access to the TOE is restricted to authorized administrators only;

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

f. Intrusion detection and prevention: The evaluators confirmed the correct operation of the Deep Packet Inspection functionality by ensuring detection of attempted exploits of known vulnerabilities on protected systems;

g. Firewall: The evaluators confirmed the correct operation of the firewall by testing the enforcement of packet filter and stateful filter policies;

h. Antimalware: The evaluators confirmed that the TOE detected and removed European Institute for Computer Antivirus (EICAR) test viruses;

i. Integrity monitoring: The evaluators confirmed that the TOE detected changes to monitored system files; and

j. Log analysis: The evaluators confirmed that the TOE alerted the administrator upon detection of anomalous logging events.

11.3 Independent Penetration Testing

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

- Reconnaissance and exploratory testing to observe application behaviour including port scanning, client side script and HTTP packet inspection;
- Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;
- Testing web application vulnerabilities associated with the management interface including injection, cross-site scripting and session manipulation attacks;
- Attempting bypass of malware detection through obfuscation; and
- Attempting to bypass audit policies through manipulation of time variables.

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

11.4 Conduct of Testing

Deep Security 7.5 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at DOMUS IT Security Lab. 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.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that Deep Security 7.5 behaves as specified in its ST, functional specification, TOE design and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

Deep Security 7.5 provides a comprehensive intrusion detection and prevention system supported by desirable security functionality. It is recommended that users wishing to deploy the evaluated configuration follow the guidance provided in the *Trend Micro Deep Security 7.5 Common Criteria Addendum to the Installation Guide*.

14 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
ST	Security Target
TOE	Target of Evaluation

15 References

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

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness, Version 1.7, July 25, 2007.

e. Trend Micro Deep Security 7.5 Security Target, 1.18, 2 August 2011.

f. Trend Micro Deep Security 7.5 EAL4+ Evaluation Technical Report, v1.0, 23 August 2011.