Certification Report

EAL 2+ Evaluation of Symantec™ Data Loss Prevention Version 11.1.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-194-CR
Version: 1.0
Date: 5 March 2012
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 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 EWA-Canada 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 5 March 2012, 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 registered trademark:

- *Symantec is a registered trademark of Symantec Corporation in the United States and other countries*

TABLE OF CONTENTS

Disclaimer ..... **i**

Foreword ..... **ii**

Executive Summary **1**

1 Identification of Target of Evaluation **2**

2 TOE Description **2**

3 Evaluated Security Functionality **2**

4 Security Target **2**

5 Common Criteria Conformance **3**

6 Security Policy **3**

7 Assumptions and Clarification of Scope **3**

7.1 SECURE USAGE ASSUMPTIONS 3
7.2 ENVIRONMENTAL ASSUMPTIONS 4
7.3 CLARIFICATION OF SCOPE 4

8 Evaluated Configuration **4**

9 Documentation **5**

10 Evaluation Analysis Activities **5**

11 ITS Product Testing **6**

11.1 ASSESSMENT OF DEVELOPER TESTS 6
11.2 INDEPENDENT FUNCTIONAL TESTING 6
11.3 INDEPENDENT PENETRATION TESTING 7
11.4 CONDUCT OF TESTING 7
11.5 TESTING RESULTS 8

12 Results of the Evaluation **8**

13 Acronyms, Abbreviations and Initializations **8**

14 References **8**

Executive Summary

Symantec™ Data Loss Prevention Version 11.1.1 (hereafter referred to as DLP), from Symantec, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

The TOE is a data loss prevention system, which provides for the detection and prevention of unauthorized use and transmission of confidential or sensitive information from secured IT resources. Once data has been identified as sensitive DLP takes action to protect the data as well as report on any violations that have occurred.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 1 February 2012 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 DLP, 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 2 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.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the DLP 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) 2 augmented evaluation is Symantec™ Data Loss Prevention Version 11.1.1 (hereafter referred to as DLP), from Symantec.

2 TOE Description

The TOE is a data loss prevention system, which provides for the detection and prevention of unauthorized use and transmission of confidential or sensitive information from secured IT resources. Once data has been identified as sensitive DLP takes action to protect the data as well as report on any violations that have occurred.

The following list provides a brief description of each major TOE component:

- The Enforce Server provides a centralized administration console that allows an authorized Administrator to manage the TOE.
- The Endpoint Server is comprised of the Endpoint Discover and Endpoint Prevent components. The Endpoint Server manages the DLP Agents which are installed on endpoint desktops and laptops.
- The Network Discover/Network Protect Server scans and prevents security violations on network servers and endpoints that do not have the DLP Agents installed. The Network Discover/Network Protect Server is connected to the corporate Local Area Network.
- The Network Monitor/Network Prevent Server scans network traffic and prevents sensitive data from leaving the target network.

A detailed description of the DLP architecture is found in Section 1.6 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for DLP is identified in Section 6 of the ST.

4 Security Target

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

Title: Security Target Symantec™ Data Loss Prevention 11.1.1

Version: Document Version 1.0
Date: 23 January 2012

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.*

DLP is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 2 augmented*, containing all security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.2 –Flaw Reporting Procedures.

6 Security Policy

DLP implements an information flow control policy which enforces administrator defined actions on the transmission of sensitive files or data. Details of this security policy can be found in Section 6 of the ST.

In addition, DLP implements policies pertaining to Security Audit, Identification and Authentication, and Security Management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of DLP 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 TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors; and
- The authorized administrators are neither careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE has access to all the IT resources it needs to perform its functions;
- Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users;
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access; and
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

7.3 Clarification of Scope

DLP is not intended to be placed or operated in a hostile environment, and should be protected by other products specifically designed to address sophisticated threats.

8 Evaluated Configuration

The evaluated configuration for DLP comprises:

a. Symantec™ DLP Enforce server software version 11.11000.10054;

b. Symantec™ DLP Network Discover server software version 11.11000.10054;

c. Symantec™ DLP Network Monitor server software version 11.11000.10054;

d. Symantec™ DLP Network Prevent server software version 11.11000.10054;

e. Symantec™ DLP Network Protect server software version 11.11000.10054;

f. Symantec™ DLP Endpoint Discover server software version 11.11000.10054;

g. Symantec™ DLP Endpoint Prevent server software version 11.11000.10054; and

h. Symantec™ DLP Agent software version 11.11000.10054.

The third party software that the TOE was tested upon is identified in Table 4 of the ST.

The publication entitled *Symantec DLP 11.1 Operational User Guidance and Preparative Procedures Supplement version 1.0* describes the procedures necessary to install and operate DLP in its evaluated configuration.

9 Documentation

The Symantec documents provided to the consumer are as follows:

a. Symantec DLP 11.1 Administration Guide, 2011;

b. Symantec DLP 11.1 Installation Guide for Windows, 2011;

c. Symantec DLP 11.1 Installation Guide for Linux, 2011;

d. Symantec DLP Oracle 11g Installation and Upgrade Guide, 2011;

e. Symantec DLP 11.1 System Requirements Guide, 2011; and

f. Symantec DLP 11.1 Operational User Guidance and Preparative Procedures Supplement version 1.0.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of DLP, including the following areas:

Development: The evaluators analyzed the DLP 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 DLP 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 DLP 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 DLP configuration management system and associated documentation was performed. The evaluators found that the DLP configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

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

The evaluators reviewed the flaw remediation procedures used by Symantec for DLP. 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 DLP. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify DLP potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the DLP in its operational environment.

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

11 ITS Product Testing

Testing at EAL 2 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 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.

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 EWA-Canada test goals:

[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.

a. Initialization: The goal of this test case is to verify that the Administrator can install and configure the TOE following the guidance provided with the product, and duplicate the settings and environment as detailed in the Security Target;

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

c. Network Discovery: The goal of this test case is to verify the TOE's ability to protect data from loss and misuse in accordance with Administrator pre-defined polices;

d. Register and Configure Detection Servers. The goal of this test case is to verify that an authroized Adminstrator can add and configure detection servers using the Enforce Server Adminstrator Console; and

e. Strong Password Policy. The goal of this test case is to verify that the TOE enforces strong passwords.

11.3 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. Port Scan: The purpose of this test case is to identify any suspicious open ports on the TOE system;

b. Concurrent Administrator Sessions: The purpose of this test case is to verify that the TOE manages concurrent administrator sessions successfully;

c. User Session Management: The purpose of this test case is to verify that the TOE destroys a user session successfully; and

d. SQL Injections: The purpose of this test case is to verify that the TOE is resistant to standard SQL injection attacks against its logon functionality.

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

11.4 Conduct of Testing

DLP 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 EWA-Canada. 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 DLP behaves as specified in its ST and functional specification.

12 Results of the Evaluation

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

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
DLP	Data Loss Prevention
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 Functionality

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 3, July 2009.

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

d. Security Target Symantec™ Data Loss Prevention 11.1.1, Document Version 1.0, 23 January 2012.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of Symantec™ Data Loss Prevention Version 11.1.1, Version 1.1, 1 February 2012.