Certification Report

Symantec Data Loss Prevention (DLP) v25.1

Sponsor and developer:	***Symantec, A Division of Broadcom*** **3421 Hill View Ave,** **Palo Alto California 94304** **USA**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2500024-01-CR**
Report version:	**1**
Project number:	**NSCIB-2500024-01**
Author(s):	**Brian Smithson**
Date:	**08 December 2025**
Number of pages:	**11**
Number of appendices:	**0**

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, 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 or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Symantec Data Loss Prevention (DLP) v25.1. The developer of the Symantec Data Loss Prevention (DLP) v25.1 is Symantec, A Division of Broadcom located in Palo Alto, California, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE (Symantec Data Loss Prevention (DLP)) is used by organizations to safeguard sensitive data such as company information, customer data, and intellectual property. Symantec DLP enables an organization to:

- Discover and locate confidential information in repositories, on file and web servers, in databases, and on endpoints (desktop and laptop systems)
- Protect confidential information through quarantine
- Monitor network traffic for transmission of confidential data
- Monitor the use of sensitive data on endpoints
- Prevent transmission of confidential data to outside locations
- Automatically enforce data security and encryption policies

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 2025-12-08 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Symantec Data Loss Prevention (DLP) v25.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Symantec Data Loss Prevention (DLP) v25.1 are advised to verify that their own environment is consistent with 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 the TOE meets the EAL2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw Reporting Procedures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CEM:2022 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 *[CC]*.

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Symantec Data Loss Prevention (DLP) v25.1 from Symantec, A Division of Broadcom located in Palo Alto, California, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Enforce Server (Windows)	25.1.00000.60229
	Detection Server (Windows Platform)	25.1.00000.60229
	Detection Server (Linux Platform)	25.1.00000.60229
	DLP Agent (Windows Platform)	25.1.00000.60234

To ensure secure usage a set of guidance documents is provided, together with the Symantec Data Loss Prevention (DLP) v25.1. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE has the following features:

- Security Audit
  - Audit entries are generated for security related events.
- User Data Protection
  - The TOE will detect and block the transfer of data identified as sensitive.
- Identification and Authentication
  - Administrative users are identified and authenticated prior to being allowed access to the Enforce Management Console. The TOE maintains username, role, and password information on each administrative user. Strong passwords are enforced and users are locked out after a number of consecutive unsuccessful authentication attempts.
- Security Management
  - The TOE provides management capabilities via a Web-based GUI, accessed via HTTPS. Management functions allow the administrators to view incidents, manage administrative user accounts, and create and manage policies and responses. A number of roles are available to support separation of duties.
- Protection of the TSF
  - The communications links between the parts of the TOE are protected using Transport Layer Security (TLS) 1.2 and 1.3. The DLP agent software is monitored for tampering and the TOE reports if the agent has been removed.
- Trusted Path/Channels
  - The communications links between the TOE components are protected using HTTPS (TLS 1.3).

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

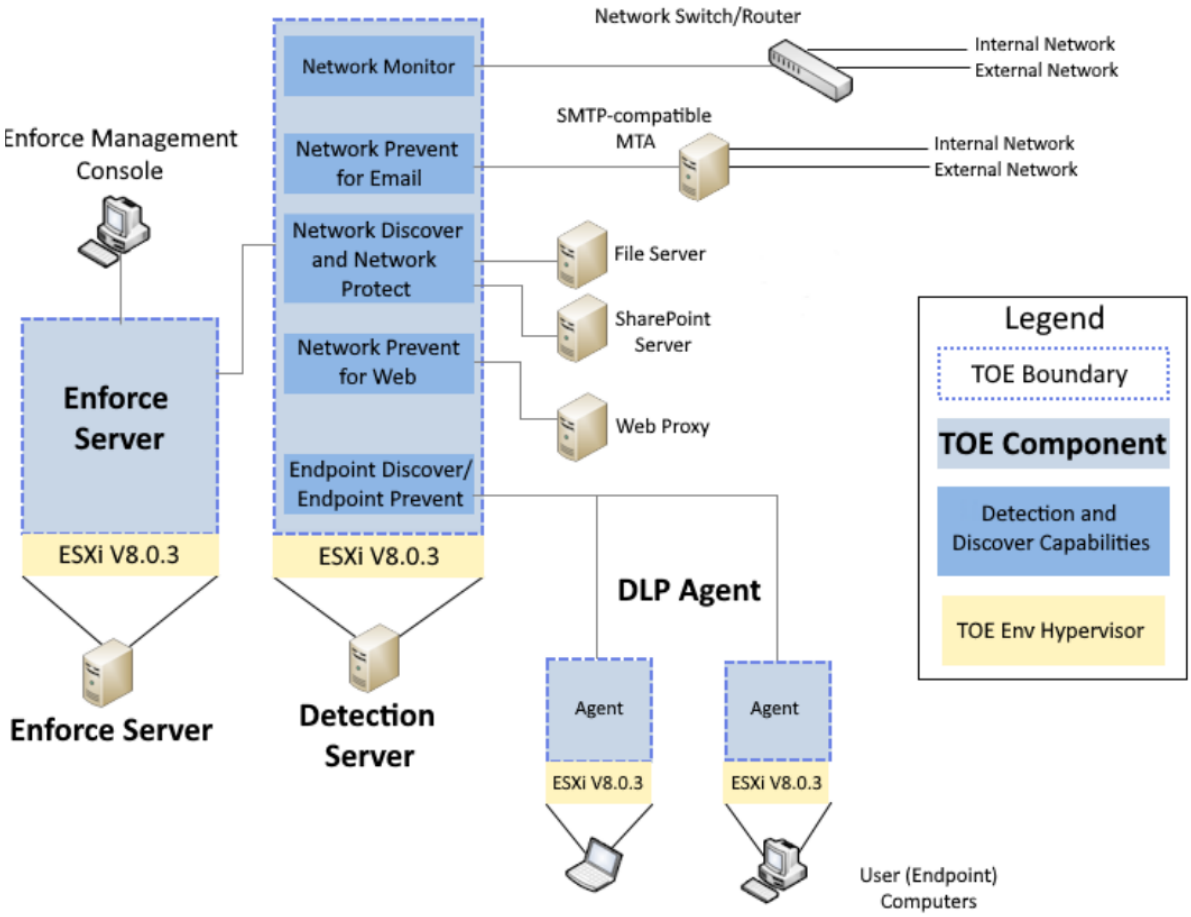
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The central component for a DLP implementation is the DLP Enforce Server, which provides a management interface for defining the policies that are enforced throughout the network. The Enforce Server works with one or more Detection servers to protect data and report on violations (called incidents). Detection servers may be deployed on a single server or in a distributed architecture, depending upon the organization's network requirements.
The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Symantec Data Loss Prevention Help Center 25.1	2025-08-18
Symantec™ Data Loss Prevention 25.1 Common Criteria Guidance Supplement, Evaluation Assurance Level (EAL): EAL2+	V0.6

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer test approach is summarized as follows:

- 11 tests in total have been performed by the developer. The test cases are categorized based on SFR classes and TSFIs. These test cases cover all TSFIs and all subsystems and subsystem interactions.

Developer test plans demonstrate operation of the TOE and satisfy the SFRs claimed in the Security Target (ST).

The security mechanisms that aren't covered by the developer or need to be more broadly tested will be covered through independent testing. The following scenarios will be tested by the evaluator on all possible combinations of the TOE components (Linux, Windows):

- To verify the TOE configuration/version.
- Verify that the application invokes the mechanisms recommended by the platform vendor for storing and setting configuration options.
- Verify default file permissions which protect the application binaries and data files from modification by unprivileged users.
- Verify the functionalities provided by the application when new credentials are configured.
- Verify that the application does not write user-modifiable files to directories that contain executable files, unless explicitly directed by the user to do so.
- Verify that the application's executable files are not changed by the application.
- Verify that persistent credentials are stored securely.
- Use Nessus to scan the TOE for potential vulnerabilities.

2.6.2 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

SFR design analysis: Based on the information obtained in the evaluation evidence, the SFR implementation details were examined. The aspects described in CEM annex B were considered.

Additional security analysis: When the implementation of the SFR was understood, a coverage check was performed on the relevant aspects of all SFRs.

Scanning the TOE using the applicable vulnerability scanning tools (e.g., NMAP, NESSUS) to collect information about the TOE and identify potential vulnerabilities.

Public vulnerability search: The evaluator performed public domain vulnerability search based on the TOE name, TOE type, and identified 3rd party security relevant libraries and/or services. Several additional potential vulnerabilities were identified during a search in the public domain.

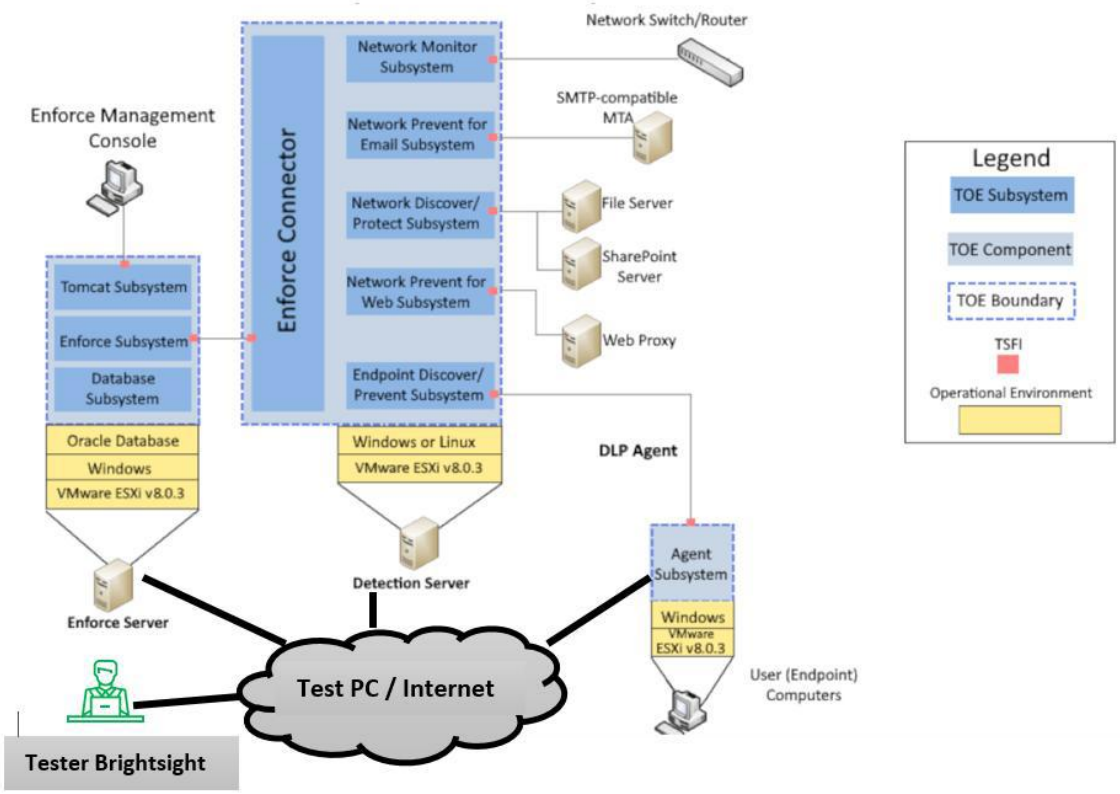
The potential vulnerabilities identified were analysed, and some of the potential vulnerabilities were concluded not exploitable within in the Basic attack potential, or covered by guidance. For remaining potential vulnerabilities, penetration tests were devised.

The evaluator devised six (6) penetration tests to verify that the TOE, in its operational environment is resistant to an attacker possessing a Basic attack potential. All tests are logical tests.

The evaluator performed all the tests (independent tests and penetration tests) in the period between 14th October, 2025 to 11th November, 2025 and with 4 man-week (160 man-hour) in total for testing and reporting.

2.6.3 Test configuration

Below is the test configuration that was used during this evaluation:



2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Symantec Data Loss Prevention (DLP) v25.1.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Symantec Data Loss Prevention (DLP) v25.1, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 2 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: *none*, which are out of scope as there are no security claims relating to these.

3 Security Target

The Symantec Data Loss Prevention (DLP) 25.1 Security Target, v2.3, 26 November 2025 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts 1 to 5, CC:2022 Revision 1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
[ETR]	Evaluation Technical Report “Symantec Data Loss Prevention (DLP) v25.1” – EAL2 with ALC_FLR.2, 25-RPT-942, v3.0, 27 November 2025
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	Symantec Data Loss Prevention (DLP) 25.1 Security Target, v2.3, 26 November 2025

(This is the end of this report.)