Symantec™ Data Loss Prevention 14.5

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 1943-000-D102
Version: 1.2
15 November 2016

Symantec Corporation
303 2nd Street 1000N
San Francisco, CA 94107
United States of America

Prepared by:
EWA-Canada
1223 Michael Street, Suite 200
Ottawa, Ontario, Canada
K1J7T2

Enabling a More Secure Future

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the TOE, the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target (ST) reference, the Target of Evaluation (TOE) reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the Information Technology (IT) environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8 Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	Symantec™ Data Loss Prevention 14.5 Security Target
ST Version:	1.2
ST Date:	15 November 2016

1.3 TOE REFERENCE

TOE Identification:	Symantec™ Data Loss Prevention 14.5 (Symantec DLP 14.5.0.24034 and Symantec DLP Agent 14.5.0.24028)
TOE Developer:	Symantec Corporation
TOE Type:	Data Protection

1.4 TOE OVERVIEW

Symantec Data Loss Prevention (DLP) may be used by organizations to safeguard sensitive data such as company information, customer data, and intellectual property. DLP provides this functionality through the discovery, monitoring, and protection of sensitive information on network resources within an organization’s IT infrastructure. Sensitive data may include credit card numbers, names, addresses, identification numbers or any data a company deems proprietary. Symantec DLP enables an organization to:

- Discover stored data on network resources
- Monitor how that data is being used
- Protect the data from being leaked or stolen

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. Detection servers may be deployed on a single server or in a distributed architecture, depending upon the organization’s network requirements. The following paragraphs describe the DLP components subject to this evaluation.

1.4.1 Enforce Server

The Enforce Server is the central management component of Symantec DLP. It provides a web-based GUI that serves as the management interface for all Symantec DLP functions.

Through the Enforce Management Console, authorized administrators define data loss policies for automatically detecting and protecting sensitive data, review and remediate incidents, and perform system administration across endpoints and managed network resources. The Enforce Server allows administrators to enforce the organization’s data security policies by pushing policies out to all other DLP components.

1.4.2 Endpoint Discover and Endpoint Prevent

The Endpoint Discover and Endpoint Prevent detection server components work with DLP agents installed on the endpoint desktops and networked laptops. Endpoint Discover detects sensitive data on the endpoints. Endpoint Prevent then monitors that sensitive data and detects when it is being copied or transferred from those devices to removable storage, network shares or cloud storage. When a policy violation is detected, the transfer may be blocked, or the user may be notified of the violation in a pop-up window.

1.4.3 Network Discover/Cloud Storage Discover and Network Protect

Network Discover/Cloud Storage Discover scans for sensitive data stored on network resources. Network Protect then acts on any discoveries in accordance with the security policy by moving or quarantining the files.

1.4.4 Network Monitor

Network Monitor is placed on the network between an internal switch or router and an external switch or router to capture and analyze the information that is being sent outside of the organization. It detects data that has been identified as sensitive over the designated protocols.

1.4.5 Network Prevent for Email

Network Prevent for Email is integrated with the Mail Transfer Agent (MTA) to provide in-line monitoring of Simple Mail Transfer Protocol (SMTP) mail. Email may be blocked in accordance with the established security policies.

1.4.6 Network Prevent for Web

The Network Prevent for Web component is integrated with a web proxy server using Internet Content Adaptation Protocol (ICAP). This allows the Network Prevent for Web component to detect confidential data in HTTP, HTTPS or FTP content. Policies may be established to cause the proxy to reject requests or remove the sensitive content.

The TOE is a software only TOE.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE consists of a single software package that may be installed in multiple configurations and with various licensing options. Note that all licensing options include the use of the Enforce Server component. The evaluated configuration of the TOE is Symantec DLP 14.5 installed in a two tier configuration with the following licenses:

- Network Prevent for Email
- Network Prevent for Web
- Network Discover/Cloud Storage Discover
- Network Protect
- Network Monitor
- Endpoint Discover

- Endpoint Protect

The Symantec DLP agent is made available through the licensing of the Endpoint Discover and Endpoint Protect components.

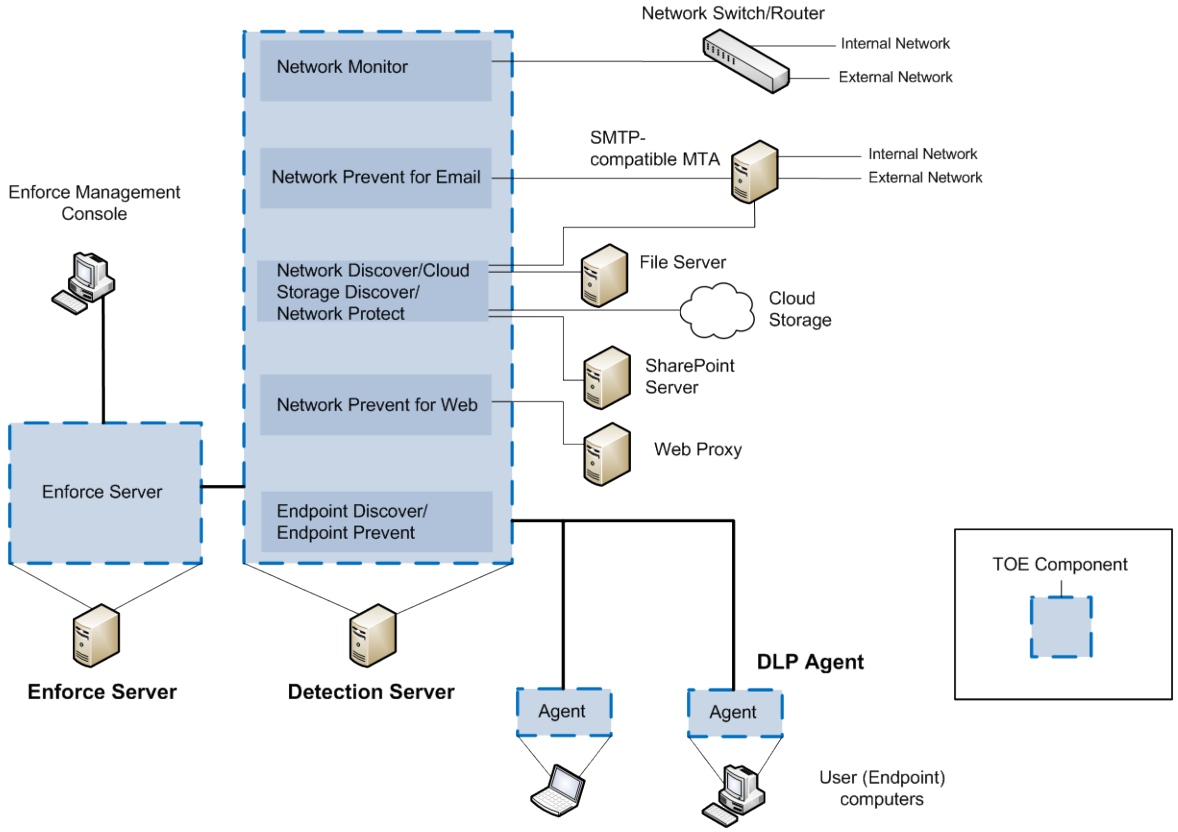

Figure 1 – TOE Boundary Diagram

1.5.2 TOE Environment

The following operating system, hardware and networking components are required to directly support the TOE components in the evaluated configuration.

TOE Component	Operating System	Hardware
Enforce Server	Windows Server 2012 R2	General purpose computing hardware
	Red Hat Enterprise Linux 7.1	General purpose computing hardware
Symantec DLP Detection Server with licenses for: • Network Prevent for Email	Windows Server 2012 R2	General purpose computing hardware
	Red Hat Enterprise Linux	General purpose

TOE Component	Operating System	Hardware
• Network Prevent for Web • Network Discover/Cloud Storage Discover • Network Protect • Network Monitor • Endpoint Discover • Endpoint Protect	7.1	computing hardware Note that the network monitor component must be installed on a system with two Network Interface Controllers (NICs).
Symantec DLP Agent	Windows 7	General purpose computing hardware
	OS X 10.11	Mac computing device

Table 1 – TOE Supporting Hardware and Software

The following components are required to be present in the operational environment in order to support the TOE in the evaluated configuration.

Non-TOE Component	Details
Enforce Management Console	The Enforce Management Console is a general purpose computing platform running a DLP-compatible browser. Firefox is used in the evaluated configuration.
Switch/Router	The network monitor component is connected to a network switch/router in order to monitor the data leaving the internal network.
MTA	In the evaluated configuration, the Network Prevent for Email component is installed in Reflecting Mode. In this mode, the Detection Server acts as an SMTP proxy that receives messages from an MTA, analyzes the messages and sends them back to the MTA. Network Discover/Cloud Storage Discover and Network Prevent scan for sensitive data on network resources, including mail servers.
File Server	Network Discover/Cloud Storage Discover and Network Prevent scan for sensitive data on network resources, including file servers. In the evaluated configuration, a Windows 2012 R2 Server acts as a file server.
SharePoint Server	Network Discover/Cloud Storage Discover and Network Prevent scan for sensitive data on network resources, including SharePoint servers. In the evaluated configuration, a Windows 2012 R2 Server with SharePoint 2013 is used.

Web Proxy	The Network Prevent for Web is supported by an ICAP compatible web proxy, situated between the Detection Server and the Internet.
Cloud Storage	Network Discover/Cloud Storage Discover scans for sensitive data on cloud storage repositories. In the evaluated configuration, Box cloud storage is used.

Table 2 – Operational Environment Supporting Hardware and Software

1.5.3 TOE Guidance

The TOE includes the following guidance documentation:

- Symantec™ Data Loss Prevention Installation Guide for Linux Version 14.5, Version 14.5a
- Symantec™ Data Loss Prevention Installation Guide for Windows Version 14.5, Version 14.5a
- Symantec™ Data Loss Prevention Administration Guide Version 14.5, Version 14.5a
- Symantec™ Data Loss Prevention Common Criteria Guidance Supplement, Version 1.0

1.5.4 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. The following breakdown also provides the description of the security features of the TOE, and loosely follows the security functional classes described in Section 6. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events.
Cryptographic Support	FIPS 140-2-validated cryptographic algorithms are provided to protect the communications links between TOE components and between the TOE and its remote administrators. Symmetric encryption is also used to protect sensitive data-at-rest.
User Data Protection	The TOE will detect and block the transfer of data identified as sensitive.

Functional Classes	Description
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. End users are prevented from removing the agent software.
Trusted Path/Channels	The communications links between the TOE and its remote administrators are protected using HTTPS (TLS 1.2).

Table 3 – Logical Scope of the TOE

1.5.5 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- Mobile Email Monitor and Mobile Prevent

Symantec DLP provides a number of mechanisms for identifying data as sensitive. For the purposes of this evaluation, keyword matching, data identifiers and Indexed Document Matching are used to demonstrate this functionality.

The following Symantec DLP data identification mechanisms are supported but not included for the purposes of this evaluation:

- Exact Data Matching
- Vector Machine Learning
- Regular expressions
- International language content
- File properties
- Enterprise Vault Data Classification
- Email subject
- Described identity matching
- Sender/recipient patterns

- Directory Group Matching

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 has to be taken into account.

2.2 ASSURANCE PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2 augmented with ALC_FLR.2 Flaw Reporting Procedures.

2.3 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 4 lists the threats addressed by the TOE. Potential threat agents are authorized TOE users, and unauthorized persons. The level of expertise of both types of attacker is assumed to be unsophisticated. TOE users are assumed to have access to the TOE, extensive knowledge of TOE operations, and to possess a high level of skill. They have moderate resources to alter TOE parameters, but are assumed not to be wilfully hostile. Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters and no physical access to the TOE.

Mitigation to the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.ACCOUNT	An unauthorized user could gain access to TOE configuration information or security management functions and use this to allow unauthorized access to information protected by the TOE.
T.AUDACC	Persons may not be held accountable for their changes to the TSF data because their actions are not recorded.
T.BYPASS	An authorized user may attempt to bypass a security mechanism resulting in disclosure of TSF data.
T.DATALEAK	An authorized user of the internal network may attempt to transmit sensitive data outside of the internal network, exposing it to unauthorized viewers.
T.DISCLOSE	An unauthorized user may be able to able to read or modify sensitive data transmitted between TOE components, or read data stored on the TOE.
T.REMOVE	An authorized user of the internal network may attempt to remove the agent software to bypass the TOE security functionality.

Table 4 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 5 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.ADMIN	The TOE shall be managed only by authorized administrators.

Table 5 – Organizational Security Policy

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 6.

Assumptions	Description
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE.
A.NOEVIL	Authorized administrators are non-hostile, appropriately trained, and follow all TOE guidance documentation.

Table 6 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.AGENT	The TOE must guard against the unauthorized removal of the agent from the endpoint.
O.AUDIT	The TOE must record use of the TOE functions, and transmission of the resources protected by the TOE.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
O.PASS	The TOE must ensure that passwords used to protect TOE access are sufficiently strong, and that a limit is placed on unsuccessful authentication attempts.
O.PROTECT	The TOE must protect organizational data identified as sensitive by detecting or blocking its transmission by network users.
O.SENDATA	The TOE must protect sensitive TSF data from disclosure and modification when transmitted between parts of the TOE or between the TOE and the administrator, and from disclosure when stored within the TOE.

Table 7 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.AUTHADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.
OE.TIMESTAMP	The operational environment will provide reliable timestamp information for the use of the TOE.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.ACCOUNT	T.AUDACC	T.BYPASS	T.DATALEAK	T.DISCLOSE	T.REMOVE	P.ADMIN	A.LOCATE	A.MANAGE	A.NOEVIL
O.ADMIN	X		X				X			
O.AGENT						X				
O.AUDIT		X	X							
O.IDENTAUTH	X		X							
O.PASS	X		X							
O.PROTECT				X						
O.SENDATA					X					

	T.ACCOUNT	T.AUDACC	T.BYPASS	T.DATALEAK	T.DISCLOSE	T.REMOVE	P.ADMIN	A.LOCATE	A.MANAGE	A.NOEVIL
OE.AUTHADMIN									X	X
OE.PHYSICAL								X		
OE.TIMESTAMP		X	X							

Table 9 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE and the Operational Environment back to the threats addressed by the TOE.

Threat: **T.ACCOUNT**	An unauthorized user could gain access to TOE configuration information or security management functions and use this to allow unauthorized access to information protected by the TOE.	
Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.PASS	The TOE must ensure that passwords used to protect TOE access are sufficiently strong, and that a limit is placed on unsuccessful authentication attempts.
Rationale:	O.ADMIN mitigates this threat by restricting the use of administrative functions to authorized users. O.IDENTAUTH helps to mitigate the threat by ensuring that only credentialed users have access to the TOE. O.PASS mitigates the threat of unauthorized access by ensuring the use of strong passwords, and a limit on the number of unsuccessful authentication attempts.	

Threat: **T.AUDACC**	Persons may not be held accountable for their changes to the TSF data because their actions are not recorded.	
Objectives:	O.AUDIT	The TOE must record use of the TOE functions, and transmission of the resources protected by the TOE.
	OE.TIMESTAMP	The operational environment will provide reliable timestamp information for the use of the TOE.
Rationale:	O.AUDIT mitigates this threat by ensuring that the audit records log the use of TOE functions, and transmission of the resources protected by the TOE. OE.TIMESTAMP mitigates the threat by ensuring that the TOE is able to make use of reliable timestamps for audit records.	

Threat: **T.BYPASS**	An authorized user may attempt to bypass a security mechanism resulting in disclosure of TSF data.	
Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.AUDIT	The TOE must record use of the TOE functions, and transmission of the resources protected by the TOE.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.PASS	The TOE must ensure that passwords used to protect TOE access are sufficiently strong, and that a limit is placed on unsuccessful authentication attempts.
	OE.TIMESTAMP	The operational environment will provide reliable timestamp information for the use of the TOE.
Rationale:	O.ADMIN mitigates this threat by ensuring that access to TSF data is protected from unauthorized use. O.AUDIT mitigates this threat by ensuring that use of TOE functions is audited, reducing the risk that bypass of security could continue undetected. O.IDENTAUTH mitigates the threat by ensuring that users must be	

	identified and authenticated in order to gain access to the TOE. O.PASS mitigates the threat of bypassing TOE security by ensuring the use of strong passwords, and a limit on the number of unsuccessful authentication attempts. OE.TIMESTAMP mitigates the threat by ensuring that the TOE is able to make use of reliable timestamps for audit records.

Threat: **T.DATALEAK**	An authorized user of the internal network may attempt to transmit sensitive data outside of the internal network, exposing it to unauthorized viewers.	
Objectives:	O.PROTECT	The TOE must protect organizational data identified as sensitive by detecting or blocking its transmission by network users.
Rationale:	O.PROTECT mitigates the threat by detecting or preventing the transmission of sensitive data.	

Threat: **T.DISCLOSE**	An unauthorized user may be able to able to read or modify sensitive data transmitted between TOE components, or read data stored on the TOE.	
Objectives:	O.SENDATA	The TOE must protect sensitive TSF data from disclosure and modification when transmitted between parts of the TOE or between the TOE and the administrator, and from disclosure when stored within the TOE.
Rationale:	O.SENDATA mitigates the threat by protecting sensitive data transmitted between parts of the TOE or between the TOE and the administrator, or stored on the TOE.	

Threat: **T.REMOVE**	An authorized user of the internal network may attempt to remove the agent software to bypass the TOE security functionality.	
Objectives:	O.AGENT	The TOE must guard against the unauthorized removal of the agent from the endpoint.
Rationale:	O.AGENT mitigates the threat by guarding against the unauthorized removal of the agent from the endpoint.	

4.3.2 Security Objectives Rationale Related to OSPs

The security objectives rationale related to OSPs traces the security objectives for the TOE back to the OSPs applicable to the TOE.

Policy: **P.ADMIN**	The TOE shall be managed only by authorized administrators.	
Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
Rationale:	O.ADMIN supports this policy by restricting access to TOE management functionality to authorized users.	

4.3.3 Security Objectives Rationale Related to Assumptions

The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, and assumptions upheld by that security objective.

Assumption: **A.LOCATE**	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE from physical attack.	

Assumption: **A.MANAGE**	There are one or more competent individuals assigned to manage the TOE.	
Objectives:	OE.AUTHADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
Rationale:	OE.AUTHADMIN supports this assumption by ensuring that trained individuals are in place to manage the TOE.	

Assumption: **A.NOEVIL**	Authorized administrators are non-hostile, appropriately trained, and follow all TOE guidance documentation.	
Objectives:	OE.AUTHADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
Rationale:	OE.AUTHADMIN supports this assumption by ensuring that the trained individuals who manage the TOE are non-hostile and follow administrative guidance.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section specifies the extended Security Functional Requirements (SFR) used in this ST. The extended component is:

FPT_PSR_EXT.1 End user software removal

5.1.1 Class FPT: PROTECTION OF THE TSF

A new family and a new SFR have been added to the Protection of the TSF class.

FPT_PSR_EXT is a new family, Prevention of software removal, and is modelled after FPT_PHP TSF physical protection. FPT_PSR_EXT.1 End user software removal is modelled after FPT_PHP.2 Notification of physical attack.

5.1.1.1 FPT_PSR_EXT Prevention of software removal

Family Behaviour

This family defines the requirements for the detection and prevention of software removal.

Component Levelling

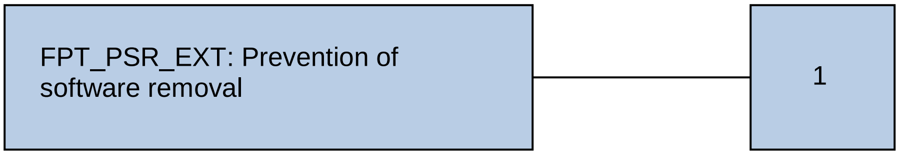

Figure 2 – FPT_PSR_EXT: Prevention of Software Removal Component Levelling

Management

There are no management activities foreseen.

Audit

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a. Minimal: Detection that the DLP Agent is not present on a designated endpoint.

5.1.1.2 FPT_PSR_EXT.1 End user software removal

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PSR_EXT.1.1 The TSF shall prevent the removal of [assignment: software component].

FPT_PSR_EXT.1.2 The TSF shall monitor the [assignment: software component] and detect that the software has been removed.

FPT_PSR_EXT.1.3 When the removal of software has been detected, the TSF shall reinstall the [assignment: software component].

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, an extended component, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 10.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
Cryptographic Support (FCS)	FCS_COP.1	Cryptographic operation
User Data Protection (FDP)	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets

Class	Identifier	Name
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PSR_EXT.1	End user software removal
Trusted path/channels (FTP)	FTP_TRP.1	Trusted path

Table 10 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*no other specifically defined auditable events*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*the cryptographic operation listed in column 1 of Table 11*] in accordance with a specified cryptographic algorithm [*listed in column 2 of Table 11*] and cryptographic key sizes [*listed in column 3 of Table 11*] that meet the following: [*standards in column 4 of Table 11*].

Operation	Algorithm	Key Size (bits)	Standard
Symmetric encryption/ decryption	AES	128, 256	FIPS 197
Asymmetric encryption/ decryption	RSA	2048	PKCS #1 v1.5

Table 11 – Cryptographic Operations

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [*DLP information flow control SFP*] on [
Subjects: Users of the internal network
Information: Content identified as sensitive
Operations: send, copy].

6.2.3.2 FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [*DLP information flow control SFP*] based on the following types of subject and information security attributes:
[*Subjects: Users of the internal network*
Subject attributes: none
Information: Content identified as sensitive
Information attributes: information identified as sensitive based on keyword matches, data identifier matches, and Indexed Document Matching].

FDP_IFF.1.2 The TSF shall permit **or deny** an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*When an attempt to send or copy information identified as sensitive outside the organization is detected, the detection server will log a record of the violation, quarantine the file, block the transfer of the data or display an on-screen notification of the violation, as configured in the response rules for that violation*].

FDP_IFF.1.3 The TSF shall enforce the [*no additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [*no additional rules*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*no additional rules*].

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [[*6*]] unsuccessful authentication attempts occur related to [*administrator logon*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lock the user out until the account is reset by an administrator*].

6.2.4.2 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to ~~individual~~ **administrative** users: [*username, role, password*].

6.2.4.3 FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [*the following rules:*

- *passwords must be at least 8 characters in length*
- *passwords must contain at least one uppercase letter*
- *passwords must contain at least one number*
- *passwords must not include more than two consecutive repeated characters*].

6.2.4.4 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.5 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MSA.1 Management of security attributes

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [*DLP information flow control SFP*] to restrict the ability to [modify, delete, [*identify*]] the security attributes [*keywords, data identifiers, indexed document content*] to [*an administrator with the 'author policies' privilege*].

Note: The DLP information flow control SFP does not control access to the security attributes used in the SFP.

Note: In the evaluated configuration, the Primary Administrator, Policy Administrator, and Policy Author roles have this privilege.

6.2.5.2 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*DLP information flow control SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Primary Administrator] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- *viewing incident information*
- *user account management*
- *policy creation and management*
- *response rule management*].

6.2.5.4 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Primary Administrator, System Administrator, User Administrator, Policy Administrator, Policy Author and Incident Responder*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

6.2.6.2 FPT_PSR_EXT.1 End user software removal

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_PSR_EXT.1.1 The TSF shall prevent the removal of [*the DLP agent software*].

FPT_PSR_EXT.1.2 The TSF shall monitor the [*the DLP agent software*] and detect that the software has been removed.

FPT_PSR_EXT.1.3 When the removal of software has been detected, the TSF shall reinstall the [*the DLP agent software*].

6.2.7 Trusted Path/Channels (FTP)

6.2.7.1 FTP_TRP.1 Trusted path

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [[*remote administration*]].

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

The following table provides a mapping between the SFRs and Security Objectives.

	O.ADMIN	O.AGENT	O.AUDIT	O.IDENTAUTH	O.PASS	O.PROTECT	O.SENDATA
FAU_GEN.1			X				
FCS_COP.1							X
FDP_IFC.1						X	
FDP_IFF.1						X	
FIA_AFL.1					X		
FIA_ATD.1				X			
FIA_SOS.1					X		
FIA_UAU.2				X			
FIA_UID.2				X			
FMT_MSA.1	X						
FMT_MSA.3	X						
FMT_SMF.1	X						
FMT_SMR.1	X						
FPT_ITT.1							X
FPT_PSR_EXT.1		X					
FTP_TRP.1							X

Table 12 – Mapping of SFRs to Security Objectives

6.3.1 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective:	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from

O.ADMIN	unauthorized use.	
Security Functional Requirements:	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Rationale:	FMT_MSA.1 provides the functionality to manage the security attributes used in the DLP information flow control SFP. FMT_MSA.3 provides the default values for the security attributes used in the DLP information flow control SFP. FMT_SMF.1 describes the security management functions required to support the claimed TOE functions. FMT_SMR.1 provides roles, which are used to restrict security management functions to authorized users.	

Objective: **O.AGENT**	The TOE must guard against the unauthorized removal of the agent from the endpoint.	
Security Functional Requirements:	FPT_PSR_EXT.1	End user software removal
Rationale:	FPT_PSR_EXT.1 ensures that the agent software cannot be easily removed, that it is detected if the software is removed, and that the software is reinstalled if it is removed.	

Objective: **O.AUDIT**	The TOE must record use of the TOE functions, and transmission of the resources protected by the TOE.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
Rationale:	FAU_GEN.1 ensures that the audit logs capture use of the TOE and actions on resources protected by the TOE.	

Objective: **O.IDENTAUTH**	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.	
Security	FIA_ATD.1	User attribute definition

Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Rationale:	FIA_ATD.1 maintains user attributes used to identify and authenticate users. FIA_UAU.2 ensures that users are authenticated before being allowed access to TOE functions. FIA_UID.2 ensures that users are identified before being allowed access to TOE functions.	

Objective: **O.PASS**	The TOE must ensure that passwords used to protect TOE access are sufficiently strong, and that a limit is placed on unsuccessful authentication attempts.	
Security Functional Requirements:	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
Rationale:	FIA_AFL.1 enforces a limit on the number of unsuccessful authentication attempts. FIA_SOS.1 ensures that strong passwords are used.	

Objective: **O.PROTECT**	The TOE must protect organizational data identified as sensitive by detecting or blocking its transmission by network users.	
Security Functional Requirements:	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Rationale:	FDP_IFC.1 and FDP_IFF.1 ensure that the transmission of sensitive information by internal network users may be detected and blocked.	

Objective: **O.SENDATA**	The TOE must protect sensitive TSF data from disclosure and modification when transmitted between parts of the TOE or between the TOE and the administrator, and from disclosure when stored within the TOE.	
Security Functional Requirements:	FCS_COP.1	Cryptographic operation
	FPT_ITT.1	Basic internal TSF data transfer protection
	FTP_TRP.1	Trusted path
Rationale:		

	FCS_COP.1 describes the cryptographic operations that are employed to protect data. FPT_ITT.1 ensures that TSF data is protected as it is transmitted between parts of the TOE. FTP_TRP.1 ensures the protection of the path between the TOE and the administrator.

6.4 DEPENDENCY RATIONALE

Table 13 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	x	The dependency is satisfied by the environment, as described by the objective OE.TIMESTAMP.
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	x	Key generation is not claimed in accordance with the guidance provided by the Canadian Common Criteria Scheme Evaluation of Cryptographic Functionality Instruction #4, July 2016
	FCS_CKM.4	x	Key destruction is not claimed in accordance with the guidance provided by the Canadian Common Criteria Scheme Evaluation of Cryptographic Functionality Instruction #4, July 2016
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FIA_AFL.1	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.
FIA_ATD.1	None	N/A	
FIA_SOS.1	None	N/A	

SFR	Dependency	Dependency Satisfied	Rationale
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_IFC.1	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied
FPT_ITT.1	None	N/A	
FPT_PSR_EXT.1	None	N/A	
FTP_TRP.1	None	N/A	

Table 13 – Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw reporting procedures (ALC_FLR.2). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.2 augmentation since there are a number of areas where current practices and procedures exceed the minimum requirements for EAL 2.

The assurance requirements are summarized in Table 14.

Assurance Class	Assurance Components	
	Identifier	Name
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification

Assurance Class	Assurance Components	
	Identifier	Name
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests (ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 14 – Security Assurance Requirements

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

7.1.1 Security Audit

Audit entries are created for events at both the Agent and the Servers. The Detection Server pulls the logs from the Agent based on the configured schedule. The logs may then be collected from the Detection Server onto the Enforce Server, where they are stored in a secure database. The logs are removed from the Detection Server once they are sent to the Enforce Server.

The logs include the date and time of the event, a description of the event, including success or failure and the name of the entity causing the event, where applicable.

TOE Security Functional Requirements addressed: FAU_GEN.1.

7.1.2 Cryptographic Support

Cryptography is used within Symantec DLP to protect sensitive data-at-rest, such as detection policies. Additionally, it is used to protect the communications between TOE components, and between the TOE and the administrator. Communication links are protected using TLS 1.2 with the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite.

Symantec DLP uses a java-based module for the Enforce Server and Detection Server components. This module is based on RSA BSAFE Crypto_J version 6.1.1.0.1, which includes algorithms validated under the Cryptographic Algorithm Validation Program. The agent uses an OpenSSL based module, which also uses FIPS-validated cryptographic algorithms. The CAVP certificate numbers are shown in Table 15.

Usage	Algorithm	CAVP Certificate Number
OpenSSL algorithms used by the agent components	HMAC DRBG for RSA	318
	AES	2397
	RSA	1240
RSA BSAFE algorithms used by the server components	HMAC DRBG for RSA	273
	AES	2249
	RSA	1154

Table 15 – Cryptographic Operations

The keys are used to encrypt sensitive files, and to support the use of TLS 1.2 protections between parts of the TOE.

TOE Security Functional Requirements addressed: FCS_COP.1.

7.1.3 User Data Protection

In order to detect sensitive data, it must first be determined what data is to be considered sensitive. Symantec DLP provides a number of mechanisms for identifying data as sensitive. For the purposes of this evaluation, keyword matching, data identifiers, and Indexed Document Matching are used to demonstrate this functionality.

Keyword matching allows matches to be made based on an identified word.

Data identifiers are algorithms that combine pattern matching with data validators to detect content. For example, the ‘Credit Card Number’ system data identifier detects numbers that match a specific pattern. The matched pattern is validated using a Luhn check algorithm. In this case, the validation is performed on the first 15 digits of the number that evaluates to equal the 16th digit. DLP supports this pattern matching for the personal identifiers used by various countries, as well as identifiers using in banking and healthcare.

Indexed Document Matching (IDM) is used to protect confidential information that is stored as unstructured data in documents and files. During the indexing process the system uses an algorithm to fingerprint each file or file contents. If a file is found to include enough of the same information, it will be considered a match.

Once a detection server has detected a policy violation, it will respond according to the response rules for that policy. For the purposes of this evaluation, the possible responses are:

- For all detection servers:
  - Log a record of the policy violation
- For Endpoint Detection
  - Quarantine a discovered sensitive file
- For Endpoint Prevent
  - Block the transfer of data that violates the policy
  - Display an on-screen notification to the endpoint user when confidential data is transferred
- For Network Prevent for Web
  - Block FTP request
  - Block HTTP/S postings
- For Network Prevent for Email
  - Block SMTP email

- For Network Protect
    - Quarantine files

TOE Security Functional Requirements addressed: FDP_IFC.1, FDP_IFF.1.

7.1.4 Identification and Authentication

For the purposes of the evaluation, Symantec DLP password authentication is used. With password authentication, the Enforce Management Console authenticates each user by determining if the supplied user name and password combination matches an active user account in the Enforce Server configuration. An active user account is authenticated if it has been assigned a valid role. When using this authentication mechanism, users enter their credentials into the Enforce Management Console's logon page and submit them over an HTTPS connection to the Enforce Server.

No functionality is available to the user prior to identification and authentication through the Enforce Management Console.

For each user, DLP maintains a username (the name that the user enters to logon to the Enforce Server), password hash and a list of roles. A user may have more than one role; each user must have at least one role to be allowed to logon to the Enforce Server.

A user is locked out after six unsuccessful logon attempts. The user is locked out until an administrator re-enables the account by deselecting the 'Account Disabled' option on the user's account information. (Note that this is the default behavior. An administrator may configure lockout after any number of unsuccessful login attempts.)

In the evaluated configuration, strong passwords are used. The use of strong passwords is set under the General System Settings, and once configured requires that passwords be at least eight characters in length, contain at least one number and at least one uppercase letter. Strong passwords cannot have more than two consecutive repeated characters.

TOE Security Functional Requirements addressed: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2.

7.1.5 Security Management

The default attributes used in the DLP information flow control SFP are permissive. No information is identified as sensitive prior to an administrator doing so. The administrator identifies information as sensitive based on keywords, data identifiers and indexed document content. Administrators are able to identify, modify and delete keywords, identifiers and indexed document content. It should be noted that the administrator does not modify the document content itself, but controls which content is indexed. Only administrators with the 'author policies' privilege are able to perform this function. This default functionality may not be changed.

Symantec DLP includes many preconfigured roles, as well as the option to create custom roles. This provides very fine grained access control of the DLP functionality. In the evaluated configuration, the System Administrator, User Administrator, Policy Administrator, Policy Author and Incident Responder roles are implemented. Additionally, an Administrator account (called Administrator) is created during installation. This account has all system privileges and role options do not apply. For the purposes of this evaluation, this account will be referred to as the Primary Administrator.

TOE Security Functional Requirements addressed: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1.

7.1.6 Protection of the TSF

Data that travels between the DLP Agent and the Detection Server, and between the Detection Server and the Enforce Server is protected using TLS 1.2. TLS 1.2 is implemented in the DLP Agent using an OpenSSL based module which uses FIPS-validated cryptographic algorithms. TLS 1.2 is implemented in the Enforce Server and Detection Server using a java module which also uses FIPS-validated cryptographic algorithms. The TLS connections use the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite by default, but this may be changed to use another TLS 1.2 supported ciphersuite. The TLS connection protects the TSF data from disclosure and modification as it passes between the TOE components.

The DLP agent software invokes both an agent service and a watchdog service on the endpoint. As a tamper-proofing measure, it is not possible for a user to individually stop either the DLP Agent or watchdog service. The agent does not appear on the Add or Remove Programs list, in Windows; Mac users must have sudo privileges in order to uninstall the agent. These measures are most effective in organizations that do not give administrator privileges to their endpoint users. The Detection Server monitors the agent, and if it does not respond, it is identified as non-reporting. The Detection Server will attempt to push the agent software to the endpoint at the next opportunity, and the event will be logged.

TOE Security Functional Requirements addressed: FPT_ITT.1, FPT_PSR_EXT.1.

7.1.7 Trusted Path/Channels

Data that travels between the Enforce Server and the administrator using the Enforce Management Console is protected using TLS 1.2. TLS 1.2 is implemented in the Enforce Server using FIPS-validated cryptographic algorithms. The TLS connection uses the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite by default, but this may be changed to another TLS 1.2 supported ciphersuite. The TLS connection protects the TSF data from disclosure and modification as it passes between the TOE components. The administrator is assured of the end point by entering the known URL of the Enforce Server. The Enforce Server is assured of the user's identity by the username and password presented at login. Only the administrator may initiate a session.

TOE Security Functional Requirements addressed: FTP_TRP.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Administrator	An administrator is any user with administrative privileges. A user in any role with access to the Enforce Management Console is considered to be an administrator.
Primary Administrator	This is the administrative user account created during DLP installation. This account has full system privileges.
Security policy	The term 'security policy' is used in this ST to describe the policies implemented within the DLP product to enforce the claimed functionality. It does not refer to the specific policies enforced by FDP_IFC.1 and FDP_IFF.1.

Table 16 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
ANSI	American National Standards Institute
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CLI	Command Line Interface
DES	Data Encryption Standard
DLP	Data Leak Prevention
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICAP	Internet Content Adaptation Protocol

Acronym	Definition
IDM	Indexed Document Matching
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IT	Information Technology
MS Exchange	Microsoft Exchange
MTA	Mail Transfer Agent
NIC	Network Interface Controller
NTP	Network Time Protocol
PKCS	Public-Key Cryptography Standards
PP	Protection Profile
RSA	Rivest, Shamir and Adleman
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
USB	Universal Serial Bus

Table 17 – Acronyms