Security Target

Symantec™ Data Loss Prevention 11.1.1

Document Version 1.0

January 23, 2012

Prepared For:

Symantec Corporation

350 Ellis Street

Mountain View, CA 94043-2202

www.symantec.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Data Loss Prevention Version 11.1. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

1 Introduction 6
1.1 ST Reference 6
1.2 TOE Reference 6
1.3 Document Organization 6
1.4 Document Conventions 7
1.5 Document Terminology 7
1.6 TOE Overview 8
1.6.1 Enforce Server 9
1.6.2 Network Discover/Network Protect 9
1.6.3 Network Monitor/Network Prevent 10
1.6.4 Endpoint Discover/Endpoint Prevent/DLP Agent 10
1.6.5 TOE Description 11
1.6.6 Physical Boundary 11
1.6.7 Hardware and Software Supplied by the IT Environment 12
1.6.8 Logical Boundary 13
1.6.9 TOE Guidance Documentation 14

2 Conformance Claims 15
2.1 Common Criteria Conformance Claim 15
2.2 Protection Profile Conformance Claim 15

3 Security Problem Definition 16
3.1 Threats 16
3.2 Organizational Security Policies 16
3.3 Assumptions 17

4 Security Objectives 18
4.1 Security Objectives for the TOE 18
4.2 Security Objectives for the Operational Environment 18
4.3 Security Objectives Rationale 19

5 Extended Components Definition 23

6 Security Requirements 24
6.1 Security Functional Requirements 24
6.1.1 Security Audit (FAU) 24
6.1.2 Information Flow Control (FDP) 25
6.1.3 Identification and Authentication (FIA) 28
6.1.4 Security Management (FMT) 29
6.2 Security Assurance Requirements 30
6.3 CC Component Hierarchies and Dependencies 30
6.4 Security Requirements Rationale 31
6.4.1 Security Functional Requirements for the TOE 31
6.4.2 Security Assurance Requirements 33
6.5 TOE Summary Specification Rationale 34

7 TOE Summary Specification 36

7.1 TOE Security Functions *36*
7.1.1 Security Audit 36
7.1.2 Identification and Authentication 37
7.1.3 Security Management 37
7.1.4 Policy Enforcement 38

List of Tables

Table 1 – ST Organization and Section Descriptions 6
Table 2 – Terms and Acronyms Used in Security Target 8
Table 3 – Evaluated Configuration for the TOE 11
Table 4 – Hardware and Software Requirements for the TOE and IT Environment 13
Table 5 – Logical Boundary Descriptions 14
Table 6 – Threats Addressed by the TOE 16
Table 7 – Organizational Security Policies 17
Table 8 – Assumptions 17
Table 9 – TOE Security Objectives 18
Table 10 – Operational Environment Security Objectives 19
Table 11 – Mapping of Assumptions, Threats, and OSPs to Security Objectives 19
Table 12 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives 22
Table 13 – TOE Functional Components 24
Table 14 – Audit Events and Details 25
Table 15 – Roles and Privileges 29
Table 16 – Security Assurance Requirements at EAL2 30
Table 17 – TOE SFR Dependency Rationale 31
Table 18 – Mapping of TOE SFRs to Security Objectives 32
Table 19 – Rationale for Mapping of TOE SFRs to Objectives 33
Table 20 – Security Assurance Measures 33
Table 21 – SFR to TOE Security Functions Mapping 34
Table 22 – SFR to TSF Rationale 35
Table 23 – Typical TOE Roles and Permissions 38

List of Figures

Figure 1 – TOE Boundary 12

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: Symantec Data Loss Prevention Version 11.1.1
ST Revision	1.0
ST Publication Date	November 16, 2011
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	Symantec Data Loss Prevention Version 11.1.1000.10054

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in italics, i.e. *assignment_value(s).*
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_UAU.1.1 (1) and FIA_UAU.1.1 (2) refer to separate instances of the FIA_UAU.1 security functional requirement component.

Italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the terms and acronyms used in this document:

TERM	DEFINITION
AES	Advanced Encryption Standard
AIM	AOL Instant Messenger
CC	Common Criteria
CD	Compact Disc
CF	Compact Flash
CIFS	Common Internet File System
CM	Configuration Management
CSV	Comma-separated values
DCM	Described Content Matching
DGM	Directory Group Matching
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DVD	Digital Versatile Disk
EAL	Evaluation Assurance Level

TERM	DEFINITION
EDM	Exact Data Matching
Exec	Executive
FTP	File Transfer Protocol
GUI	Graphical User Interface
ID	Identification
IDM	Indexed Document Matching
ISM	InfoSec Manager
HRM	Human Resources Manager
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IM	Instant Message
IP	Internet Protocol
ISM	InfoSec Manager
ISR	InfoSec Responder
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MSN	Microsoft Network
MTA	Mail Transfer Agent
NNTP	Network News Transfer Protocol
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SCSI	Small Computer System Interface
SD	Secure Digital
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
USB	Universal Serial Bus
URL	Uniform Resource Locator
VML	Vector Machine Learning

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

Symantec's Data Loss Prevention Suite enables organizations to safeguard customer data, company information, intellectual property, and other sensitive or classified information. DLP mitigates an

organization's risk of data compromise by providing for the discovery, monitoring, and protection of confidential or sensitive information wherever it might exist within an organization's IT infrastructure. Sensitive data can include credit card numbers, names, addresses, identification numbers or any data a company deems proprietary. Symantec's DLP solution enables an organization to:

- Discover and locate confidential information on file and Web servers, databases, and endpoints
- Monitor network traffic for transmission of confidential data
- Monitor the use of sensitive data on managed computers
- Prevent transmission of confidential data to outside locations
- Enforce data security and encryption policies
- Protect confidential information through quarantine

Using the Web-based central management console, sensitive data is identified and then secured regardless of its location or point of egress, be it the network, a removable storage device, endpoints (desktop and laptop systems), or other data repositories. DLP discovers exposed confidential data through a combination of deployed agents and scanning capabilities. DLP collects information via deployed DLP Agents and Servers. Once a violation is discovered, DLP takes action to protect the data as well as report on any violations that have occurred.

In order to provide the broad spectrum of services provided by DLP while maintaining scalability, DLP has multiple components which can either run on a single server or can be deployed in a distributed manner to support higher performance. DLP includes the following components as described below.

1.6.1 Enforce Server

The Enforce Server is the central management component of the Symantec DLP Suite. It provides a web-based GUI that serves as the management console for all Symantec DLP products. The Enforce Server administration console can be accessed from any workstation with a web browser that has access to the DLP Enforce Platform Server.

Through the administration console, authorized administrators create data loss policies for automatically detecting and protecting sensitive data, perform incident workflow and remediation, generate reports, and configure role-based access and system management options. Additionally the Enforce Server enables administrators to automatically enforce an organization's data security policies by pushing policies out to all other DLP components.

1.6.2 Network Discover/Network Protect

Network Discover scans networked file shares, Web content servers, databases, document repositories, and endpoint systems at high speeds to detect exposed data and documents. Network Discover enables companies to understand exactly where confidential data is exposed. Network Protect is an application that sits on the Network Discover Server and adds protection functionality to the Network Discover Server. Network Protect reduces risk by removing exposed confidential data, intellectual property, and classified information from open file shares on network servers or desktop computers.

1.6.3 Network Monitor/Network Prevent

Network Monitor accurately detects confidential information across configured network protocols and content types before it leaves the network. Real-time monitoring and reporting deliver constant visibility on data security. Network Monitor Servers gather network traffic from scanned ports or taps, and reports on private or proprietary data leaking as it moves across the network. This gathered data is then analyzed. The Enforce Server defines the policy groups, protocols, and protocol filters that control the Network Monitor Servers. The incidents that servers find are organized into reports, alerts, and actions on the Enforce Server. A network of Network Monitor Servers can be deployed on the company network to report on network activity and policy compliance. Network Monitor Servers can enforce a uniform set of policies or specialized policies based on the location and purpose of the server. Network Monitor gives organizations the ability to monitor all network communications, including:

- Email
- Instant messaging
- Web mail and Web postings
- File transfers
- Network news
- Peer-to-peer
- Telnet
- All other TCP sessions through any port.

Network Prevent proactively stops data loss through email and Web communications. Network Prevent integrates with existing email message chain and Web infrastructure technologies to capture network communications and block those transmissions that contain confidential data. Network Prevent blocks email, Web (HTTP/HTTPS), and FTP communications that contain confidential data.

1.6.4 Endpoint Discover/Endpoint Prevent/DLP Agent

The Endpoint Server is comprised of Endpoint Discover and Endpoint Prevent. The Endpoint Server manages the DLP Agents which are installed on endpoint desktops and laptops. Endpoint Discover detects sensitive data on desktop or laptop endpoint computers. It consists of at least one Endpoint Server and at least one Symantec DLP Agent that runs on a managed device. The Agent collects the specified data and sends incidents back to the Endpoint Server for analysis. In addition, Endpoint Discover allows for the quarantine of confidential files to a secure location.

Endpoint Prevent detects and prevents sensitive data from moving from a managed device with the DLP Agent installed on it also known as an endpoint computer. It consists of at least one Endpoint Server and all the Symantec DLP Agents running on the endpoint computers that are connected to it. Endpoint Prevent detects sensitive data on the following data transfers:

- Removable media devices
- IM
- HTTP/HTTPS

- Email/SMTP
- FTP
- CD/DVD
- Print/Fax
- Clipboard

The Network or Endpoint Discover, Protect, Monitor, and Prevent Servers can be installed as stand-alone products or in combination. Regardless of which stand-alone products an authorized administrator deploys, the Enforce Server is always the central management component of the DLP Suite.

1.6.5 TOE Description

The TOE is comprised of the DLP software only. Table 4 – Hardware and Software Requirements for the TOE and IT Environment identifies any major non-TOE hardware and software that is required by the TOE including the TOE minimum requirements.

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 it is then secured, whether it is exiting the network, being copied to a removable storage device, or being stored on workstations or data repositories. A typical deployment includes at least one of each TOE components as described in Section 1.6. To support the understanding of Figure 1, the following list provides a brief description of each major component:

- The Enforce Server provides a centralized administration console that allows an authorized administrator to manage the entire TOE.
- The Endpoint Server is comprised of Endpoint Discover and Endpoint Prevent. 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 secured corporate LAN or target network.
- The Network Monitor/Network Prevent Server sits on the DMZ scanning network traffic and preventing sensitive data from leaving the target network.

1.6.6 Physical Boundary

The TOE is a software TOE and is defined as the Data Loss Prevention Version 11.1. In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	Data Loss Prevention Version 11.1
IT Environment	Workstations meeting the requirements specified in Table 4 – Hardware and Software Requirements for the TOE

Table 3 – Evaluated Configuration for the TOE

The TOE boundary is shown below:

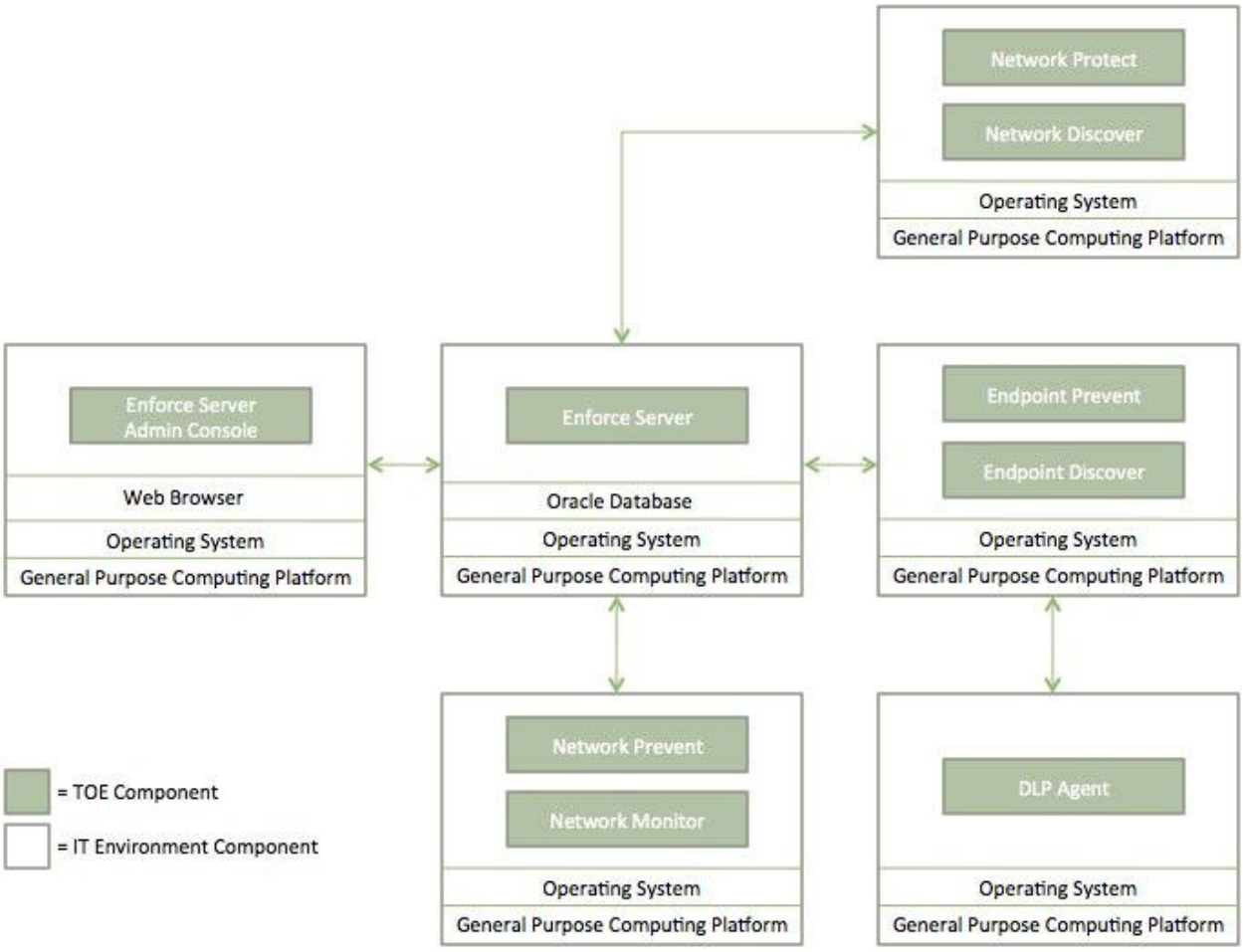

Figure 1 – TOE Boundary

Note: TOE components are described in Section 1.6 - TOE Overview.

1.6.7 Hardware and Software Supplied by the IT Environment

The TOE is a software-only TOE. The following table identifies the minimum hardware and software requirements for components provided by the IT Environment:

Component	Minimum Requirement
Enforce Server and Enforce Server Admin Console Hardware	2x3.0 GHz or faster processor, 6-8 GB or more Random Access Memory, with at least 500 GB hard drive space

Component	Minimum Requirement
Enforce Server and Enforce Server Admin Console Software	• Microsoft Windows Server 2003, Enterprise Edition (32-bit) with Service Pack 2 or later • Microsoft Windows Server 2008 R2, Enterprise Edition (64-bit) or later • Red Hat Enterprise Linux 5 (32-bit or 64-bit) Update 2 or later
Network Discover Hardware Network Monitor Hardware Network Prevent Hardware Network Protect Hardware Endpoint Discover Hardware Endpoint Prevent Hardware	2x3.0 GHz or faster processor, 6-8 GB or more Random Access Memory, with at least 140 GB hard drive space
Network Discover Software Network Monitor Software Network Prevent Software Network Protect Software Endpoint Discover Software Endpoint Prevent Software	• Microsoft Windows Server 2003, Enterprise Edition (32-bit) with Service Pack 2 or later • Microsoft Windows Server 2008 R2, Enterprise Edition (64-bit) or later • Red Hat Enterprise Linux 5 (32-bit or 64-bit) Update 2 or later
Endpoint / DLP Agent Hardware	General Purpose Computing Platform
Endpoint / DLP Agent Software	• Microsoft Windows Server 2003 (32-bit) with Service Pack 2 or Windows Server 2003 R2 (32-bit) • Microsoft Windows XP Professional with Service Pack 3 (32-bit) • Microsoft Windows Vista Enterprise or Business with Service Pack 1 or Service Pack 2 (32-bit) • Microsoft Windows 7 Enterprise, Professional, or Ultimate (32-bit or 64-bit)
Other software	• WinPcap 4.1.1 or higher • Java Runtime Environment (JRE) All servers 1.6.0_14 or higher • Apache Tomcat version 5.5.27 or higher • Oracle Database 11g version 11.2 (32-bit or 64-bit) or Oracle 10g database version 10.2.0.4 (32-bit only) with the most recent Critical Patch Update. • Microsoft Internet Explorer 7.x or 8.x • Mozilla Firefox 3.x

Table 4 – Hardware and Software Requirements for the TOE and IT Environment

1.6.8 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Security Audit	The TOE generates audit records for the actions of the DLP Components. The security relevant Administrator actions within the DLP Admin Console are audited.
Identification and Authentication	The TOE provides functionality to allow administrators to verify their claimed identity. The Identification and Authentication TSF ensures that only

TSF	DESCRIPTION
	legitimate administrators can gain access to the configuration settings and management settings of the TOE. Administrators must log in with a valid user name and password before the server will permit the administrators to manage the TOE.
Security Management	The TOE provides a set of commands for administrators to manage the security functions, configuration, and other features of the DLP Server components. The Security Management function specifies user roles with defined access for the management of the TOE components.
Policy Enforcement	The TOE scans endpoint computers to find the information that an authorized administrator has defined as sensitive. The TOE prevents sensitive data from moving off of an endpoint computer. The TOE reports an incident when it detects data that matches the detection parameters of a policy rule.

Table 5 – Logical Boundary Descriptions

1.6.9 TOE Guidance Documentation

The following guidance documentation is provided as part of the TOE:

- Symantec Data Loss Prevention System Requirements and Compatibility Guide
- Symantec Data Loss Prevention Install Guide
- Symantec Data Loss Prevention Administration Guide

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 conformant and Part 3 conformant at Evaluation Assurance Level 2 augmented with ALC_FLR.2 – Flaw Reporting.

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data

Table 6 – Threats Addressed by the TOE

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION

POLICY	DESCRIPTION
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.
P.SENSITIVE_DATA	The TOE shall enforce security policies on transmission of sensitive files or data.

Table 7 – Organizational Security Policies

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.ACCESS	The TOE has access to all the IT resources it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT Systems the TOE monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

Table 8 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCESS	The TOE must allow authorized users to access only authorized TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions on the management system.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDENTIFY	The TOE must be able to identify users prior to allowing access to TOE functions and data on the management system.
O.INTEGRITY	The TOE must ensure the integrity of all TOE data.
O.SENSITIVE_DATA	The TOE shall take specified actions upon transmission of identified sensitive files or data.

Table 9 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTALL	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.
OE.INTEROP	The TOE is interoperable with the managed systems it monitors
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.AUDIT_PROTECT	The IT Environment will provide the capability to protect audit information generated by the TOE via mechanisms outside the TSC.
OE.AUDIT_REVIEW	The IT Environment will provide the capability for authorized administrators to review audit information generated by the TOE.
OE.CRYPTO	The IT Environment will provide the cryptographic functionality and protocols required for the TOE to securely transfer information between distributed portions of the TOE.
OE.DATABASE	Those responsible for the TOE must ensure that access to the database via mechanisms outside the TOE boundary (e.g., DBMS) is restricted to authorized users only.

OBJECTIVE	DESCRIPTION
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect TOE data via mechanisms outside the TSC.
OE.STORAGE	The IT Environment will store TOE data in the database and retrieve it when directed by the TOE.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE

Table 10 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable). The following table provides a high level mapping of coverage for each threat, assumption, and policy:

OBJECTIVE / THREAT / ASSUMPTION	O.EADMIN	O.ACCESS	O.IDENTIFY	O.INTEGRITY	OE.INSTALL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTEROP	O.AUDITS	O.SENSITIVE_DATA	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.DATABASE	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.CRYPTO	OE.STORAGE
A.ACCESS									✓										
A.ASCOPE									✓										
A.DATABASE															✓				
A.DYNMIC								✓	✓										
A.LOCATE						✓													
A.MANAGE								✓											
A.NOEVIL					✓	✓	✓												
A.PROTCT						✓													
P.ACCACT			✓							✓							✓		
P.ACCESS		✓	✓											✓	✓				
P.INTEGRITY				✓								✓				✓		✓	✓
P.MANAGE	✓	✓	✓		✓		✓	✓											
P.PROTCT						✓							✓					✓	✓
T.COMDIS		✓	✓										✓						
T.COMINT		✓	✓	✓									✓						
T.IMPCON	✓	✓	✓		✓														
T.LOSSOF		✓	✓	✓															
T.NOHALT		✓	✓																
T.PRIVIL		✓	✓																
P.SENSITIVE_ DATA											✓								

Table 11 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

The following table provides detailed evidence of coverage for each threat, policy, and assumption:

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.ACCESS	The TOE has access to all the IT resoiurces it needs to perform its functions. The OE.INTEROP objective ensures the TOE has the needed access.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors. The OE.INTEROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users. The OE.DATABASE objective ensures that access to any mechanisms outside the TOE boundary that may be used to access the database is configured by the administrators such that only authorized users may utilize the mechanisms.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors. The OE.INTEROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will managed appropriately.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OE.INSTALL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The OE.PHYCAL provides for the physical protection of the hardware and software.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDENTIFY objective supports this objective by ensuring each user is uniquely identified. The OE.AUDIT_REVIEW objective provides the ability for administrators to review the audit records generated by the TOE so that accountability for administrator actions can be determined.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses via the web interface. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions. The OE.SD_PROTECTION and OE.DATABASE objectives support this policy for mechanisms outside the TSC via IT Environment protections of the TOE data. The OE.SD_PROTECTION and O.ACCESS objectives support this policy for mechanisms inside the TSC via TOE protections of the TOE data.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGRITY objective ensures the protection of TOE data from modification. The OE.AUDIT_PROTECT objective ensures the integrity of audit records in the database generated by the TOE using access mechanisms outside the TSC respectively. The OE.CRYPTO objective requires the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit. The OE.STORAGE objective requires the IT Environment to provide storage and retrieval mechanisms for TOE data for use by the TOE. The OE.TIME objective supports this policy by providing a time stamp for insertion into the TOE data records.
P.MANAGE	The TOE shall only be managed by authorized users. The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTALL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment. The OE.CRYPTO objective requires the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit. The OE.STORAGE objective requires the IT Environment to provide storage and retrieval mechanisms for TOE data for use by the TOE.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The OE.PROTECT objective supports the TOE protection from the IT Environment.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The O.INTEGRITY objective ensures no TOE data will be modified. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The OE.INSTALL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The O.INTEGRITY objective ensures no TOE data will be deleted.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.
P.SENSITVE_DATA	The TOE shall enforce security policies on transmission of sensitive files or data.The O.SENSITIVE_DATA objective requires the TOE to take specified actions upon the transmission of identified sensitive files or data.

Table 12 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

This Security Target does not include any extended components.

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
Information Flow Control	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.1	Timing of Authentication
	FIA_UID.1	Timing of Identification
	FIA_SOS.1	Verification of Secrets
Security Management	FMT_MTD.1	Management of TSF Data
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 13 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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) *The events identified in* Table 14 – Audit Events and Details.

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, *the information detailed in* Table 14 – Audit Events and Details.

Application Note: The auditable events for the (not specified) level of auditing are included in the following table:

COMPONENT	EVENT	DETAILS
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to the TOE and TOE data	Object IDs, Requested access
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FIA_ATD.1	All changes to TSF data (including passwords) result in an audit record being generated. Note that passwords are not configured, so no audit records for rejection of a tested secret will be generated.	
FIA_UAU.1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions.	User identity, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 14 – Audit Events and Details

6.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.2 Information Flow Control (FDP)

6.1.2.1 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the *DLP Information Flow Control SFP* on

Subjects: External IT entities attempting to transfer or transmit identified sensitive data

Information: Files and content stored on the managed system or transferred from the managed system

Operations:

Endpoint Discover Component:

- *Sends incidents to the Endpoint Server.*
- *Sends the associated incident data to the Endpoint Server for analysis.*
- *Quarantine File*

Endpoint Prevent Component:

- *Block*
- *User Cancel*
- *Notify*
- *Quarantine*

Network Monitor/Network Prevent Component:

- *Identify sensitive network content*
- *Block SMTP Message*
- *Modify SMTP Message*
- *Remove HTTP/HTTPS Content*
- *Block HTTP/HTTPS Content*
- *Block FTP Request*

Network Discover/Network Protect Component:

- *Identify sensitive files*
- *Quarantine File*
- *Copy File.*

6.1.2.2 FDP_IFF.1 – Simple Security Attributes

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:

Subject Security Attributes:

- *Monitoring enabled / disabled*

Information security attributes

- *Content*
    - *For matches based on exact content from profiled structured data (database, CSV); exact document content from profiled documents; similar document content from profiled documents; described content, message context, and identity patterns; exact identities from synchronized or profiled directory server (LDAP); and any unique data defined by extending detection capabilities],*
- *Data transfer type*
    - *Removable media devices, IM, HTTP/HTTPS, Email, FTP, CD/DVD, Print/Fax, Clipboard data] and protocol signature [Email (SMTP), Web (HTTP), File Transfer (FTP), Newsgroups (NNTP), TCP, Telnet and SSL*

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

A. Monitoring option is enabled for the service and information structure type and:

1. *The attribute is not covered by policy*
2. *The attribute is assigned an action of "notify" via policy*

Or

B. DLP monitoring is disabled for the subject and information structure type.

Or

C. No response rule is configured.

FDP_IFF.1.3 The TSF shall enforce ~~the~~ *no other additional rules.*

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: *No explicit authorization rules*.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *No explicit denial rules*.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) User name;

b) Authentication data;

c) *Permission Sets.*

6.1.3.2 FIA_SOS.1 Verification of secrets

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

- *must contain:*
  - *at least eight characters;*
  - *at least one number;*
  - *and at least one uppercase letter;*
- *and cannot have more than two repeated characters in succession.*

6.1.3.3 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.4 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to *perform the functions in the table below* to *the respective roles in the table below*.

ROLE	ABILITY
• System Administrator, Limited Administrator	• Add/remove user/group to a role • Create, edit, delete role • View, edit user name, password, role, DLP Information Flow Control SFP parameters • View reports • Configure TOE (Create Server, Discover Targets for Scanning)
• Incident Responder, Limited Administrator	• View, remediate, and delete incidents
• User Administrator, Limited Administrator	• Add/remove user/group to a role • Create, edit, delete role
• Policy Administrator, Limited Administrator	• Add/remove user/group to a policy management role
• Policy Author, Limited Administrator	• View, create policies/policy groups

Table 15 – Roles and Privileges

6.1.4.2 FMT_MSA.1 - Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the *DLP Information Flow Control SFP* to restrict the ability to *change_default, query, modify, and delete* the security attributes *defined in FDP_IFF.1.1* to *the System Administrator*.

6.1.4.3 FMT_MSA.3 – Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the *DLP Information Flow Control SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

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

6.1.4.4 FMT_SMF.1 Specification of Management Functions

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

a) User Account management

b) Incident management

c) DLP Policy and Rule management.

6.1.4.5 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: *System Administrator, Incident Responder, User Administrator, Policy Administrator, Policy Author, Limited Administrator.*

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

6.2 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) augmented by ALC_FLR.2. The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	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
ASE: Security Target Evaluation	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
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 16 – Security Assurance Requirements at EAL2

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components	FPT_STM.1	Satisfied by OE.TIME in the environment
FAU_GEN.2	No other components	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied
FDP_IFC.1	No other components	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components	FDP_IFC.1 FMT_MSA.3	Satisfied Satisfied
FIA_ATD.1	No other components	None	n/a
FIA_UAU.1	No other components	FIA_UID.1	Satisfied
FIA_UID.1	No other components	None	n/a
FIA_SOS.1	No other components	None	n/a
FMT_MTD.1	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_MSA.1	No other components	FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied Satisfied
FMT_MSA.3	No other components	FMT_MSA.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components	None	n/a
FMT_SMR.1	No other components	FIA_UID.1	Satisfied

Table 17 – TOE SFR Dependency Rationale

6.4 Security Requirements Rationale

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

6.4.1 Security Functional Requirements for the TOE

The following table provides a high level mapping of coverage for each security objective:

SFR \ OBJECTIVE	O.ACCESS	O.AUDITS	O.EADMIN	O.IDENTIFY	O.INTEGRITY	O.SENSITIVE_DATA
FAU_GEN.1		✓				
FAU_GEN.2		✓				
FDP_IFC.1						✓
FDP_IFF.1						✓
FIA_ATD.1				✓		
FIA_UID.1	✓			✓		
FIA_UAU.1	✓			✓		
FIA_SOS.1	✓			✓		

SFR \ OBJECTIVE	O.ACCESS	O.AUDITS	O.EADMIN	O.IDENTIFY	O.INTEGRITY	O.SENSITIVE_DATA
FMT_MTD.1	✓		✓		✓	
FMT_MSA.1	✓					
FMT_MSA.3	✓					
FMT_SMF.1	✓		✓			
FMT_SMR.1	✓		✓			

Table 18 – Mapping of TOE SFRs to Security Objectives

The following table provides detailed evidence of coverage for each security objective:

OBJECTIVE	RATIONALE
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. Users authorized to access the TOE are determined using an identification and authentication process [FIA_UAU.1, FIA_UID.1]. The permitted access to TOE data by the roles and permissions is defined [FMT_MTD.1, FMT_SMF.1]. The TOE specifies metrics for password complexity in authentication (FIA_SOS.1). The management of security attirubtes is restricted (FMT_MSA.1.) The default values of security attributes are restrictive in nature (FMT_MSA.3).
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions on the management system. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The user associated with the events must be recorded [FAU_GEN.2].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The functions and roles required for effective management are defined [FMT_SMF.1, FMT_SMR.1], and the specific access privileges for the roles and permissions is enforced [FMT_MTD.1].
O.IDENTIFY	The TOE must be able to identify users prior to allowing access to TOE functions and data on the management system. Security attributes of subjects used to enforce the security policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are determined using a identification process of a username/password combination [FIA_UID.1 and FIA_UAU.1]. The TOE specifies metrics for password complexity in authentication (FIA_SOS.1).
O.INTEGRITY	The TOE must ensure the integrity of all TOE data. Only authorized administrators of the System may query or add TOE data [FMT_MTD.1].

OBJECTIVE	RATIONALE
O.SENSITIVE_DATA	The TOE shall take specified actions upon transmission of sensitive files or data. The TOE implements data classification to identify/track sensitive data and Protection Rules to act when sensitive data is transmitted inappropriately [FDP_IFC.1 and FDP_IFF.1].

Table 19 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Assurance Requirements

This section identifies the Configuration Management, Delivery/Operation, Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: Symantec Data Loss Prevention Version 11.1
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: Symantec Data Loss Prevention Version 11.1
ADV_TDS.1: Basic Design	Basic Design: Symantec Data Loss Prevention Version 11.1
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Symantec Data Loss Prevention Version 11.1
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Symantec Data Loss Prevention Version 11.1
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: Symantec Data Loss Prevention Version 11.1
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: Symantec Data Loss Prevention Version 11.1
ALC_DEL.1: Delivery Procedures	Delivery Procedures: Symantec Data Loss Prevention Version 11.1
ALC_FLR.2: Flaw Reporting	Flaw Reporting: Symantec Data Loss Prevention Version 11.1
ATE_COV.1: Evidence of Coverage	Security Testing: Symantec Data Loss Prevention Version 11.1
ATE_FUN.1: Functional Testing	Security Testing: Symantec Data Loss Prevention Version 11.1
ATE_IND.2: Independent Testing – Sample	Provided by CCTL

Table 20 – Security Assurance Measures

6.4.2.1 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
2. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.
3. Consistent with current best practice for tracking and fixing flaws as well as providing fixes to customers.

6.5 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

SFR \ TSF	Policy Enforcement	Identification and Authentication	Security Management	Audit
FAU_GEN.1				✓
FAU_GEN.2				✓
FDP_IFC.1	✓			
FDP_IFF.1	✓			
FIA_ATD.1			✓	
FIA_UID.1		✓		
FIA_UAU.1		✓		
FIA_SOS.1		✓		
FMT_MTD.1			✓	
FMT_MSA.1			✓	
FMT_MSA.3			✓	
FMT_SMF.1			✓	
FMT_SMR.1			✓	

Table 21 – SFR to TOE Security Functions Mapping

SFR	TSF AND RATIONALE
FAU_GEN.1	**Audit –** User actions area audited according to the events specified in the table with the SFR.

SFR	TSF AND RATIONALE
FAU_GEN.2	**Audit –** The audit log records include the associated user name when applicable.
FDP_IFC.1	**Policy Enforcement** – The TOE implements data classification to identify/track sensitive data and Protection Rules to act when sensitive data is transmitted or transferred inappropriately.
FDP_IFF.1	**Policy Enforcement** – The TOE implements data classification to identify/track sensitive data and Protection Rules to act when sensitive data is transmitted or transferred inappropriately.
FIA_ATD.1	**Security Management** – User security attributes are associated with the user account via User Account management.
FIA_UID.1	**Identification and Authentication** – The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FIA_UAU.1	**Identification and Authentication** – The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FIA_SOS.1	**Identification and Authentication** – The TSF places strict requirements on password complexity.
FMT_MTD.1	**Security Management** – The Administrator status and user permissions determine the access privileges of the user to TOE data.
FMT_MSA.1	**Security Management** – The TOE ensures the access to the security attributes are restricted as to enforce the access control policy for the TOE.
FMT_MSA.3	**Security Management** – The TOE ensures the default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE.
FMT_SMF.1	**Security Management** – The management functions that must be provided for effective management of the TOE are defined and described.
FMT_SMR.1	**Security Management** – The TOE provides the roles specified in the SFR. When a User Account is created or modified, the role is specified by setting or clearing the Administrator status for the user.

Table 22 – SFR to TSF Rationale

7 TOE Summary Specification

7.1 TOE Security Functions

The security functions described in the following subsections fulfill the security requirements that are defined in Section 6.1 – Security Functional Requirements. The security functions performed by the TOE are as follows:

- Security Audit
- Identification and Authentication
- Security Management
- Policy Enforcement

7.1.1 Security Audit

Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The resulting audit records can be examined to determine which security-relevant activities took place and who (i.e., which user) is responsible for those activities.

Symantec DLP audits the actions taken by all administrators of the product. As administrators authenticate to, configure, or use Symantec DLP, their actions are logged in the operation log files. Each action that is logged includes the date and time of the event, the ID of the administrator that caused the action, and some indication if the event is a failed action, for example a failure to authenticate.

Symantec DLP provides a number of different log files that record information about the behavior of the software. All of the logs are stored as log files on the database in the IT Environment. The Symantec DLP log files fall into these categories: operational log files, debug log files, and installation log files.

7.1.1.1 Operational log files

Operational log files record detailed information about the tasks the software performs and any errors that occur while the software performs those tasks. The contents of the operational log files can be used to verify that the software functions as expected. In addition, all security-related administrator actions are logged within the operational log files. These log files can also be used to troubleshoot any problems in the way the software integrates with other components of the DLP system.

7.1.1.2 Debug log files

Debug log files record fine-grained technical details about the individual processes or software components that comprise DLP. The contents of debug log files are not intended for use in diagnosing system configuration errors or in verifying expected software functionality. The debug log files do not

need to be examined to administer or maintain DLP. However, Symantec Support may ask an authorized administrator to provide debug log files for further analysis when a problem is reported.

7.1.1.3 Installation log files

Installation log files record information about the DLP installation tasks that are performed on a particular computer. An administrator can use these log files to verify an installation or troubleshoot installation errors.

7.1.2 Identification and Authentication

The Enforce Server requires that each administrator be successfully identified and authenticated with a username and password before being allowed access to the Enforce Server administration console. Administrators are required to use strong passwords that are enforced by the TOE. Strong passwords must contain at least eight characters, at least one number, and at least one uppercase letter. Strong passwords cannot have more than two repeated characters in a row.

7.1.3 Security Management

Security management specifies how DLP manages several aspects of the TSF including TSF data and security functions. TSF data includes configuration data of the TOE, audit data, and data collected by the TOE. The TOE provides authorized administrators with the Enforce Server administration console to manage the security functions and TSF data of the TOE.

DLP provides role-based access control to govern how authorized administrators can access product features and functionality. For example, a role might let an authorized administrator view reports, but prevent the administrator from creating policies or deleting incidents. Likewise, a role might let an authorized administrator author policy response rules but not detection rules. Roles determine what a user can see and do in the Enforce Server administration console. The summary of available roles and their privileges is as follows:

ROLE	PRIVILEGE
System Administrator	This role provides access to the System module and associated menu options in the Enforce Server administration console. Users in this role can monitor and manage the Enforce Server and detection servers(s). These detection servers include Network Discover Server, Network Monitor Server, Network Prevent Server (Email), Network Prevent Server (Web), and Endpoint Server.Users in this role can also deploy detection servers and run Network Discover scans.
User Administrator	This role grants users the right to manage users and roles. Typically this role grants no other access or privileges. Because of the potential for misuse, it is recommended that no more than two people in the organization be assigned this role (primary and backup).
Policy Administrator	This role grants users the right to manage policies and response rules. Typically this role grants no other access or privileges. Because of the potential for misuse, it is recommended that no more than two people in the organization be assigned this role (primary and backup).

ROLE	PRIVILEGE
Policy Author	This role provides access to the Policies module and associated menu options in the Enforce Server administration console. This role is suited for information security managers who track incidents and respond to risk trends. An information security manager can author new policies or modifying existing policies to prevent data loss.
Incident Responder	This role provides access to the Incidents module and associated menu options in the Enforce Server administration console. Users in this role can track and remediates incidents. Businesses often have at least two incident responder roles that provide two levels of privileges for viewing and responding to incidents. A first-level responder may view generic incident information, but cannot access incident details (such as sender or recipient identity). In addition, a first-level responder may also perform some incident remediation, such as escalating an incident or informing the violator of corporate security policies. A second-level responder might be escalation responder who has the ability to view incident details and edit custom attributes. A third-level responder might be an investigation responder who can create response rules, author policies, and create policy groups.
Limited Administrator	The System Administrator can define custom privilege levels that may include one or more of the default role definitions. For example, a Policy Administrator may also have Policy Auditor rights.

Table 23 – Typical TOE Roles and Permissions

Roles and policy groups can be combined to limit the policies and detection servers that an administrator can configure. The System Administrator user (created during installation) has access to every part of the system and therefore is not a member of any access-control role. The management console ensures the default values of security attributes are restrictive in nature as to enforce the DLP Information Flow Control Policy for the TOE.

7.1.4 Policy Enforcement

DLP collects information via the DLP Agents, Network Discover Servers, and Network Monitor Servers. Endpoint Discover uses DLP Agents to scan endpoint computers to find the information that an authorized administrator has defined as sensitive. The detection engine does not rely on file extensions to identify file type. The detection server checks the binary signature of the file to match its type. In the event that a file is in violation of the configured policies, Endpoint Discover sends an incident report back to the Enforce Server administration console. In addition, Endpoint Discover allows for the quarantine of confidential files to a secure location.

Endpoint Prevent uses the DLP Agents to stop sensitive data from moving off of an endpoint computer. Endpoint Prevent blocks data transfers from a hard drive to a removable media device. Removable media includes the following devices:

- USB flash drive
- SD card
- Compact flash card

- FireWire connected device

When the DLP Agent detects that a violation has occurred, the data is blocked from being transferred. An incident is created and sent to the Endpoint Server. When a violation occurs, the DLP Agent displays a pop-up notification to the user that informs the user that the violation has occurred. The notification also requires a justification for the file transfer. This justification appears in the incident snapshot.

A DLP Agent is installed on each endpoint computer that an administrator wants to scan. The Enforce Server controls the DLP Agent and applies the policies and rules of that Endpoint Server. The DLP Agent contains an encrypted data store[1], called the Agent Store. It acts as a buffer or holding space for the incidents and files that the DLP Agent sends to the Endpoint Server. If the DLP Agent is disconnected from the Endpoint Server, the Agent Store holds the incidents and files until a connection is re-established.

The Endpoint Server connects to both Endpoint Prevent and Endpoint Discover. The Endpoint Server connects all of the DLP Agents that are deployed on endpoint computers to the Enforce Server. The Endpoint Server pushes the policies that an authorized administrator creates out to the DLP Agents. Any violations that are detected by the Symantec DLP Agents are sent to the Endpoint Server which then forwards them on to the Enforce Server. In addition, the Endpoint Server contains the detection policies for Endpoint Discover.

Network Discover scans networked file shares, Web content servers, databases, document repositories, and endpoint systems at high speeds to detect exposed data and documents. Network Discover enables authorized administrators to understand exactly where confidential data is exposed and helps significantly reduce the risk of data loss. Once Network Discover finds a security breach, Network Protect, which sits on the Network Discover Server, removes the exposed confidential data, intellectual property, and/or classified information from open file shares on network servers or desktop computers. Network Protect will remediate the security breach by quarantining the exposed files or enforcing corporate access control and encryption policies. Network protect will access the managed device and will set the file permissions for the sensitive data on the device and encrypt[2] the data to meet corporate policies.

Network Monitor provides packet capture of network traffic. The Network Monitor Servers gather network traffic from scanned ports or taps, and report on private or proprietary data leaking as it moves across the network. The Enforce Server defines the policy groups, protocols, and protocol filters that control the Network Monitor Servers.

Authorized users in the environment are able to review the collected TOE data via reports that are generated by the TOE. Only authorized users that have been assigned a specific role and permissions are able to review the TOE data which is presented in reports. See Table 15 – Roles and Privileges to

[1] This encryption is provided by the environment and is not specifically included in this evaluation.
[2] While the action of “encrypt” is included as a function of the TOE, the actual cryptography is provided by the environment and is not specifically included in this evaluation.

view the specific user roles that have access to the incidents and reportsTOE data. An authorized administrator can use incident reports to track and respond to incidents. DLP reports an incident when it detects data that matches the detection parameters of a policy rule. Such data may include specific file content, an email sender or recipient, attachment file properties, or many other types of information. Each piece of data that matches detection parameters is called a match, and a single incident may include any number of individual matches. DLP tracks incidents for all detection servers. These servers include Network Discover Server, Network Monitor Server, Network Prevent Server (Email), Network Prevent Server (Web), and Endpoint Server.

End of Document
