

RSA, The Security Division of EMC

RSA® Data Loss Prevention Suite

v6.5

Security Target

Evaluation Assurance Level: EAL2
Augmented with ALC_FLR.1
Document Version: 0.7

Prepared for:



RSA, The Security Division of EMC

174 Middlesex Turnpike
Bedford, MA 01730
Phone: (877) 772-4900
Fax: (781) 515-5010

<http://www.rsa.com>

Prepared by:



Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050

<http://www.corsec.com>

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2008-07-07	Amy Nicewick	Initial draft.
0.2	2008-08-01	Amy Nicewick	Removed SFRs related to encryption; added Guidance documents to section 1.4.1.
0.3	2008-12-19	Amy Nicewick	Addressed PETR v0.1-1, and changed version number to v6.5.
0.4	2009-02-10	Zac Corbet	Updated product name to include registered trademark. Updated RSA company name. Added statement regarding Figure 1.
0.5	2009-03-12	Amy Nicewick	Addressed follow-up verdicts and CB OR 1.
0.6	2009-03-19	Amy Nicewick	Added FDP_IFC.1 and FDP_IFF.1.
0.7	2009-04-20	Amy Nicewick	Addressed minor issues.

Table of Contents

REVISION HISTORY	2
TABLE OF CONTENTS	3
TABLE OF FIGURES	4
TABLE OF TABLES	4
1 SECURITY TARGET INTRODUCTION	6
1.1 PURPOSE.....	6
1.2 SECURITY TARGET AND TOE REFERENCES	7
1.3 TOE OVERVIEW	7
1.3.1 <i>Brief Description of the Components of the TOE</i>	9
1.3.2 <i>DLP Network</i>	9
1.3.3 <i>DLP Endpoint</i>	11
1.3.4 <i>DLP Datacenter</i>	12
1.3.5 <i>DLP Enterprise Manager</i>	13
1.3.6 <i>Policies</i>	14
1.3.7 <i>TOE Environment</i>	15
1.4 TOE DESCRIPTION	16
1.4.1 <i>Physical Scope</i>	17
1.4.2 <i>Logical Scope</i>	18
1.4.3 <i>Physical and Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE</i>	20
2 CONFORMANCE CLAIMS	21
3 SECURITY PROBLEM DEFINITION	22
3.1 THREATS TO SECURITY.....	22
3.2 ORGANIZATIONAL SECURITY POLICIES	23
3.3 ASSUMPTIONS	23
4 SECURITY OBJECTIVES	24
4.1 SECURITY OBJECTIVES FOR THE TOE.....	24
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT	25
4.2.1 <i>IT Security Objectives</i>	25
4.2.2 <i>Non-IT Security Objectives</i>	25
5 EXTENDED COMPONENTS DEFINITION	26
5.1 EXTENDED TOE SECURITY FUNCTIONAL COMPONENTS	26
5.1.1 <i>Class FIH: Incident Handling</i>	27
5.2 EXTENDED TOE SECURITY ASSURANCE COMPONENTS	30
6 SECURITY REQUIREMENTS	31
6.1 CONVENTIONS	31
6.2 SECURITY FUNCTIONAL REQUIREMENTS	31
6.2.1 <i>Class FAU: Security Audit</i>	33
6.2.2 <i>Class FDP: User Data Protection</i>	35
6.2.3 <i>Class FIA: Identification and Authentication</i>	43
6.2.4 <i>Class FMT: Security Management</i>	44
6.2.5 <i>Class FTA: TOE Access</i>	50
6.2.6 <i>Class EXT_FIH: Incident Handling</i>	51
6.3 SECURITY ASSURANCE REQUIREMENTS	53
7 TOE SUMMARY SPECIFICATION	54
7.1 TOE SECURITY FUNCTIONS.....	54
7.1.1 <i>Security Audit</i>	55

7.1.2	<i>User Data Protection</i>	56
7.1.3	<i>Identification and Authentication</i>	56
7.1.4	<i>Security Management</i>	56
7.1.5	<i>TOE Access</i>	57
7.1.6	<i>Incident Handling</i>	57
8	RATIONALE	58
8.1	CONFORMANCE CLAIMS RATIONALE	58
8.2	SECURITY OBJECTIVES RATIONALE.....	58
8.2.1	<i>Security Objectives Rationale Relating to Threats</i>	58
8.2.2	<i>Security Objectives Rationale Relating to Policies</i>	61
8.2.3	<i>Security Objectives Rationale Relating to Assumptions</i>	61
8.3	RATIONALE FOR EXTENDED SECURITY FUNCTIONAL REQUIREMENTS	62
8.4	RATIONALE FOR EXTENDED TOE SECURITY ASSURANCE REQUIREMENTS	62
8.5	SECURITY REQUIREMENTS RATIONALE.....	63
8.5.1	<i>Rationale for Security Functional Requirements of the TOE Objectives</i>	63
8.5.2	<i>Security Assurance Requirements Rationale</i>	67
8.5.3	<i>Dependency Rationale</i>	67
9	ACRONYMS AND TERMINOLOGY	71
9.1	ACRONYMS.....	71
9.2	TERMINOLOGY	73

Table of Figures

FIGURE 1 - DEPLOYMENT CONFIGURATION OF THE TOE.....	8
FIGURE 2 - SAMPLE DLP NETWORK DEPLOYMENT	10
FIGURE 3 - SAMPLE DLP ENDPOINT DEPLOYMENT	11
FIGURE 4 - SAMPLE DLP DATACENTER DEPLOYMENT	12
FIGURE 5 - PHYSICAL TOE BOUNDARY.....	18
FIGURE 6 – IT SECURITY OBJECTIVES	25
FIGURE 7 - EXT_FIH: INCIDENT HANDLING CLASS DECOMPOSITION.....	27
FIGURE 8 - EXT_FIH_ARP INCIDENT AUTOMATIC RESPONSE FAMILY DECOMPOSITION	28
FIGURE 9 - INCIDENT ANALYSIS FAMILY DECOMPOSITION	29

Table of Tables

TABLE 1 - ST AND TOE REFERENCES	7
TABLE 2 – TOE ENVIRONMENT COMPONENTS	15
TABLE 3 - CC AND PP CONFORMANCE.....	21
TABLE 4 - THREATS	22
TABLE 5 - ASSUMPTIONS	23
TABLE 6 - SECURITY OBJECTIVES FOR THE TOE	24
TABLE 7 - NON-IT SECURITY OBJECTIVES	25
TABLE 8 - EXTENDED TOE SECURITY FUNCTIONAL REQUIREMENTS.....	26
TABLE 9 - TOE SECURITY FUNCTIONAL REQUIREMENTS.....	31
TABLE 10 - MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR.....	44
TABLE 11 – STATIC ATTRIBUTE INITIALISATION	48
TABLE 12 - ASSURANCE REQUIREMENTS	53
TABLE 13 - MAPPING OF TOE SECURITY FUNCTIONS TO SECURITY FUNCTIONAL REQUIREMENTS	54
TABLE 14 - THREATS:OBJECTIVES MAPPING.....	58
TABLE 15 - ASSUMPTIONS:OBJECTIVES MAPPING.....	61

TABLE 16 - OBJECTIVES:SFRs MAPPING.....63
TABLE 17 - FUNCTIONAL REQUIREMENTS DEPENDENCIES67
TABLE 18 - ACRONYMS.....71

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the RSA® Data Loss Prevention Suite v6.5, and will hereafter be referred to as the TOE throughout this document. The software-only TOE is a suite of products that allows an enterprise to identify sensitive information stored on its computers, as it is transmitted between Information Technology (IT) entities, and as it is being copied, saved, or printed.

1.1 Purpose

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats:

- Security Target Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem Definition (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components Definition (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs)) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terminology (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	RSA, The Security Division of EMC RSA® Data Loss Prevention Suite v6.5 Security Target
ST Version	Version 0.7
ST Author	Corsec Security, Inc. Amy Nicewick
ST Publication Date	2009-04-20
TOE Reference	RSA® Data Loss Prevention Suite v6.5 build 6.5.0.2179
Keywords	Data Loss Prevention, DLP, Datacenter, Network, Endpoint

1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

RSA's Data Loss Prevention (DLP) suite of products allows an enterprise to identify sensitive information in text format stored on its computers, and as it is being transmitted between IT entities or being copied, saved, or printed. The TOE then takes actions based on pre-defined policies to protect the information from loss and misuse. There are four products within the DLP suite that provide this functionality: DLP Enterprise Manager, DLP Datacenter, DLP Network, and DLP Endpoint. The DLP Datacenter, DLP Network, and DLP Endpoint are managed through the DLP Enterprise Manager, a web application with a consistent user interface across all the products. The DLP Datacenter, DLP Network, and DLP Endpoint can each be used independently, or integrated with one or both of the others, to provide the sensitive data protection required by RSA's customers. However, in order for any one of the other products to work, the DLP Enterprise Manager must also be installed. This is because the DLP Enterprise Manager is necessary to provide administrative access to the other products, and without it, there would be no way to manage the other products.

Each product consists of one or more components, as shown in Figure 1. The DLP Network product consists of the following components:

- DLP Network Controller
- DLP Network Sensor
- DLP Network Interceptor
- DLP Network ICAP Server

The DLP Endpoint product consists of the following components:

- DLP Endpoint Enterprise Coordinator
- DLP Endpoint Site Coordinator

- DLP Endpoint Agent

The DLP Datacenter product consists of the following components:

- DLP Datacenter Enterprise Coordinator
- DLP Datacenter Site Coordinator
- DLP Datacenter Grid Worker
- DLP Datacenter Agent

The DLP Enterprise Manager is a stand-alone component that comprises the DLP Enterprise Manager product.

Figure 1 shows the four DLP products available in the DLP Suite. Note: This diagram depicts the architecture of the DLP Suite as it appears in stand-alone mode, but only one Enterprise Coordinator is supported when deployed as a suite.

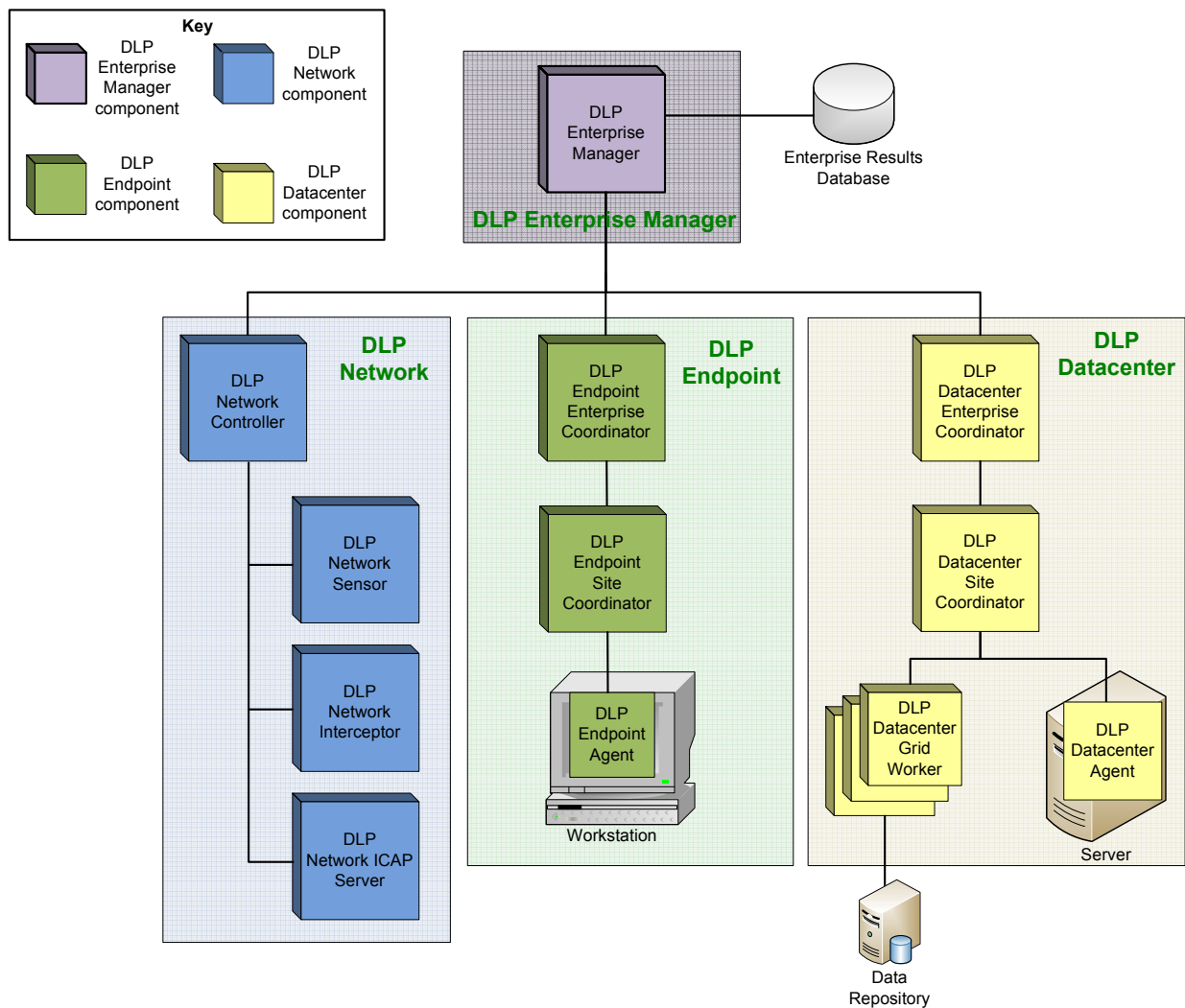


Figure 1 - Deployment Configuration of the TOE

1.3.1 Brief Description of the Components of the TOE

The DLP Datacenter, DLP Network, and DLP Endpoint products perform content analysis on documents and transmissions using a shared, policy-driven engine. Using these policies, an enterprise can examine communications, track end-user¹ actions, and locate stored documents that contain sensitive content, and determine whether the action being taken on that content should be permitted. Sensitive content might include Personally Identifiable Information (PII), such as Social Security Numbers, Non-Public Personal Information (NPI), such as email addresses, or information protected by the Payment Card Industry (PCI) Data Security Standard, such as credit card information. DLP policies can define documents or transmissions as sensitive based on their content, sender, receiver, owner, source, destination, device, file type, or file size. RSA provides built-in, expert policies for immediate use. Administrators² of the DLP products can also build their own custom policies to identify sensitive content specific to their enterprise.

1.3.2 DLP Network

The DLP Network product detects sensitive data while it is being transmitted across the network, and generates events and incidents reflecting policy violations. The targeted data is referred to as “Data In Motion”. DLP Network can automatically monitor or block identified transmissions, or quarantine messages that may need prior approval before leaving the network. In addition, encryption of emails containing sensitive content can be performed by the operational environment when the TOE is configured to do so. Figure 2 below shows a typical DLP Network deployment.

¹ End-users are those individuals accessing the targeted computers on the network.

² Administrators are those individuals who perform management functions on the TOE.

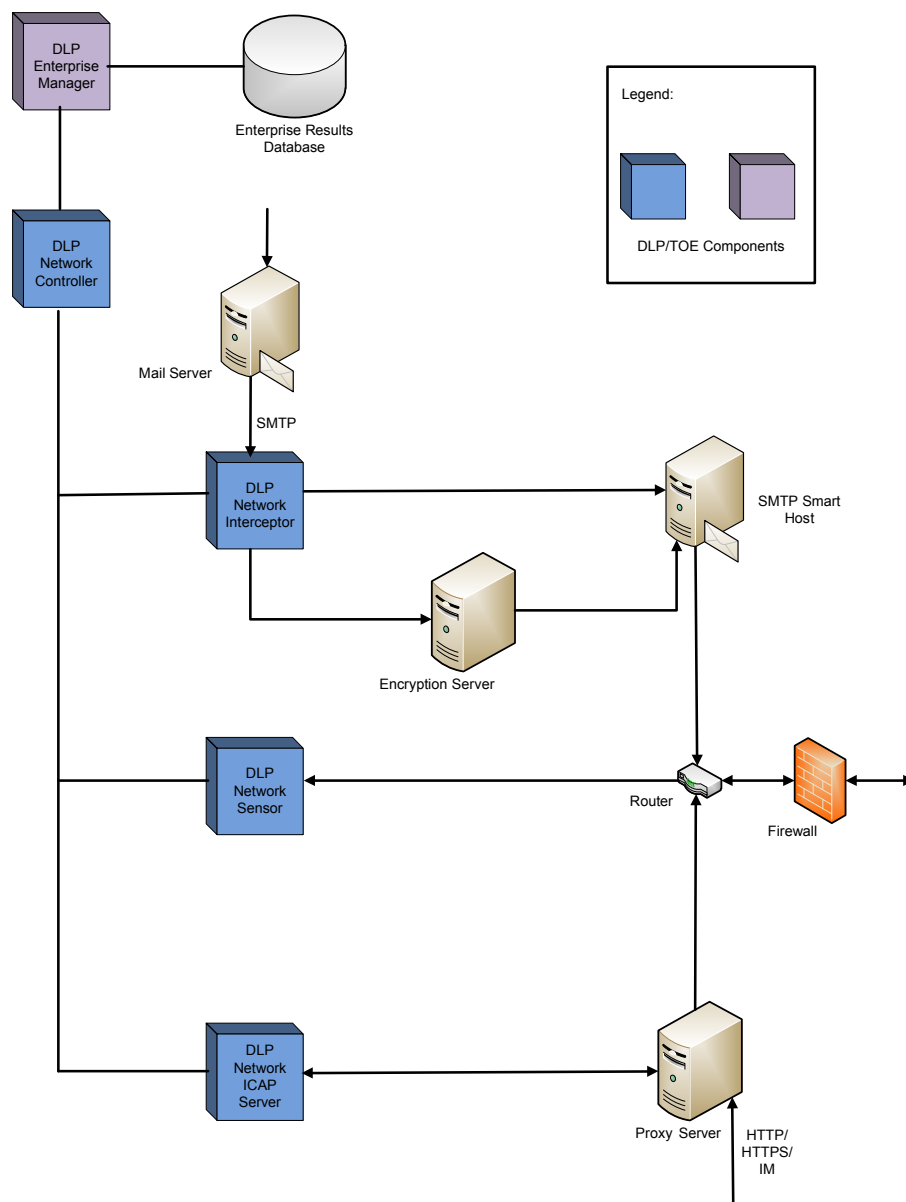


Figure 2 - Sample DLP Network Deployment³

DLP Network includes a number of components that integrate to prevent the loss of sensitive information from the targeted network. The DLP Network Controller is the main appliance that maintains information about confidential data and content transmission policies. There are three types of devices that are managed by the DLP Network Controller: DLP Network Sensors, Interceptors, and ICAP servers. These devices monitor network transmissions and report or intercept identified transmissions. DLP Network Sensors are installed at network boundaries. They passively monitor traffic crossing the network boundaries, and analyze it for the presence of sensitive content. DLP Network Interceptors are also installed at network boundaries, but they allow administrators to implement policies that quarantine or reject email traffic that contains sensitive content. DLP Network ICAP Servers are special

³ SMTP – Simple Mail Transfer Protocol; ICAP – Internet Content Adaptation Protocol; HTTP – HyperText Transfer Protocol; HTTPS – Secure HyperText Transfer Protocol; IM – Instant Messaging

purpose server devices that allow administrators to implement monitoring or blocking of HTTP, HTTPS, or File Transfer Protocol (FTP) traffic containing sensitive content.

In addition, Administrators can view log entries captured by DLP Network through the Command Line Interface (CLI) on each of the appliances, or through the DLP Enterprise Manager.

1.3.3 DLP Endpoint

The DLP Endpoint product provides control over confidential information being manipulated by end-users. The targeted data is referred to as “Data In Use”. DLP Endpoint monitors data activity for irregularities, alerts administrators to at-risk processes, and blocks the loss of sensitive content from the network’s computers. Figure 3 below shows a typical DLP Endpoint deployment.

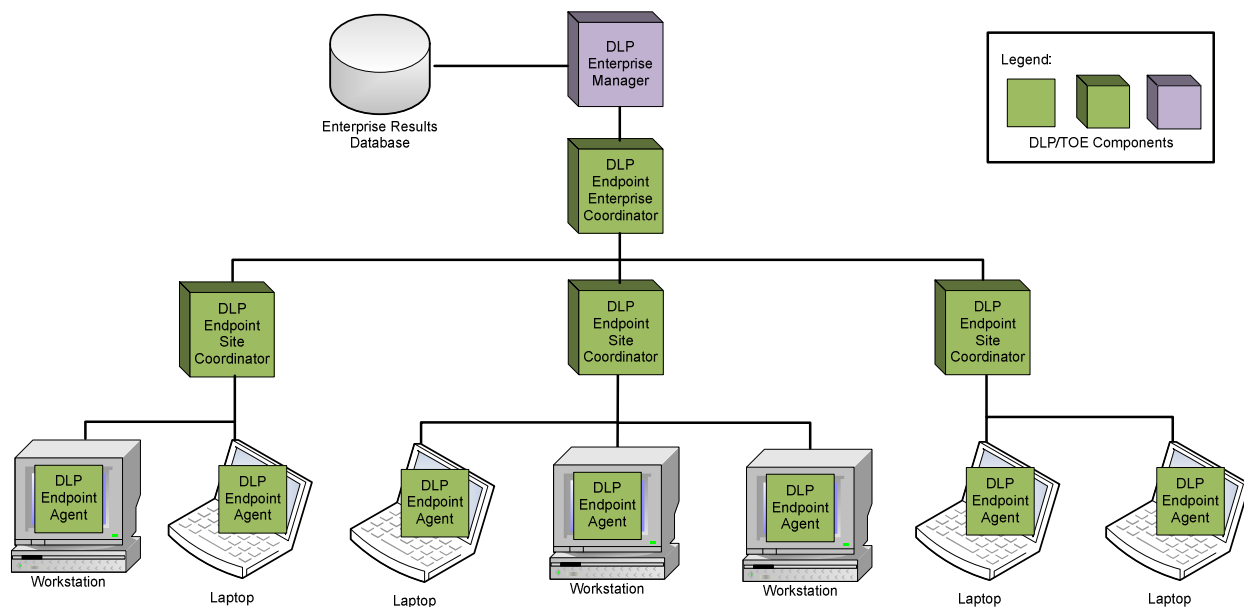


Figure 3 - Sample DLP Endpoint Deployment

DLP Endpoint consists of three components: DLP Endpoint Agent, DLP Endpoint Site Coordinator, and DLP Endpoint Enterprise Coordinator. The DLP Endpoint Agent enforces policies on usage of data, resulting in blockages, justifications, or notifications, and generates events that describe the violations and the actions taken to enforce the policies. DLP Endpoint Agents push these events to the DLP Endpoint Site Coordinator, and also retrieve configuration settings and policy files from the DLP Endpoint Site Coordinator. The DLP Endpoint Agent is a service that starts when the computer starts, and monitors end-user actions as long as the computer is running. DLP Endpoint Agents run from within the targeted machine’s operating system, and are transparent to desktop applications. The DLP Endpoint Agent injects itself into each running process on the targeted machine, and intercepts and monitors application calls. When an application call for an end-user action such as copy, move, or print is intercepted, the DLP Endpoint Agent extracts the content of the document involved, and performs an analysis on the content to determine if a policy violation has occurred. If so, the DLP Endpoint Agent sends an event to the DLP Endpoint Site Coordinator, and the action is either allowed or disallowed, depending on the policy. The DLP Endpoint Agent displays a system tray icon to the end-user to provide messages and accept justification text from end-users.

Each DLP Endpoint Agent receives its instructions from a DLP Endpoint Site Coordinator, and returns results to it. DLP Endpoint Site Coordinators are services that manage scans for a local network. An enterprise may install as many DLP Endpoint Site Coordinator as it wishes to coordinate scans on DLP Endpoint Agents that are dispersed widely throughout the enterprise.

The DLP Endpoint Enterprise Coordinator is the master controller of a DLP Endpoint deployment. It sends instructions to, and gathers scan results from, all DLP Endpoint Site Coordinator installed in the enterprise.

The DLP Endpoint Enterprise Coordinator manages the policies and the collection of events from DLP Endpoint Site Coordinator throughout the network, and passes the information to the DLP Enterprise Manager for display in the Graphical User Interface (GUI). In addition, the DLP Endpoint Enterprise Coordinator, DLP Endpoint Site Coordinator, and DLP Endpoint Agent capture audit logs and download them to the DLP Enterprise Manager where they can be viewed through the GUI.

1.3.4 DLP Datacenter

The DLP Datacenter product provides the ability to identify sensitive content stored on laptops, desktops, and servers distributed through a corporate environment. The targeted data is referred to as “Data At Rest”. DLP Datacenter scans the organization’s networks, examining files on all designated machines. Figure 4 below shows a typical DLP Datacenter deployment.

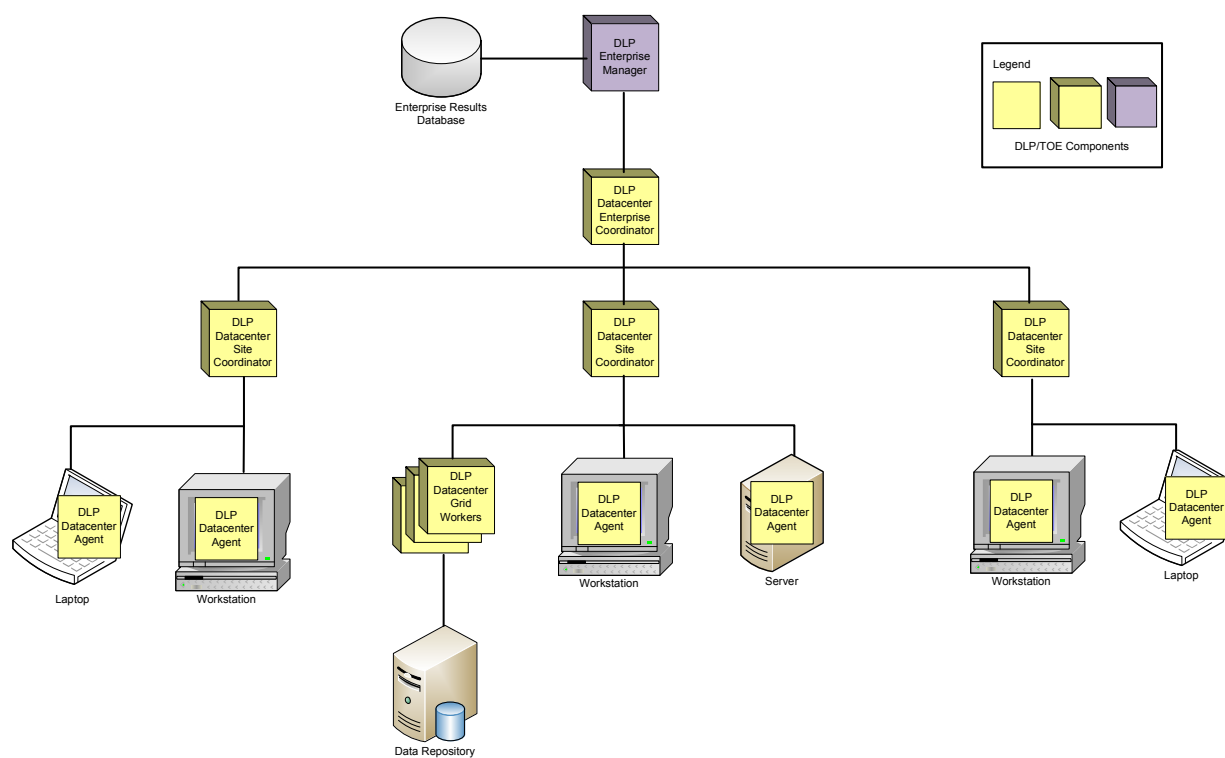


Figure 4 - Sample DLP Datacenter deployment

Several components of the DLP Datacenter product work together to perform scans and act on the information gathered from them. DLP Datacenter Agents are small programs that perform the analysis on the designated machines. Because the DLP Datacenter Agents are deployed onto the selected machines, sensitive data does not have to be moved to a central location for analysis.

Each DLP Datacenter Agent receives its instructions from a DLP Datacenter Site Coordinator, and returns results to it. DLP Datacenter Site Coordinators are services that manage scans for a local network. An enterprise may install as many DLP Datacenter Site Coordinators as it wishes to coordinate scans on DLP Datacenter Agent that are dispersed widely throughout the enterprise.

The DLP Datacenter Enterprise Coordinator is the master controller of a DLP Datacenter deployment. It sends instructions to, and gathers scan results from, all DLP Datacenter Site Coordinator installed in the enterprise.

Finally, the DLP Enterprise Manager is the interface to the DLP Datacenter for all administrators. Administrators may be security specialists that analyze incidents generated by the DLP Datacenter components, or other specialists or system administrators that design and run the scans.

When the DLP Datacenter product scans, it accesses a specific scan group, or set of machines on the network that the administrator specifies as being of interest. Administrators may define as many scan groups, of any size, as is required. There are two types of scan groups available: agent-scan groups for agent-based scans on desktops or laptops, and grid-scan groups for grid scans on large data depositories. In addition, DLP Datacenter Agents can be temporary or permanent. Temporary DLP Datacenter Agents exist on the target machine only while a scan is in progress. After the DLP Datacenter Agent completes its analysis of the target machine, it removes itself from that machine. Permanent DLP Datacenter Agents remain on the target machine indefinitely. If, during a scan, DLP Datacenter encounters a target machine or grid machine that does not have a permanent DLP Datacenter Agent installed, it will install a DLP Datacenter Agent to use during that scan.

In agent-based scans, a DLP Datacenter Agent is installed on every machine whose content is being scanned. Requests for scans are passed from the DLP Enterprise Manager to the DLP Datacenter Enterprise Coordinator, and then to the appropriate DLP Datacenter Site Coordinator. The DLP Datacenter Site Coordinator then installs or connects to a DLP Datacenter Agent on each target machine in the scan group, and instructs it to start scanning the machine. The DLP Datacenter Agents access and analyze all files on its host, then send results containing information about files that violate the pre-configured policies back to the DLP Datacenter Site Coordinator. The DLP Datacenter Site Coordinator then collates the results and forwards them to the DLP Datacenter Enterprise Coordinator. The DLP Datacenter Enterprise Coordinator in turn forwards the results to the DLP Enterprise Manager, which displays them to the administrator.

In grid scans, a special grid of dedicated machines is set up with temporary or permanent DLP Datacenter Agents (called DLP Datacenter Grid Worker) that retrieve and analyze data from a large storage repository, such as Storage Area Network (SAN) or Network-Attached Storage (NAS) systems. In this setup, the DLP Datacenter Grid Workers are installed on dedicated machines instead of on the target machine that is being scanned. Similarly to agent-based scans, requests are passed from the DLP Enterprise Manager to the DLP Datacenter Enterprise Coordinator, and then to the appropriate DLP Datacenter Site Coordinator. The DLP Datacenter Site Coordinator then installs or connects to the DLP Datacenter Grid Worker in the grid machines, and divides up the scanning work among them until the entire data repository has been scanned. The DLP Datacenter Grid Workers access and analyze all files they have been directed to scan, and send the results back to the DLP Datacenter Site Coordinator. The DLP Datacenter Site Coordinator then forwards the results to the DLP Datacenter Enterprise Coordinator, which in turn forwards them to the DLP Enterprise Manager. The DLP Enterprise Manager displays the results to the administrator.

In addition, the DLP Datacenter Enterprise Coordinator and DLP Datacenter Site Coordinator capture audit logs and download them to the DLP Enterprise Manager where they can be viewed through the GUI.

1.3.5 DLP Enterprise Manager

DLP Enterprise Manager is a web application with which an administrator configures and manages all the other DLP products. DLP Enterprise Manager is accessed through a standard web browser. Each installation of DLP products typically includes only one instance of DLP Enterprise Manager. In the evaluated configuration only one instance of DLP Enterprise Manager is installed. DLP Enterprise Manager requires a database, called the Enterprise Results Database, for storing the configurations, security policies, and the results of analyses performed by the other components. Through the DLP Enterprise Manager, administrators can create, modify, and delete policies, manage administrators, groups, and roles, customize notifications when a violation of security has been detected, update product licenses, download log files, import and export configurations, delete events⁴ and incidents⁵, and view DLP documentation. The DLP Enterprise Manager stores and retrieves data to and from the Enterprise Results Database.

⁴ An “event” is any action or state detected by a TOE component that violates the security policy being enforced.

1.3.6 Policies

Sensitive content is information the enterprise needs to be protected from loss or misuse. The DLP suite uses modules called content blades to detect sensitive content. Content blades are the detection components of DLP policies. Content blades use two methods for detecting sensitive content: 1) creating descriptions of the content to be detected and 2) creating fingerprints of specific sensitive documents. These methods implement the detection rules of a policy.

In addition to detection rules, each DLP policy also implements product-specific rules that detect attributes that may or may not be allowed. For DLP Network, the attribute rules include:

- protocol characteristics, such as SMTP,
- transmission characteristics, such as sender or recipient,
- device characteristics, such as a device's name or Internet Protocol (IP) address, and
- file characteristics, such as file extensions.

For DLP Endpoint, attribute rules include:

- end-user actions, such as Save to Removable Drive,
- file attributes, such as file extensions, and
- file source and destination attributes, such as device type.

And for DLP Datacenter, the attribute rules include:

- file dates, such as "files last modified" dates.

Policy actions are automatically performed by a DLP product when specified rules are matched. Possible policy actions include the following:

DLP Network:

- Allow
- Audit only
- Quarantine and audit
- Block and audit
- Tag for encryption⁶

DLP Endpoint:

- Allow
- Audit only
- Notify and audit
- Justify and audit
- Block and audit

DLP Datacenter:

- Allow
- Audit only

⁵ "Incidents" are events or groups of events that require some sort of action to be taken by the TOE.

⁶ Note the use of the term "tag for encryption" is to represent a rule selector and not the action of encryption. Encryption, if selected and available, is done by a third-party product, and is outside the scope of this evaluation.

- Apply RMS template⁷

An allow action causes the attempted end-user action to be permitted. An audit action generates an event describing the violation. A quarantine action forces access to the sensitive content to be restricted to a designated end-user or group. A block action disallows the attempted violation. A notify action causes a notification of the violation to be sent to the end-user who committed it. A justify action causes a popup message to appear to the end-user, requiring the end-user to provide text justifying the attempted action. Each policy action taken is captured in an event record, and passed to the DLP Enterprise Manager for viewing by the administrator.

In addition to rules that generate events, the DLP products also generate “incidents”, which are higher-level issues that require manual remediation by an administrator. Incidents are identified and managed using incident rules, notification rules, and escalation rules. Incident rules define how one or more related events can generate an incident. Notification rules specify the individuals or groups to be notified when an incident is created. Escalation rules specify the individuals or groups that are to be notified and other actions that are to occur when an incident remains open beyond a certain amount of time.

1.3.7 TOE Environment

The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- DLP Network appliances;
- Customer-provided hardware for DLP Endpoint and DLP Datacenter;
- Microsoft Internet Explorer 6 web browser installed on the Enterprise Manager appliance;
- Targeted customer workstations, servers, and laptops on which DLP Endpoint Agents, DLP Datacenter Agents, and DLP Datacenter Grid Workers will be installed;
- A Microsoft SQL Server 2005 Database to serve as the Enterprise Results Database.

The TOE environment requires the components listed in Table 2 for the CC evaluated configuration:

Table 2 – TOE Environment Components

Component	Machine	Operating System	CPU	Available RAM	Free Storage
DLP Enterprise Manager appliance	Customer Hardware	Windows 2003 Server	Single-core 1 GigaHertz (GHz)	2 Gigabytes (GB)	20 GB
Microsoft SQL Server 2005 Database	Customer Hardware	Window 2003 Server	1 GHz	2 GB	20 GB
DLP Network Controller appliance	RSA Appliance	TabOS based on CentOS v5.1	As provided with appliance		

⁷ RMS is the Microsoft Active Directory Rights Management Services, which implements DRM (Digital Rights Management) for documents. An RMS template contains automatic policy actions on DLP Datacenter events, such as adding rights to sensitive files. For more information, please see the *RSA DLP Datacenter v6.5 User Guide*.

Component	Machine	Operating System	CPU	Available RAM	Free Storage
DLP Network Sensor appliance	RSA Appliance	TabOS based on CentOS v5.1	As provided with appliance		
DLP Network Interceptor appliance	RSA Appliance	TabOS based on CentOS v5.1	As provided with appliance		
DLP Network ICAP Server appliance	RSA Appliance	TabOS based on CentOS v5.1	As provided with appliance		
DLP Endpoint Enterprise Coordinator appliance	Customer Hardware	Windows 2003 Server	Single-core 1 GHz	2 GB	20 GB
DLP Endpoint Site Coordinator appliance	Customer Hardware	Windows 2003 Server	Dual-core 2 GHz	2 GB	20 GB
DLP Endpoint Agent host machine	Customer Hardware	Windows 2003/Vista	(as determined by customer)	(as determined by customer)	(as determined by customer)
DLP Datacenter Enterprise Coordinator appliance	Customer Hardware	Windows 2003 Server	Single-core 1 GHz	2 GB	20 GB
DLP Datacenter Site Coordinator appliance	Customer Hardware	Windows 2003 Server	Dual-core 2 GHz	2 GB	20 GB
DLP Datacenter Agent host machine	Customer Hardware	Windows 2003/Vista	(as determined by customer)		
DLP Datacenter Grid Worker appliance	Customer Hardware	Windows 2003/Vista	(as determined by customer)		

1.4 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.4.1 Physical Scope

Figure 5 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is software that runs on RSA appliances or customer-provided hardware compliant to the minimum software and hardware requirements as listed in Table 2. The TOE is installed in an enterprise network as depicted in the figure below. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- DLP Enterprise Manager v6.5.0.2179 software
- DLP Network Controller v6.5.0.2164 software
- DLP Network Sensor v6.5.0.2164 software
- DLP Network Interceptor v6.5.0.2164 software
- DLP Network ICAP Server v6.5.0.2164 software
- DLP Endpoint Enterprise Coordinator v6.5.0.86 software
- DLP Endpoint Site Coordinator v6.5.0.86 software
- DLP Endpoint Agent v6.5.0.86 software
- DLP Datacenter Enterprise Coordinator v6.5.0.86 software
- DLP Datacenter Site Coordinator v6.5.0.86 software
- DLP Datacenter Agent v6.5.0.86 software
- DLP Datacenter Grid Worker v6.5.0.86 software.

The following guides are required reading and part of the TOE:

- RSA DLP Network 6.5 User Guide, 24 November 2008
- RSA DLP Network 6.5 Deployment Guide, 24 November 2008
- RSA DLP Datacenter 6.5 User Guide, 08 December 2008
- RSA DLP Datacenter 6.5 Deployment Guide, 24 November 2008
- RSA DLP Endpoint 6.5 User Guide, 24 November 2008
- RSA DLP Endpoint 6.5 Deployment Guide, 24 November 2008
- RSA, The Security Division of EMC Data Loss Prevention Suite v6.5 Guidance Supplement, Document Version 0.2

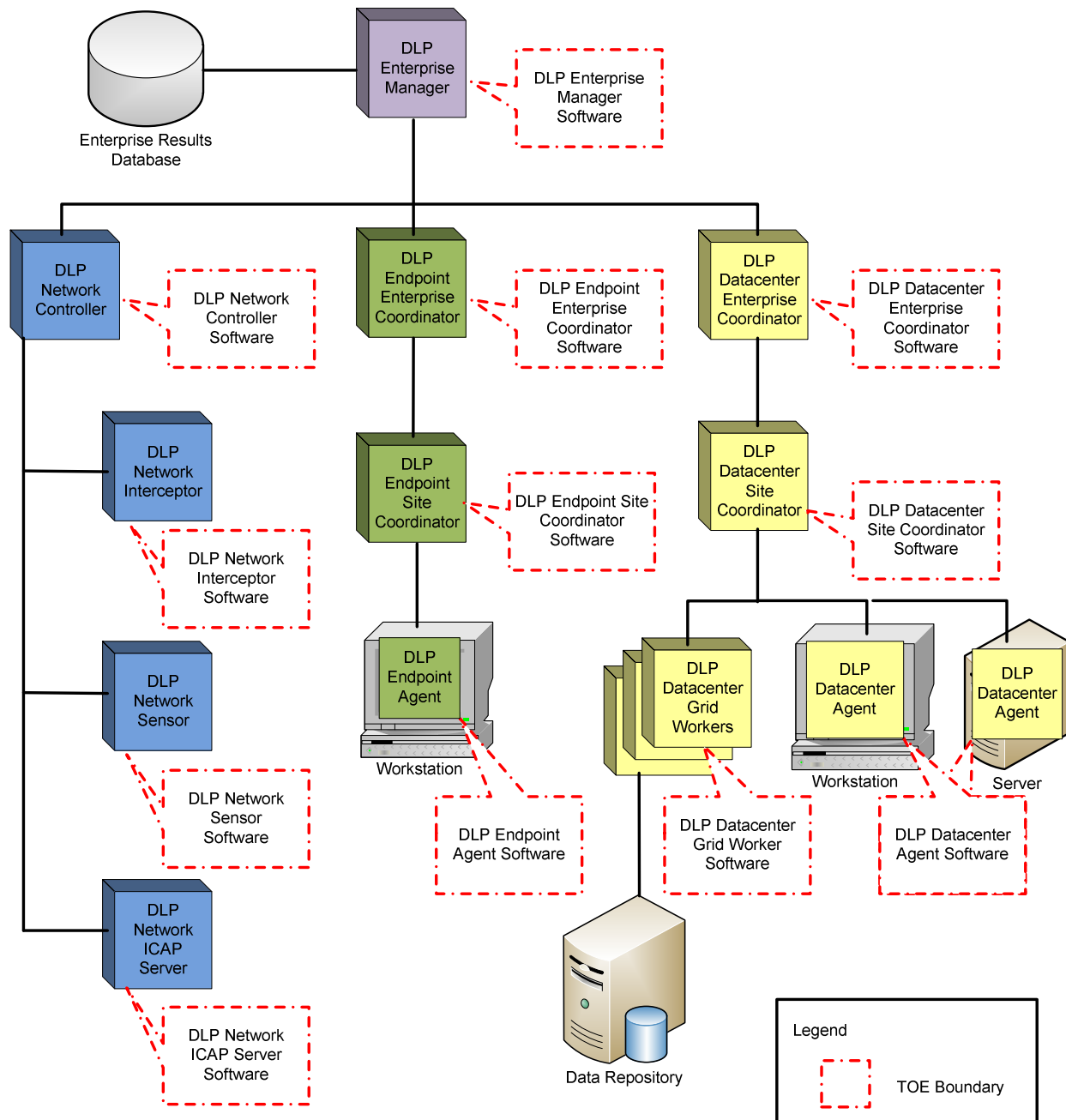


Figure 5 - Physical TOE Boundary

1.4.2 Logical Scope

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication

- Security Management
- Protection of the TSF⁸
- TOE Access
- Incident Handling

1.4.2.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation and viewing of audit data. Administrators can view audit log entries captured by DLP Network through the Command Line Interface (CLI) on each of the appliances. Audit logs captured by DLP Network, DLP Endpoint and DLP Datacenter are forwarded to the DLP Enterprise Manager where they can be viewed through the GUI.

1.4.2.2 User Data Protection

The TOE allows authorized administrators to enforce a rigid Administrative Access Control Security Functional Policy for administrators accessing the TOE. The TOE enforces administrator-configurable policies on access to sensitive data:

- DLP Network Security Functional Policies enforce rules governing the ability of end-users to transmit sensitive data across or out of the network.
- DLP Endpoint Security Functional Policies enforce rules governing the ability of end-users to take actions on data on targeted machines.
- DLP Datacenter Security Functional Policies enforce rules governing the suitability of files on targeted machines to store sensitive data.⁹

1.4.2.3 Identification and Authentication

Administrators must be identified and authenticated before they can perform any management tasks on the TOE or TOE data. Administrators authenticate to the DLP Enterprise Manager with a user ID and password through a web browser, and to the DLP Network appliances with a user ID and password through the CLI. Once administrators are authenticated, they may perform management tasks as allowed by their permissions.

1.4.2.4 Security Management

Security Management functions define roles and role management functionality of the TOE. The TOE maintains an Admin Role, which has access to all TOE management functionality. The Admin Role can define one or more Limited Admin Roles, and assign permissions to them as appropriate. Each administrator is also assigned a user group and user ID, which help to further define the permissions granted.

Permissive or Restrictive default values for security attributes defined by the Security Functional Policies are enforced by the TSF, and alternative default values may be specified by the Admin Role.

1.4.2.5 TOE Access

The TOE terminates an interactive session after thirty minutes of user inactivity.

1.4.2.6 Incident Handling

Analysis of events generated by the TOE is performed, and a determination about whether an incident should be generated is made. For each incident generated, the action taken in response by the TOE is defined.

⁸ TSF – TOE Security Functionality

⁹ Please note that any encryption action that is applied to a policy is outside the scope of this CC evaluation. All encryption takes place in the operational environment of the TOE.

1.4.2.7 Security Considerations in the TOE Environment:

Some audit logs captured by DLP Network are stored in the Operating System log files, but can be downloaded to the DLP Enterprise Manager and viewed through the GUI.

1.4.3 Physical and Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

Features and functionality that are not part of the evaluated configuration of the TOE are:

- Operating System
- Hardware
- Enterprise Results Database
- Encryption of data
- Data repositories, workstations, and servers on which the TOE performs scans

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007; CC Part 2 extended; CC Part 3 conformant; PP claim (none).
PP Identification	None
Evaluation Assurance Level	EAL 2 augmented with Basic Flaw Remediation (ALC_FLR.1)

3 Security Problem Definition

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The potential threat agents are divided into two categories:

- Attackers who are not TOE administrators: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE administrators: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE administrators are, however, assumed not to be willfully hostile to the TOE, and are therefore not included as threat agents in Table 4 below.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 - Security Objectives.

The following threats are applicable:

Table 4 - Threats

Name	Description
T.IA	A threat agent may attempt to compromise the TOE by attempting actions that it is not authorized to perform on the TOE.
T.INFO_CAPTURE	An external attacker or malicious insider may sniff the communication channel between the TOE and a remote administrator in order to capture or modify information sent between the two.
T.MASQUERADE	A threat agent masquerading as the TOE may capture valid identification and authentication data for a legitimate administrator of the TOE in order to gain unauthorized access to the TOE.
T.NO_AUDIT	A threat agent may perform security-relevant operations on the TOE without being held accountable for it.
T.SENSITIVE_CONTENT	A threat agent may access non-public or confidential information held by targeted assets in violation of the TOE's security functional policies.

Name	Description
T.UNAUTH	A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.
T.INT_CONF	An unauthorized user may attempt to disclose or compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.DATALOSS	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this Security Target.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 - Assumptions

Name	Description
A.LOCATE	The TOE resides in a physically controlled access facility that prevents unauthorized physical access.
A.NOEVIL	Authorized administrators who manage the TOE are non-hostile and are appropriately trained to use, configure, and maintain, the TOE, and follow all guidance.
A.SECURECOMMUNICATION	It is assumed that the IT environment will provide a secure line of communication between distributed portions of the TOE and between the TOE and remote administrators.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment. .

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 6 - Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators, may exercise such control.
O.IDAUTH	The TOE shall require that administrators of the TOE be identified and authenticated before allowing any TSF-mediated activity to be performed by them.
O.SEC_ACCESS	The TOE shall ensure that only authorized administrators are granted access to the security functions, configurations, and associated data.
O.LOG	The TOE shall generate logs of management operations performed on the TOE.
O.INCIDENT	The TOE shall analyze all events and generate incidents according to configured policies.
O.NOTIFICATION	The TOE shall generate and deliver alerts according to configured policies upon generating an incident.
O.SENSITIVE_CONTENT	The TOE shall take specified actions on transmissions, end-user actions, and files identified as containing or accessing non-public or confidential information.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Figure 6 – IT Security Objectives

Name	Description
OE.SECURECOMMUNICATION	The operational environment will provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote administrators.
OE.TIMESTAMP	The TOE Environment must provide reliable timestamps for the TOE's use.
OE.LOG	The TOE Environment shall securely store logs of management operations performed on the TOE that are generated by the TOE.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 7 - Non-IT Security Objectives

Name	Description
NOE.TRUSTED_ENV	The TOE shall reside in a physically secure location, safe from compromise by malicious insiders or outsiders.

5 Extended Components Definition

This section defines the extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs) met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 8 identifies all extended SFRs implemented by the TOE

Table 8 - Extended TOE Security Functional Requirements

Name	Description
EXT_FIH_ARP.1	Incident alarms
EXT_FIH_SAA.1	Incident analysis

5.1.1 Class FIH: Incident Handling

Incident Handling functions involve analyzing generated events and determining whether an incident should be generated, and a notification of that generation created and delivered to the configured administrator. The EXT_FIH: Incident Handling class was modeled after the CC FAU: Security audit class. The extended family and related components for EXT_FIH_AMP: Incident automatic response was modeled after the CC family FAU_AMP: Security audit automatic response. The extended family and related components for EXT_FIH_SAA: Incident analysis were modeled after the CC family and related components for FAU_SAA: Security audit analysis.

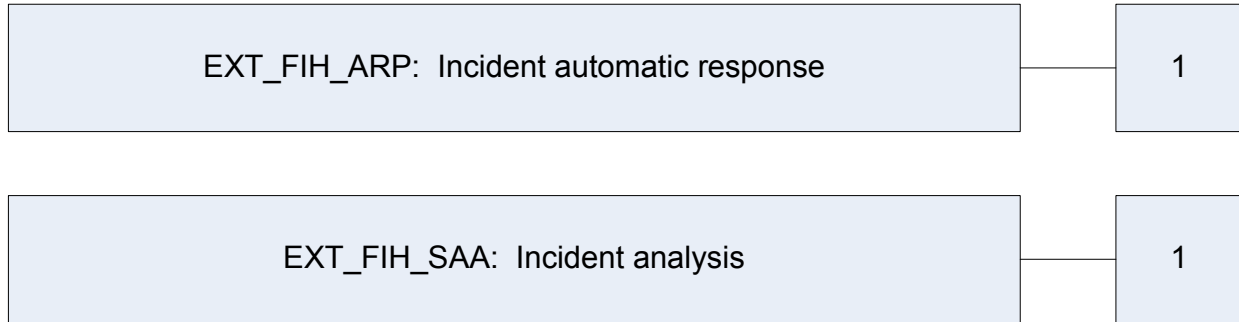


Figure 7 - EXT_FIH: Incident Handling Class Decomposition

5.1.1.1 Incident automatic response (EXT_FIH_ARP)

Family Behaviour

This family defines the response to be taken in case of generation of an incident.

Component Leveling

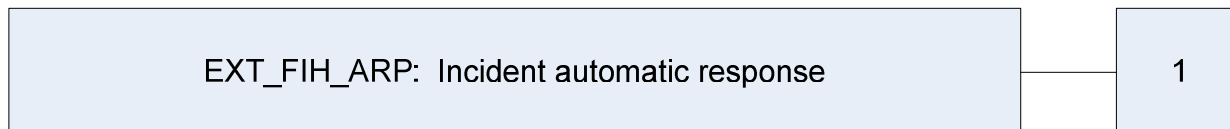


Figure 8 - EXT_FIH_ARP Incident automatic response family decomposition

EXT_FIH_ARP.1 Incident alarms, provides the capability to generate email notifications to pre-configured administrators when an incident is generated.

Management: EXT_FIH_ARP.1

The following actions could be considered for the management functions in FMT:

- The management (addition, removal, or modification) of actions.

Audit: EXT_FIH_ARP.1

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

- Minimal: Actions taken due to potential incidents.

EXT_FIH_ARP.1 Incident alarms

Hierarchical to: No other components

Dependencies: EXT_FIH_SAA.1 Incident analysis

This component will provide authorized administrators the capability to receive notifications of incident generation. This information needs to be in a human understandable presentation.

EXT_FIH_ARP.1.1 The TSF shall take [assignment: *list of actions*] upon detection of a potential incident.

5.1.1.2 Incident analysis (EXT_FIH_SAA)

Family Behaviour

This family defines the requirements for automated means that analyze events looking for incidents.

Component Leveling

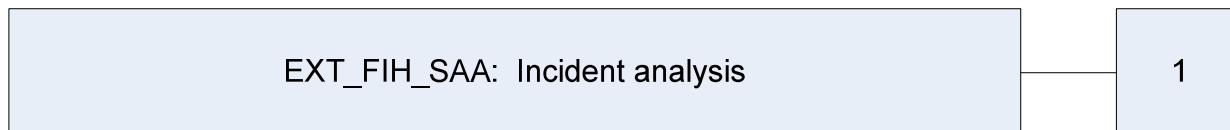


Figure 9 - Incident analysis family decomposition

In EXT_FIH_SAA.1 Incident analysis, basic threshold detection on the basis of a fixed rule set is required.

Management: EXT_FIH_SAA.1

The following actions could be considered for the management functions in FMT:

- Maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.

Audit: EXT_FIH_SAA.1

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

- Minimal: Enabling and disabling of any of the analysis mechanisms;
- Minimal: Automated response performed by the tool.

EXT_FIH_SAA.1 Incident analysis

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control
FDP_ACF.1 Security attribute based access control

EXT_FIH_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the generated policy-based events and based upon these rules generate an incident.

EXT_FIH_SAA.1.2 The TSF shall enforce the following rules for monitoring policy-based events:

- **Accumulation or combination of [assignment: *subset of defined events*] known to indicate a potential incident;**
- **[assignment: *any other rules*].**

5.2 Extended TOE Security Assurance Components

This section specifies the extended SARs for the TOE. The extended SARs are organized by class. There are no extended SARs implemented by the TOE.

6 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Parts 2 and 3 of the CC, and are shown as follows:

- Completed assignment statements are identified using *[italicized text within brackets]*.
- Completed selection statements are identified using *[underlined italicized text within brackets]*.
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSP Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using “EXT_” at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FDP_ACC.1(a) Subset Access Control would be the first iteration and FDP_ACC.1(b) Subset Access Control would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓	✓	
FAU_SAR.1	Audit review		✓	✓	
FDP_ACC.1(a)	Subset access control		✓		✓
FDP_ACF.1(a)	Security attribute based access control		✓		✓
FDP_ACC.1(b)	Subset access control		✓		✓
FDP_ACF.1(b)	Security attribute based access control		✓		✓
FDP_ACC.1(c)	Subset access control		✓		✓
FDP_ACF.1(c)	Security attribute based access control		✓		✓

Name	Description	S	A	R	I
FDP_ACC.1(d)	Subset access control		✓		✓
FDP_ACF.1(d)	Security attribute based access control		✓		✓
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FIA_UAU.2	User authentication before any action			✓	
FIA_UID.2	User identification before any action			✓	
FMT_MOF.1	Management of security functions behaviour	✓	✓	✓	
FMT_MSA.1(a)	Management of security attributes	✓	✓		✓
FMT_MSA.1(b)	Management of security attributes	✓	✓		✓
FMT_MSA.1(c)	Management of security attributes	✓	✓		✓
FMT_MSA.1(d)	Management of security attributes	✓	✓		✓
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FTA_SSL.3	TSF-initiated termination		✓		
EXT_FIH_ARP.1	Incident alarms		✓		
EXT_FIH_SAA.1	Incident analysis		✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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) [*management actions, as follows:*
 - o *Create, update, delete users;*
 - o *Create, update, delete groups;*
 - o *Create, update, delete roles;*
 - o *Create, update, delete Network Controller configurations;*
 - o *Create, update, delete Enterprise Coordinator configurations;*
 - o *Successful login;*
 - o *Logout;*
 - o *Failed login;*
 - o *Create, update, delete, reorder, enable, disable policies;*
 - o *Delete, logically delete events;*
 - o *Delete, logically delete incidents;*
 - o *Remediation actions (set acl, quarantine, move to secure, delete)*

].

Application Note: Start-up and shutdown of the audit functions are implied by the initiation and cessation of the generation of any audit records.

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*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*administrators*] with the capability to read [*all audit information stored in the DLP Network Operating System logs through the CLI, and all audit information stored by the Enterprise Manager in the Enterprise Results database through the Enterprise Manager GUI*] from the audit records.

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the ~~user~~ **administrator** to interpret the information.

Dependencies: FAU_GEN.1 Audit data generation

6.2.2 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1(a)

The TSF shall enforce the [Administrative Access Control SFP¹⁰] on

[

Subjects: users¹¹ attempting to establish an interactive session with the TOE

Objects: User Interface menu items, policies, incidents, events, reports, administrative management data

Operations: All interactions between the subjects and objects identified above

].

Dependencies: FDP_ACF.1(a) Security attribute based access control

FDP_ACF.1(a) Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1(a)

The TSF shall enforce the [Administrative Access Control SFP] to objects based on the following:

[

Subject attributes:

1. *User role*
2. *User group*
3. *User ID*
4. *User's permissions*

And Object attributes:

1. *Permissions assigned to objects*
2. *Absence of permissions assigned to objects*].

¹⁰ SFP – Security Functional Policy

¹¹ “User” may refer to any individual attempting to access the TOE or the targeted TOE devices or data (administrators or end-users).

FDP_ACF.1.2(a)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. *If the subject has the Admin Role, access is granted*
2. *If a subject requests access to an object that has no assigned permissions, access is granted*
3. *If a subject who does not have the Admin Role requests access to an object that has assigned permissions, the permissions of the subject are examined to determine if the subject has permission to access the object. If a match is found, access is granted*
4. *If none of the above rules apply, access is denied*

].

FDP_ACF.1.3(a)

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *[no additional rules]*.

FDP_ACF.1.4(a)

The TSF shall explicitly deny access of subjects to objects based on ~~the~~ *[no additional rules]*.

Dependencies: **FDP_ACC.1(a) Subset access control**
FMT_MSA.3 Static attribute initialization

FDP_ACC.1(b) Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1(b)

The TSF shall enforce the *[DLP Network Access Control SFP]* on

[

Subjects: End-Users

Objects: Data

Operations: Transmission of objects listed above by subjects listed above

].

Dependencies: **FDP_ACF.1(b) Security attribute based access control**

FDP_ACF.1(b) Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1(b)

The TSF shall enforce the [*DLP Network Access Control SFP*] to objects based on the following:

[

Subject attributes:

1. *End-User ID*
2. *End-User Group*

And Object attributes:

1. *Words*
2. *Phrases*
3. *Character patterns*
4. *Document fingerprints*
5. *Protocol*
6. *DLP device detected by*

].

FDP_ACF.1.2(b)¹²

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

Evaluate the configured policy rules and

1. *Record an event if the result of the evaluation is “audit”*
2. *Prevent access to the data by any end-user other than the pre-configured end-user if the result of the evaluation is “quarantine”*

].

FDP_ACF.1.3(b)

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(b)

¹² Please note that the DLP Network Access Control SFP is executed prior to the DLP Network Information Flow Control SFP (FDP_IFC.1, FDP_IFF.1).

The TSF shall explicitly deny access of subjects to objects based on the [*no additional rules*].

Dependencies: FDP_ACC.1(b) Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACC.1(c) Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1(c)

The TSF shall enforce the [*DLP Endpoint SFP*] on

[

Subjects: End-Users

Objects: Data

Operations: Copy, paste, cut, move, save, print, capture, send, or embed operations on objects listed above by subjects listed above

].

Dependencies: FDP_ACF.1(c) Security attribute based access control

FDP_ACF.1(c) Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1(c)

The TSF shall enforce the [*DLP Endpoint SFP*] to objects based on the following:

[

Subject attributes:

1. *End-User ID*
2. *End-User Group*

And Object attributes:

1. *Words*
2. *Phrases*
3. *Character patterns*
4. *File extension*
5. *File size*
6. *File destination*

].

FDP_ACF.1.2(c)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

Evaluate the configured policy rules and

1. *allow the end-user action if the result of the evaluation is “allow”*
2. *Record an event if the result of the evaluation is “audit”*
3. *Notify the pre-configured end-user if the result of the evaluation is “notify”*
4. *Request justification text from the identified end-user if the result of the evaluation is “justify”*
5. *Block the end-user action if the result of the evaluation is “block”*

].

FDP_ACF.1.3(c)

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(c)

The TSF shall explicitly deny access of subjects to objects based on the [*no additional rules*].

Dependencies: **FDP_ACC.1(c) Subset access control**
FMT_MSA.3 Static attribute initialization

FDP_ACC.1(d) Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1(d)

The TSF shall enforce the [*DLP Datacenter SFP*] on

[

Subjects: Files on desktops, laptops, servers, or data repositories

Objects: Data

Operations: subjects listed above containing objects listed above

].

Dependencies: **FDP_ACF.1(d) Security attribute based access control**

FDP_ACF.1(d) Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1(d)

The TSF shall enforce the [*DLP Datacenter SFP*] to objects based on the following:

[*Subject attributes:*

1. *Date modified*
2. *Date created*
3. *Other file dates*

And Object attributes:

1. *Words*
2. *Phrases*
3. *Character patterns*
4. *Document fingerprints*

].

FDP_ACF.1.2(d)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[*Evaluate the configured policy rules and*

1. *allow the retention of data if the result of the evaluation is “allow”*
2. *Record an event if the result of the evaluation is “audit”*
3. *Record an event and apply the designated RMS template if the result of the evaluation is “apply RMS template”*

].

FDP_ACF.1.3(d)

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(d)

The TSF shall explicitly deny access of subjects to objects based on the [*no additional rules*].

Dependencies: FDP_ACC.1(d) Subset access control
FMT_MSA.3 Static attribute initialization

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1

The TSF shall enforce the [DLP Network Information Flow Control SFP] on [End-Users, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP].

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1

The TSF shall enforce the [DLP Network Information Flow Control SFP] based on the following types of subject and information security attributes:

[

Subject attributes:

1. *End-User ID*
2. *End-User Group*

And Information attributes:

1. *Words*
2. *Phrases*
3. *Character patterns*
4. *Document fingerprints*
5. *Protocol*
6. *DLP device detected by*

].

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:

[

Evaluate the configured policy rules and

1. *Allow the transmission if the result of the evaluation is “allow”*
2. *Record an event if the result of the evaluation is “audit”*

3. *Block the transmission if the result of the evaluation is “block”*
4. *Forward the transmission for encryption if the result of the evaluation is “tag for encryption”¹³*

].

FDP_IFF.1.3

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

FDP_IFF.1.4

The TSF shall provide the following [*no additional SFP capabilities*].

FDP_IFF.1.5

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

FDP_IFF.1.6

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

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

¹³ Note the use of the term “tag for encryption” is to represent a rule selector and not the action of encryption. Encryption, if selected and available, is done by a third-party product, and is outside the scope of this evaluation.

6.2.3 Class FIA: Identification and Authentication

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1

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

Dependencies: No dependencies

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [Take action as listed in Table 10 below] the functions [See functions listed in Table 10 below] to [the roles listed in Table 10 below].

Table 10 - Management of Security Functions Behavior

Security Function	Admin Role	Limited Admin Role
Management of Users, Groups, and Roles	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>
Management of DLP Network Configuration	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>
Management of DLP Endpoint Configuration	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>
Management of DLP Datacenter Configuration	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>
Management of Content Blades	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>
Management of Email Server Configuration	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>

Security Function	Admin Role	Limited Admin Role
Management of Notification Templates	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>
Management of Policies	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>
Management of Reports	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>
Management of Policy Templates	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>
System Maintenance	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>
Management of Incidents	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>
Management of Events	<u>determine the behaviour of</u> <u>modify the behaviour of</u>	<u>determine the behaviour of</u> <u>modify the behaviour of</u> <u>(when given permission by the Admin Role)</u>

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1(a) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(a)

The TSF shall enforce the [*Administrative Access Control SFP*] to restrict the ability to [*change default, query, modify, delete.*] the security attributes [*User role, User ID, User group, User permissions, Permissions assigned to objects*] to [*the Admin Role, authorized Limited Admin Roles*].

Dependencies: FDP_ACC.1(a) Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1(b) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(b)

The TSF shall enforce the [*DLP Network Access Control SFP, DLP Network Information Control SFP*] to restrict the ability to [*change default, query, modify, delete.*] the security attributes [*end-user ID, end-user group, words, phrases, character patterns, document fingerprints, protocol, DLP device*] to [*the Admin Role, authorized Limited Admin Roles*].

Dependencies: [FDP_ACC.1(b) Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1(c) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*DLP Endpoint SFP*] to restrict the ability to [*change default, query, modify, delete.*] the security attributes [*end-user ID, end-user group, words, phrases, character patterns, file extension, file size, file destination*] to [*the Admin Role, authorized Limited Admin Roles*].

Dependencies: FDP_ACC.1(c) Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1(d) Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1(d)

The TSF shall enforce the [*DLP Datacenter SFP*] to restrict the ability to [*change default, query, modify, delete.*] the security attributes [*date file modified, date file created, other file dates, words, phrases, character patterns, document fingerprints*] to [*the Admin Role, authorized Limited Admin Roles*].

Dependencies: FDP_ACC.1(d) Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*See SFPs listed in Table 11 below*] to provide [*See default value listed in Table 11 below*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the [*Admin Role*] to specify alternative initial values to override the default values when an object or information is created.

Table 11 – Static Attribute Initialisation

SFP Security Attribute	Administrative Access Control SFP	DLP Network Access Control SFP/ DLP Network Information Flow Control SFP	DLP Endpoint SFP	DLP Datacenter SFP
User role	restrictive	n/a	n/a	n/a
User ID	restrictive	Restrictive	Restrictive	n/a
User group	restrictive	Restrictive	Restrictive	n/a
User permissions	restrictive	n/a	n/a	n/a
Object permissions	restrictive	n/a	n/a	n/a
Words	n/a	Permissive	Permissive	Permissive
Phrases	n/a	Permissive	Permissive	Permissive
Character patterns	n/a	Permissive	Permissive	Permissive
Document fingerprints	n/a	Permissive	n/a	Permissive
Protocol	n/a	Permissive	n/a	n/a
File size	n/a	n/a	Permissive	n/a
DLP device	n/a	Permissive	n/a	n/a
File extension	n/a	n/a	Permissive	n/a
File size	n/a	n/a	Permissive	n/a
File destination	n/a	n/a	Permissive	n/a
Date modified	n/a	n/a	n/a	Restrictive
Date created	n/a	n/a	n/a	Restrictive
Other file dates	n/a	n/a	n/a	Restrictive

Dependencies: FMT_MSA.1(a) Management of security attributes
FMT_MSA.1(b) Management of security attributes
FMT_MSA.1(c) Management of security attributes
FMT_MSA.1(d) Management of security attributes
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*management of security functions behaviour, management of security attributes*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Admin Role, Limited Admin Roles*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.5 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [*thirty minutes of user inactivity*].

Dependencies: No dependencies

6.2.6 Class EXT_FIH: Incident Handling

EXT_FIH_ARP.1 Incident alarms

Hierarchical to: No other components.

EXT_FIH_ARP.1.1

The TSF shall take

[

One or more of the following notification and escalation actions depending upon the configured policy:

- *For DLP Network:*
 - *Notify sender*
 - *Notify sender's manager*
 - *Notify identified end-user*
 - *Notify identified group*
 - *Notify administrator*
 - *Notify assignee*
 - *Notify assignee's manager*
 - *Increase severity of the incident*
- *For DLP Endpoint:*
 - *Notify end-user*
 - *Notify end-user's manager*
 - *Notify other end-user*
 - *Notify group*
 - *Notify assignee*
 - *Notify assignee's manager*
 - *Increase severity of the incident*
- *For DLP Datacenter:*
 - *Notify file owner*
 - *Notify file owner's manager*
 - *Notify end-user*
 - *Notify group*

- *Notify assignee*
- *Notify assignee's manager*
- *Increase severity of the incident*

] upon detection of a potential incident.

Dependencies: EXT_FIH_SAA.1 Incident analysis

EXT_FIH_SAA.1 Incident analysis

Hierarchical to: No other components.

EXT_FIH_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the generated policy-based events and based upon these rules generate an incident.

EXT_FIH_SAA.1.2.

The TSF shall enforce the following rules for monitoring policy-based events:

- Accumulation or combination of
 - [
 - The following rules:*
 - *For each event generated by DLP Network, create an incident;*
 - *For all events generated by DLP Endpoint, if the number of events by a given end-user within the configured time window matches the configured level in the policy, generate an incident;*
 - *For events generated by DLP Datacenter, create an incident for all events for a given policy that, as configured singly or in combination,*
 - *occur on a single computer,*
 - *are owned by the same file owner, or*
 - *are within the same shared directories*
 -]
 - known to indicate a potential incident;
- [no other rules].

Dependencies: FDP_ACC.1(b) Subset access control
 FDP_ACF.1(b) Security attribute based access control
 FDP_ACC.1(c) Subset access control
 FDP_ACF.1(c) Security attribute based access control
 FDP_ACC.1(d) Subset access control
 FDP_ACF.1(d) Security attribute based access control

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.1. Table 12 - Assurance Requirements summarizes the requirements.

Table 12 - Assurance Requirements

Assurance Requirements	
Class ALC : Life Cycle 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.1 Basic Flaw Remediation
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional and assurance requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 13 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
User Data Protection	FDP_ACC.1(a)	Subset access control
	FDP_ACF.1(a)	Security attribute based access control
	FDP_ACC.1(b)	Subset access control
	FDP_ACF.1(b)	Security attribute based access control
	FDP_ACC.1(c)	Subset access control
	FDP_ACF.1(c)	Security attribute based access control
	FDP_ACC.1(d)	Subset access control
	FDP_ACF.1(d)	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication	FIA_UAU.2	User authentication before any action

TOE Security Function	SFR ID	Description
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1(a)	Management of security attributes
	FMT_MSA.1(b)	Management of security attributes
	FMT_MSA.1(c)	Management of security attributes
	FMT_MSA.1(d)	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
TOE Access	FTA_SSL.3	TSF-initiated termination
Incident Handling	EXT_FIH_ARP.1	Incident alarms
	EXT_FIH_SAA.1	Incident analysis

7.1.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation and viewing of audit data. The TOE captures logs of management events such as policy changes. Start-up and shutdown of the audit functions are implied by the initiation and cessation of the generation of any audit records.

The DLP Enterprise Manager and each of the DLP controllers, coordinators, and agents generate audit logs. Each of the DLP controllers, coordinators, and agents download audit logs to the DLP Enterprise Manager, which then stores them on the Enterprise Results database. Administrators can then analyze or forward the audits to Customer Support. Some audits generated by the DLP Network are stored on the syslog of the DLP Network device that generates them.

Administrators can also view audits captured by the TOE through the DLP Enterprise Manager GUI, and some of the logs captured by DLP Network through the CLI on each of the DLP Network appliances.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1.

7.1.2 User Data Protection

The TOE allows authorized administrators to enforce a rigid Administrative Access Control Security Functional Policy for administrators accessing the TOE. Administrators with the Admin Role have permission to perform any and all administrative functions on the TOE. Other administrators may access user interface menu items, policies, incidents, events, reports, and administrative management data if given the appropriate permissions by the Admin Role. Depending on permissions granted, administrators may create, update, delete, or modify the data to which access has been granted. Access is granted to objects based on the administrator's role, group, and user ID.

The TOE enforces administrator-configurable Security Functional Policies on access to sensitive data, as follows:

DLP Network SFPs enforce rules governing the ability of end-users to transmit sensitive data across or out of the network. These policies base their decisions on such things as the content of the data (words, phrases, character patterns, and document fingerprints), and on other attributes such as protocol, file size, sender, recipient, source IP, destination IP, source host, destination host, destination URL, and which DLP device detected the violation. The resulting possible policy actions include: allow the transmission, record an event, block the transmission, encrypt the transmission¹⁴, and quarantine the data transmitted. (Note that the DLP Network Access Control SFP is executed before the DLP Network Information Flow Control SFP.)

DLP Endpoint SFPs enforce rules governing the ability of end-users to take actions on data on targeted machines. These policies base their decisions on such things as the content of the data (words, phrases, character patterns, and document fingerprints), and on other attributes such as file extension, file size, file source, and file destination. End-user actions that are monitored include copy, paste, cut, move, print, capture, send, and embed. The resulting possible policy actions include: allow the end-user action, record an event, notify the end-user, request a justification from the end-user, and block the end-user action.

DLP Datacenter SFPs enforce rules governing the suitability of files on targeted machines to store sensitive data. These policies base their decisions on such things as the content of the data (words, phrases, character patterns, and document fingerprints), and on other attributes such as date the file was last modified, date the file was created, and other file dates. The resulting possible policy actions include: allow the retention of the data, and record an event.

TOE Security Functional Requirements Satisfied: FDP_ACC.1(a), FDP_ACF.1(a), FDP_ACC.1(b), FDP_ACF.1(b), FDP_ACC.1(c), FDP_ACF.1(c), FDP_ACC.1(d), FDP_ACF.1(d).

7.1.3 Identification and Authentication

Administrators must be identified and authenticated before they can perform any management tasks on the TOE or TOE data. Administrators authenticate to the DLP Enterprise Manager with a user ID and password through a web browser, and to the DLP Network appliances with a user ID and password through the CLI. Once administrators are authenticated, they may perform management tasks as allowed by their permissions.

TOE Security Functional Requirements Satisfied: FIA_UAU.2, FIA_UID.2.

7.1.4 Security Management

Security Management functions define roles and role management functionality of the TOE. The TOE maintains an Admin Role, which has access to all TOE management functionality. The Admin Role can define one or more

¹⁴ However, encryption is done by a third-party product, and is outside the scope of this CC evaluation.

Limited Admin Roles, and assign permissions to them as appropriate. Each administrator is also assigned a user group and user identifier (ID), which help to further define the permissions granted. The functions administrators may manage, depending on permissions granted, include: users, groups, roles, DLP Network configuration, DLP Endpoint configuration, DLP Datacenter configuration, content blades, notification email server configuration, message notification templates, policies, reports, policy templates, system maintenance, incidents, and events.

Permissive or Restrictive default values for security attributes defined by the Security Functional Policies are enforced by the TSF, and alternative default values may be specified by the Admin Role.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.1(c), FMT_MSA.1(d), FMT_MSA.3, FMT_SMF.1, FMT_SMR.1.

7.1.5 TOE Access

The TOE terminates an interactive session after thirty minutes of user inactivity. This time interval is non-configurable.

TOE Security Functional Requirements Satisfied: FTA_SSL.3.

7.1.6 Incident Handling

Analysis of events generated by the TOE is performed, and a determination about whether an incident should be generated is made. For each DLP product, policies are configured to generate incidents based on specific event data. DLP Network generates an incident for every event generated. DLP Endpoint generates an incident for each pre-configured number of events generated by a given end-user within a specified period of time. DLP Datacenter generates an incident for all events for a given policy that either occur on a single computer, are owned by the same file owner, or are within the same shared directories. For each incident generated, the action taken in response by the TOE is defined. Possible actions by DLP Network are 'audit', 'quarantine', 'block', 'notify sender', 'notify sender's manager', 'notify identified end-user', 'notify identified group', 'notify administrator', 'notify assignee', 'notify assignee's manager', and 'increase severity of the incident'. Possible actions by DLP Endpoint are 'justify', 'block', 'notify end-user', 'notify end-user's manager', 'notify other end-user', 'notify group', 'notify assignee', 'notify assignee's manager', and 'increase severity of the incident'. Possible actions by DLP Datacenter are 'notify file owner', 'notify file owner's manager', 'notify end-user', 'notify group', 'notify assignee', 'notify assignee's manager', and 'increase severity of the incident'.

TOE Security Functional Requirements Satisfied: EXT_FIH_ARP.1, EXT_FIH_SAA.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Parts 2 and 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1. There are two extended SFRs contained within this ST: EXT_FIH_ARP.1 and EXT_FIH_SAA.1. These were included to define the security functionality provided by the generation of incidents by the TOE.

There are no protection profile claims for this Security Target.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives is complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 14 - Threats:Objectives Mapping

Threats	Objectives	Rationale
T.IA A threat agent may attempt to compromise the TOE by attempting actions that it is not authorized to perform on the TOE.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators, may exercise such control.	O.ADMIN requires that only authorized TOE administrators be allowed to perform management actions on the TOE. This prevents unauthorized users from performing actions that compromise the TOE.
	O.IDAUTH The TOE shall require that administrators of the TOE be identified and authenticated before allowing any TSF-mediated activity to be performed by them.	O.IDAUTH requires that all TOE administrators be identified and authenticated before being allowed to perform any actions on the TOE. This ensures that only authenticated administrators are able to access the TOE.
	O.SEC_ACCESS The TOE shall ensure that only authorized administrators are granted access to the security functions, configurations, and associated data.	O.SEC_ACCESS requires that only authorized administrators be given access to the TOE's security functions, configurations, and associated data. This ensures that no unauthorized users are permitted to perform such actions.

Threats	Objectives	Rationale
<p>T.INFO_CAPTURE</p> <p>An external attacker or malicious insider may sniff the communication channel between the TOE and a remote administrator in order to capture or modify information sent between the two.</p>	<p>OE.SECURECOMMUNICATION</p> <p>The operational environment will provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote administrators.</p>	<p>OE.SECURECOMMUNICATION requires that information being transmitted between the TOE and TOE administrators never be modified or disclosed. This prevents external attackers and malicious insiders from capturing or modifying that data.</p>
<p>T.MASQUERADE</p> <p>A threat agent masquerading as the TOE may capture valid identification and authentication data for a legitimate administrator of the TOE in order to gain unauthorized access to the TOE.</p>	<p>OE.SECURECOMMUNICATION</p> <p>The operational environment will provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote administrators.</p>	<p>OE.SECURECOMMUNICATION requires that information being transmitted between the TOE and TOE administrators never be modified or disclosed. This prevents threat agents from capturing identification and authentication data as it is transmitted.</p>
<p>T.NO_AUDIT</p> <p>A threat agent may perform security-relevant operations on the TOE without being held accountable for it.</p>	<p>OE.TIMESTAMP</p> <p>The TOE Environment must provide reliable timestamps for the TOE's use.</p>	<p>OE.TIMESTAMP requires that the TOE Environment provide timestamps for use in the audit logs. This helps prevent threat agents from performing security-relevant actions without being held accountable.</p>
	<p>OE.LOG</p> <p>The TOE Environment shall securely store logs of management operations performed on the TOE that are generated by the TOE.</p>	<p>OE.LOG requires that the TOE Environment store logs captured by the TOE of management operations performed on the TOE. This prevents threat agents from performing security-relevant actions without detection.</p>
	<p>O.LOG</p> <p>The TOE shall generate logs of management operations performed on the TOE.</p>	<p>O.LOG requires that the TOE capture logs of management operations performed on the TOE. This prevents threat agents from performing security-relevant actions without detection.</p>
<p>T.SENSITIVE_CONTENT</p> <p>A threat agent may access non-public or confidential information held by targeted assets in violation of the TOE's security functional policies.</p>	<p>O.INCIDENT</p> <p>The TOE shall analyze all events and generate incidents according to configured policies.</p>	<p>O.INCIDENT requires that the TOE analyze all events generated by the TOE, and generate incidents according to configured policy. Administrators use these incidents to determine if policy violations involving non-public or confidential information have occurred.</p>
	<p>O.NOTIFICATION</p>	<p>O.NOTIFICATION requires that the TOE generate and deliver alerts</p>

Threats	Objectives	Rationale
	<p>The TOE shall generate and deliver alerts according to configured policies upon generating an incident.</p>	<p>according to configured policies upon generating an incident. This alerts the administrator to policy violations involving the access or transmission of non-public or confidential information.</p>
	<p>O.SENSITIVE_CONTENT</p> <p>The TOE shall take specified actions on transmissions, end-user actions, and files identified as containing or accessing non-public or confidential information.</p>	<p>O.SENSITIVE_CONTENT requires that the TOE take specified actions on transmissions, end-user actions, and files identified as containing or accessing non-public or confidential information. This prevents threat agents from accessing that information.</p>
<p>T.UNAUTH</p> <p>A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.</p>	<p>O.ADMIN</p> <p>The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators, may exercise such control.</p>	<p>O.ADMIN requires that the TOE allow only authorized TOE administrators to manage its functions and data. This prevents unauthorized users from gaining access to security data on the TOE.</p>
<p>T.INT_CONF</p> <p>An unauthorized user may attempt to disclose or compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.</p>	<p>OE.SECURECOMMUNICATION</p> <p>The operational environment will provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote administrators.</p>	<p>OE.SECURECOMMUNICATION requires that the information passing between separate parts of the TOE and between the TOE and trusted remote administrators be protected from unauthorized disclosure and modification. This prevents unauthorized users from disclosing or modifying the data collected and produced by the TOE.</p>
	<p>O.IDAUTH</p> <p>The TOE shall require that administrators of the TOE be identified and authenticated before allowing any TSF-mediated activity to be performed by them.</p>	<p>O.IDAUTH requires that the TOE identify and authenticate administrators before allowing any TSF-mediated activity to be performed by them. This prevents unauthorized users from accessing the data collected by the TOE.</p>
	<p>O.SEC_ACCESS</p> <p>The TOE shall ensure that only authorized administrators are granted access to the security functions, configurations, and associated data.</p>	<p>O.SEC_ACCESS requires that the TOE ensure that only authorized administrators be granted access to the data of the TOE. This prevents unauthorized users from accessing the data collected and produced by the TOE.</p>

Threats	Objectives	Rationale
T.DATALOSS An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.	OE.SECURECOMMUNICATION The operational environment will provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote administrators.	OE.SECURECOMMUNICATION requires that information passing between separate parts of the TOE and between the TOE and trusted remote administrators be protected from unauthorized disclosure and modification. This prevents unauthorized users from removing or destroying data collected and produced by the TOE.
	O.IDAUTH The TOE shall require that administrators of the TOE be identified and authenticated before allowing any TSF-mediated activity to be performed by them.	O.IDAUTH requires that administrators of the TOE be identified and authenticated before allowing any TSF-mediated activity to be performed by them. This prevents unauthorized users from removing or destroying data collected and produced by the TOE.
	O.SEC_ACCESS The TOE shall ensure that only authorized administrators are granted access to the security functions, configurations, and associated data.	O.SEC_ACCESS requires that the TOE ensure that only authorized administrators be granted access to the TOE data. This prevents unauthorized users from removing or destroying data collected and produced by the TOE.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no policies defined for this Security Target.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 15 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.LOCATE The TOE resides in a physically controlled access facility that prevents unauthorized physical access.	NOE.TRUSTED_ENV The TOE shall reside in a physically secure location, safe from compromise by malicious insiders or outsiders.	NOE.TRUSTED_ENV ensures that the TOE shall reside in a physically secure location, thereby preventing unauthorized physical access.

Assumptions	Objectives	Rationale
<p>A.NOEVIL</p> <p>Authorized administrators who manage the TOE are non-hostile and are appropriately trained to use, configure, and maintain, the TOE, and follow all guidance.</p>	<p>NOE.TRUSTED_ENV</p> <p>The TOE shall reside in a physically secure location, safe from compromise by malicious insiders or outsiders.</p>	<p>NOE.TRUSTED_ENV ensures that authorized administrators shall not compromise the TOE.</p>
<p>A.SECURECOMMUNICATION</p> <p>It is assumed that the IT environment will provide a secure line of communication between distributed portions of the TOE and between the TOE and remote administrators.</p>	<p>OE.SECURECOMMUNICATION</p> <p>The operational environment will provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote administrators.</p>	<p>OE.SECURECOMMUNICATIONS ensures that all communications between TOE components and between the TOE and remote administrators is protected.</p>

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

A family of EXT_FIH requirements was created to specifically address incidents generated by the TOE. The purpose of this family of requirements is to define how incidents are identified and generated by each DLP product (DLP Network, DLP Endpoint, and DLP Datacenter). These requirements exhibit functionality that can be easily documented in the Development class assurance evidence and thus do not require any additional Assurance Documentation.

EXT_FIH_SAA.1 was stated explicitly to specify that under what conditions an incident will be generated for each of the DLP products (DLP Network, DLP Endpoint, and DLP Datacenter). This requirement was modeled after FAU_SAA.1, which uses audit records as the source of the analysis. EXT_FIH_SAA.1 uses the events generated by the TOE as the source of the analysis.

EXT_FIH_ARP.1 was stated explicitly to specify that notifications will be sent out, or other actions taken, when an incident is generated. This requirement was modeled after FAU_ARP.1, which uses the potential violations identified by EXT_FIH_SAA.1 as the reason for the action. EXT_FIH_ARP.1 uses the incidents generated by the TOE as the reason for the action.

8.4 Rationale for Extended TOE Security Assurance Requirements

No extended Security Assurance Requirements are defined for this Security Target.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 16 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE administrators with the appropriate privileges and only those TOE administrators, may exercise such control.	FAU_SAR.1 Audit review	The SFR meets the objective by allowing TOE administrators to review audit logs generated by the TOE.
	FMT_MOF.1 Management of security functions behaviour	The SFR meets the objective by requiring that TOE administrators be allowed to perform security functions according to the role and permissions granted to them.
	FMT_MSA.1(a) Management of security attributes	The SFR meets the objective by requiring that only the Admin Role and authorized Limited Admin roles be permitted to perform all management actions on the TOE, according to the Administrative Access Control Security Functional Policy.
	FMT_MSA.3 Static attribute initialisation	The SFR meets the objective by requiring that only the Admin Role specify alternative default values for security attributes.
	FMT_SMF.1 Specification of management functions	The SFR meets the objective by providing management of security functions behaviour and management of security attributes.
	FMT_SMR.1 Security roles	The SFR meets the objective by maintaining the roles Admin Role and Limited Admin Roles, and by associated users with these roles.
O.IDAUTH The TOE shall require that administrators of the TOE be identified and authenticated before allowing any TSF-mediated activity to be performed by them.	FIA_UAU.2 User authentication before any action	The SFR meets the objective by requiring that TOE administrators be successfully authenticated before allowing any TSF-mediated actions to be performed by them.
	FIA_UID.2	The SFR meets the objective by requiring that TOE administrators be

Objective	Requirements Addressing the Objective	Rationale
	User identification before any action	successfully identified before allowing any TSF-mediated actions to be performed by them.
	FTA_SSL.3 TSF-initiated termination	The SFR meets the objective by terminating administrator sessions when a specified time interval of inactivity has passed. This prevents unauthorized users from gaining access to a live session.
<p>O.SEC_ACCESS</p> <p>The TOE shall ensure that only authorized administrators are granted access to the security functions, configurations, and associated data.</p>	<p>FDP_ACC.1(a)</p> <p>Subset access control</p>	<p>The SFR meets the objective by ensuring that authorized administrators are permitted to access security functions, configurations, and data based on the Administrative Access Control Security Functional Policy.</p>
	<p>FDP_ACF.1(a)</p> <p>Security attribute based access control</p>	<p>The SFR meets the objective by enforcing the Administrative Access Control Security Functional Policy, by which authorized administrators are permitted to access security functions, configurations, and data based on the permissions granted to their roles, groups, and user ids.</p>
	<p>FMT_MSA.1(a)</p> <p>Management of security attributes</p>	<p>The SFR meets the objective by requiring that only the Admin Role and authorized Limited Admin roles be permitted to perform all management actions on the TOE, according to the Administrative Access Control Security Functional Policy.</p>
	<p>FMT_MSA.1(b)</p> <p>Management of security attributes</p>	<p>The SFR meets the objective by requiring that only the Admin Role and authorized Limited Admin roles be permitted to perform management actions on the DLP Network policies, according to the DLP Network Access Control Security Functional Policy and the DLP Network Information Flow Control Security Functional Policy.</p>
	<p>FMT_MSA.1(c)</p> <p>Management of security attributes</p>	<p>The SFR meets the objective by requiring that only the Admin Role and authorized Limited Admin roles be permitted to perform management actions on the DLP Endpoint policies, according to the DLP Endpoint</p>

Objective	Requirements Addressing the Objective	Rationale
		Security Functional Policy.
	FMT_MSA.1(d) Management of security attributes	The SFR meets the objective by requiring that only the Admin Role and authorized Limited Admin roles be permitted to perform management actions on the DLP Datacenter policies, according to the DLP Datacenter Security Functional Policy.
	FMT_MSA.3 Static attribute initialisation	The SFR meets the objective by requiring that only the Admin Role specify alternative default values for security attributes.
	FTA_SSL.3 TSF-initiated termination	The SFR meets the objective by ensuring that only authorized administrators gain access to the security functions, configurations, and associated data of the TOE by terminating interactive sessions after 30 minutes of inactivity.
O.LOG The TOE shall generate logs of management operations performed on the TOE.	FAU_GEN.1 Audit Data Generation	The SFR meets the objective by generating logs for management actions on the TOE.
	FAU_SAR.1 Audit review	The SFR meets the objective by allowing review of audit logs generated by the TOE.
O.INCIDENT The TOE shall analyze all events and generate incidents according to configured policies.	EXT_FIH_SAA.1 Incident analysis	The SFR meets the objective by analyzing all events and generating incidents according to configured policies.
O.NOTIFICATION The TOE shall generate and deliver alerts according to configured policies upon generating an incident.	EXT_FIH_ARP.1 Incident alarms	The SFR meets the objective by alerting TOE administrators to the generation of an incident.
O.SENSITIVE_CONTENT The TOE shall take specified actions on transmissions, end-user actions, and files identified as	FDP_ACC.1(b) Subset access control	The SFR meets the objective by ensuring that end-users are restricted in transmitting data containing sensitive information, according to the DLP Network Access Control Security

Objective	Requirements Addressing the Objective	Rationale
containing or accessing non-public or confidential information.		Functional Policy.
	FDP_ACF.1(b) Security attribute based access control	The SFR meets the objective by enforcing the DLP Network Access Control Security Functional Policy, by which end-users are restricted from transmitting data containing sensitive information.
	FDP_ACC.1(c) Subset access control	The SFR meets the objective by ensuring that end-users are restricted from copying, pasting, cutting, moving, saving, printing, capturing, sending, or embedding data containing sensitive information, according to the DLP Endpoint Security Functional Policy.
	FDP_ACF.1(c) Security attribute based access control	The SFR meets the objective by enforcing the DLP Endpoint Security Functional Policy, by which end-users are restricted from copying, pasting, cutting, moving, saving, printing, capturing, sending, or embedding data containing sensitive information.
	FDP_ACC.1(d) Subset access control	The SFR meets the objective by ensuring that files on desktops, laptops, servers, or data repositories are restricted from containing sensitive information, according to the DLP Datacenter Security Functional Policy.
	FDP_ACF.1(d) Security attribute based access control	The SFR meets the objective by enforcing the DLP Datacenter Security Functional Policy, by which files on desktops, laptops, servers, or data repositories may or may not contain sensitive information.
	FDP_IFC.1 Subset information flow control	The SFR meets the objective by ensuring that end-users are restricted in transmitting data containing sensitive information, according to the DLP Network Information Flow Control Security Functional Policy.
	FDP_IFF.1 Simple security attributes	The SFR meets the objective by enforcing the DLP Network Information Flow Control Security Functional Policy, by which end-users

Objective	Requirements Addressing the Objective	Rationale
		are restricted from transmitting data containing sensitive information.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 17 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 17 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Timestamps are provided by the operational environment, therefore this dependency is met.
FAU_SAR.1	FAU_GEN.1	✓	
FDP_ACC.1(a)	FDP_ACF.1(a)	✓	
FDP_ACF.1(a)	FMT_MSA.3	✓	
	FDP_ACC.1(a)	✓	
FDP_ACC.1(b)	FDP_ACF.1(b)	✓	
FDP_ACF.1(b)	FDP_ACF.1(b)	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_MSA.3	✓	
FDP_ACC.1(c)	FDP_ACF.1(c)	✓	
FDP_ACF.1(c)	FMT_MSA.3	✓	
	FDP_ACC.1(c)	✓	
FDP_ACC.1(d)	FDP_ACF.1(d)	✓	
FDP_ACF.1(d)	FMT_MSA.3	✓	
	FDP_ACC.1(d)	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FIA_UAU.2	FIA_UID.1	✓	Because FIA_UID.2 is hierarchical to FIA_UID.1, and FIA_UID.2 is included in this evaluation, this dependency is met.
FIA_UID.2	None		
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(a)	FMT_SMR.1	✓	
	FDP_ACC.1(a)	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(b)	FDP_ACC.1(b)	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(c)	FMT_SMF.1	✓	
	FDP_ACC.1(c)	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(d)	FDP_ACC.1(d)	✓	
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1(b)	✓	
	FMT_MSA.1(c)	✓	
	FMT_MSA.1(d)	✓	
	FMT_MSA.1(a)	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None		
FMT_SMR.1	FIA_UID.1	✓	Because FIA_UID.2 is hierarchical to FIA_UID.1, and FIA_UID.2 is included in this evaluation, this dependency is met.
FTA_SSL.3	None		
EXT_FIH_ARP.1	EXT_FIH_SAA.1	✓	
EXT_FIH_SAA.1	FDP_ACC.1(b)	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FDP_ACF.1(b)	✓	
	FDP_ACC.1(c)	✓	
	FDP_ACF.1(c)	✓	
	FDP_ACC.1(d)	✓	
	FDP_ACF.1(d)	✓	

9 Acronyms and Terminology

9.1 Acronyms

Table 18 - Acronyms

Acronym	Definition
CC	Common Criteria
CLI	Command Line Interface
DLP	Data Loss Prevention
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol
ID	Identifier
IM	Instant Messaging
IP	Internet Protocol
IT	Information Technology
NAS	Network-Attached Storage
NPI	Non-Public Personal Information
OSP	Organizational Security Policy
PCI	Payment Card Industry
PII	Personally Identifiable Information

Acronym	Definition
PP	Protection Profile
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

9.2 Terminology

End-users are those individuals accessing the targeted computers on the network.

Administrators are those individuals who perform management functions on the TOE.