RSA, The Security Division of EMC

RSA® Data Loss Prevention Suite v9.0

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.7

Prepared for:

RSA, The Security Division of EMC
174 Middlesex Turnpike
Bedford, MA 01730
United States of America

Phone: +1 877 722 4900
Fax: +1 781 515 5010
http://www.rsa.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the RSA® Data Loss Prevention Suite v9.0, 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 is divided into nine sections, as follows:

- 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 (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 (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 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 Terms (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 v9.0 Security Target
ST Version	Version 0.7
ST Author	Corsec Security, Inc.
ST Publication Date	9/17/2012
TOE Reference	RSA® Data Loss Prevention Suite v9.0 (Complete version numbers with build as follows: RSA DLP Network v9.0.0.10027, RSA DLP Endpoint v9.0.0.10041, RSA DLP Datacenter v9.0.0.10041, RSA DLP Enterprise Manager v9.0.0.10051)
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[1]
- DLP Network Exchange Transport Agent

The DLP Endpoint product consists of the following components:

- DLP Enterprise Coordinator
- DLP Endpoint Site Coordinator
- DLP Endpoint Agent

The DLP Datacenter product consists of the following components:

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

The DLP Enterprise Manager is the centralized point of control for the components listed above, and exists as an individual component comprising the DLP Enterprise Manager product.

Figure 1 below shows the four DLP products available in the DLP Suite. Note: The DLP Datacenter and DLP Endpoint components when deployed individually in stand-alone mode require a DLP Enterprise Coordinator; however, only one DLP Enterprise Coordinator is supported when deployed as a suite.

[1] ICAP – Internet Content Adaptation Protocol

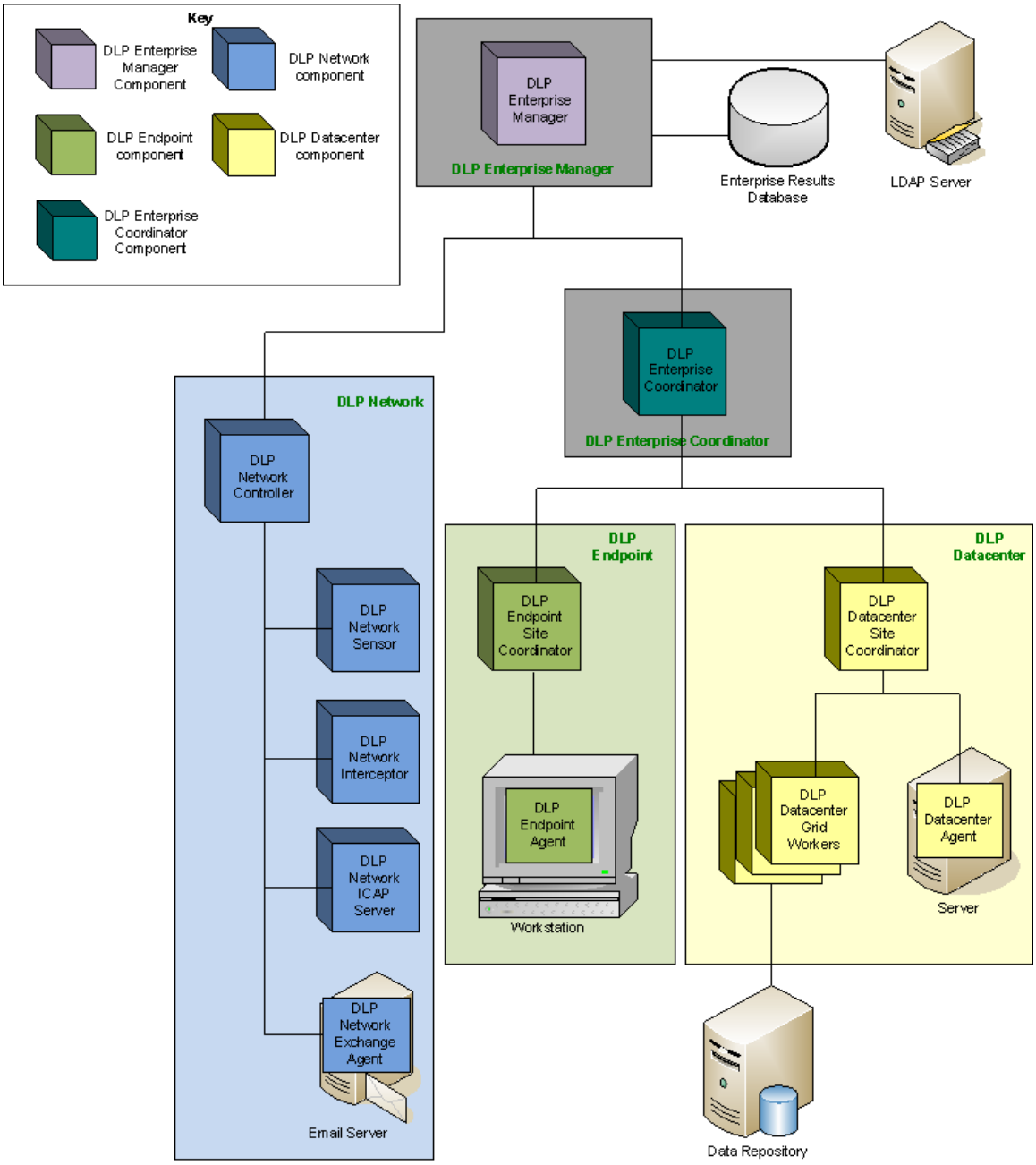

Figure 1 – Deployment Configuration of the TOE

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-user[2] 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

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

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. Administrators[3] 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, 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.

DLP Network is capable of transparently monitoring and mediating access control over a wide variety of application layer protocols, including:

- HyperText Transport Protocol (HTTP)
- Secure HTTP (HTTPS)
- ActiveSync
- Simple Mail Transport Protocol (SMTP)
- File Transfer Protocol (FTP)
- Telnet
- Internet Message Access Protocol (IMAP)
- Post Office Protocol 3 (POP3)
- Instant Messaging (IM) chat file transfer protocols, such as Yahoo, MSN[4], Google, and AOL[5]

Figure 2 below shows a typical DLP Network deployment.

[3] Administrators are those individuals who perform management functions on the TOE.
[4] MSN – Refers to the online service of MSN, formerly known as the Microsoft Network
[5] AOL – America Online

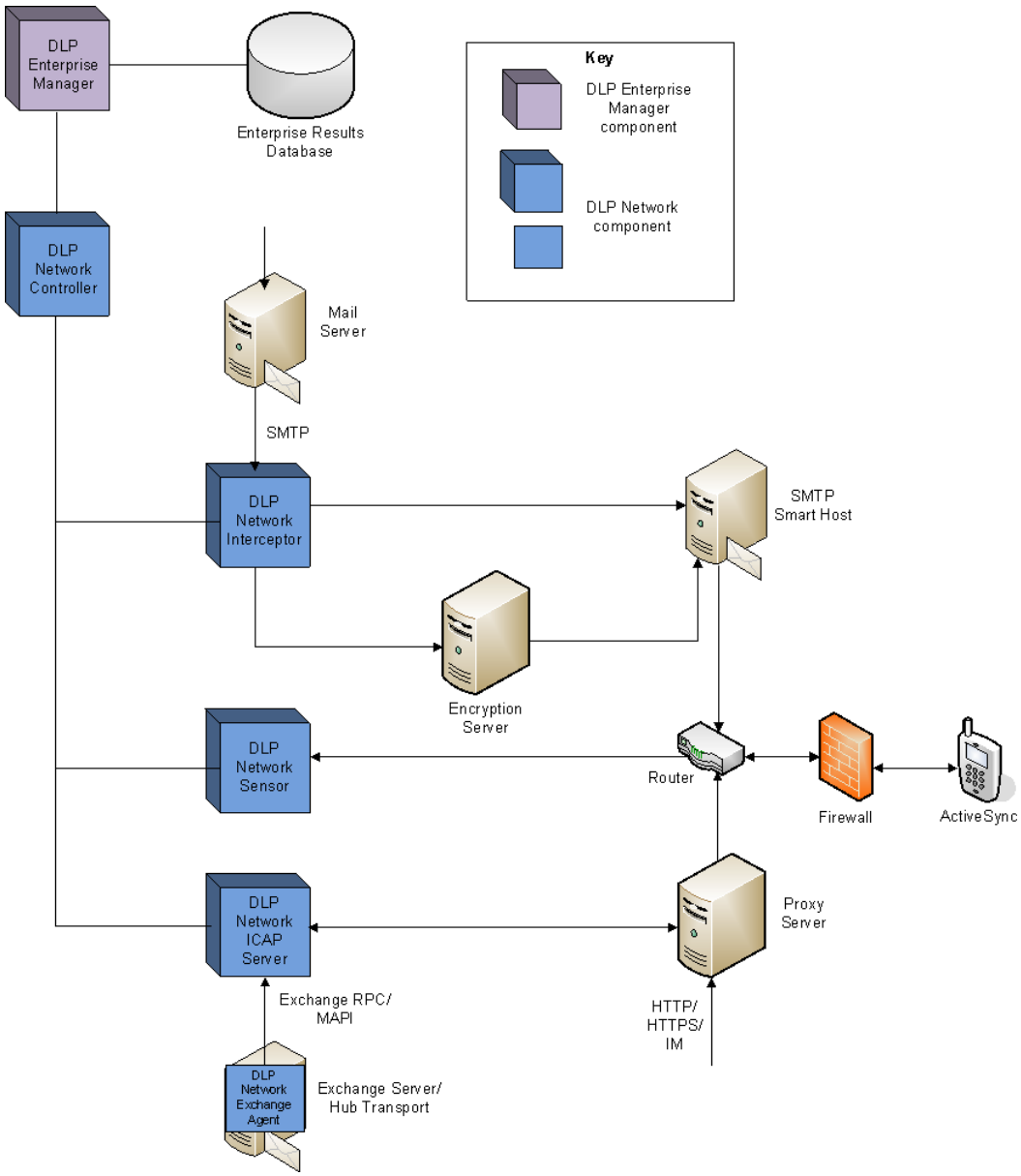

Figure 2 – Sample DLP Network Deployment[6]

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 both IPv4 and IPv6 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 purpose server devices that allow administrators to implement monitoring or blocking of HTTP, HTTPS, or FTP traffic containing sensitive content.

[6] RPC – Remote Procedure Call, MAPI – Messaging Application Programming Interface

The DLP Network ICAP Server can also be integrated directly with a Microsoft Exchange Server to monitor and control ActiveSync transmissions to prevent sensitive emails from leaving the organization for users accessing the email system from mobile devices. In addition, a specialized Exchange plug-in, known as the DLP Network Exchange Transport Agent, can be installed on the Exchange Hub Transport to provide an "internal ethical wall" that mediates the transfer of internal emails based on policy. Once configured, the DLP Network ICAP Server intercepts and analyzes all emails processed by the Hub Transport and applies actions based on content, sender and recipients, and other factors, ensuring that DLP is enforced internally as well as externally.

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.

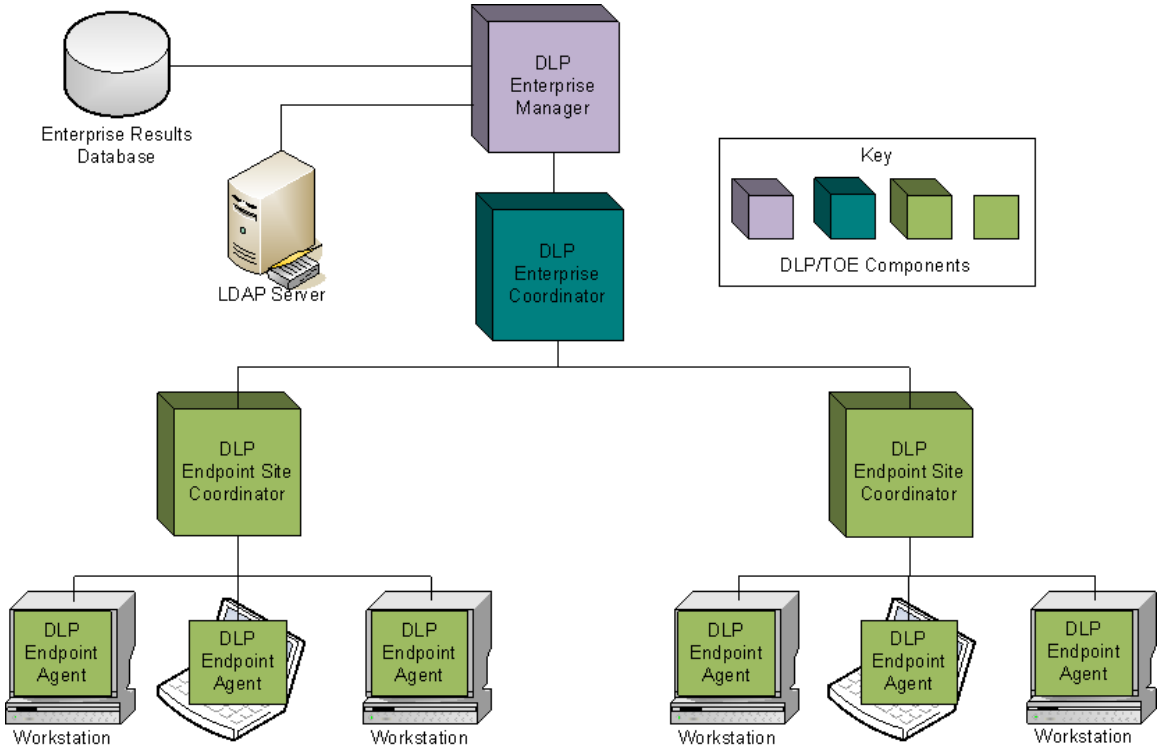

Figure 3 – Sample DLP Endpoint Deployment

DLP Endpoint consists of three components: DLP Endpoint Agent, DLP Endpoint Site Coordinator, and DLP 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. Administrators can also specify Custom Actions, which enable the DLP Endpoint Agent to enforce custom actions upon detection of a violation.

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 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 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 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.

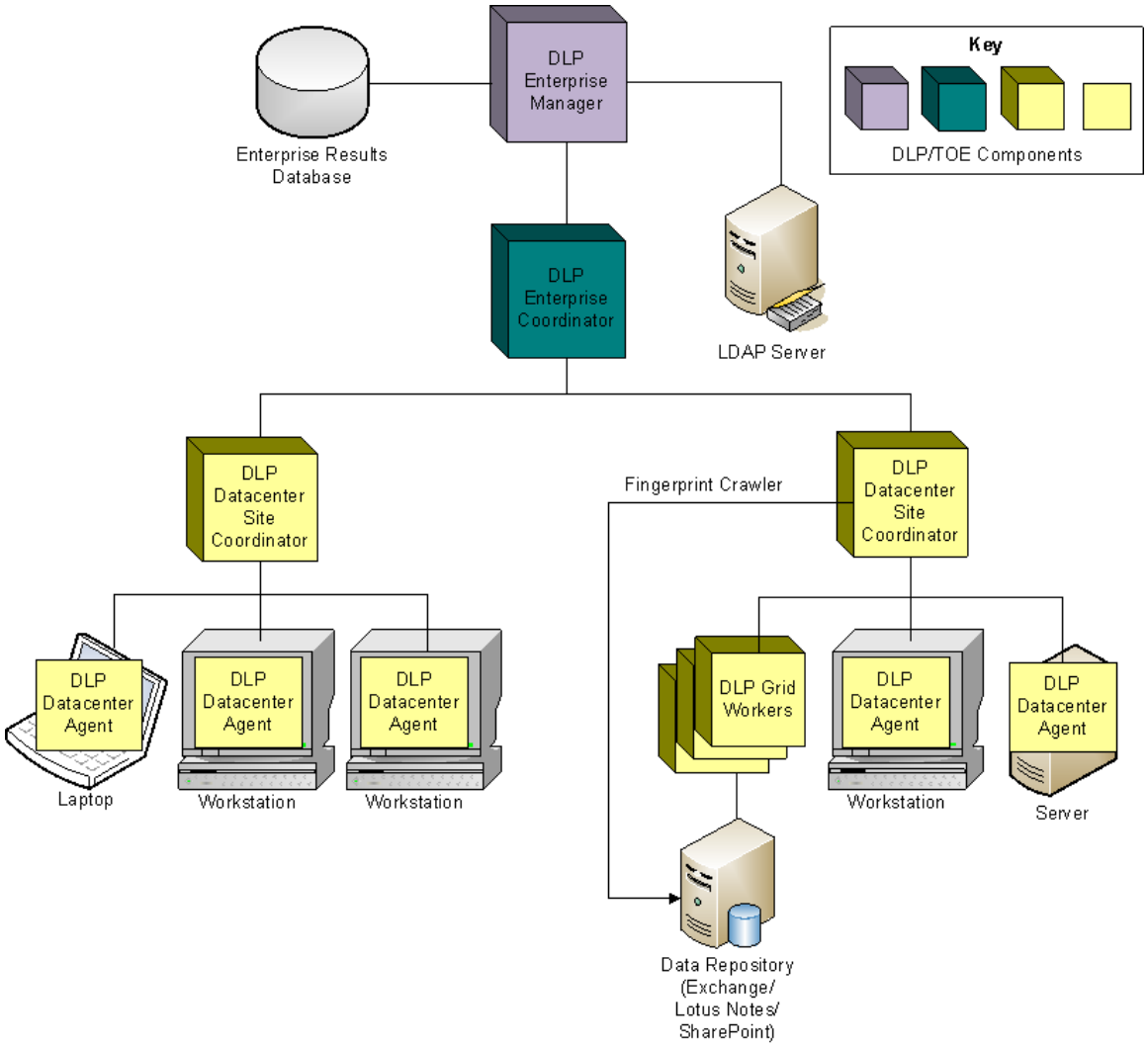

Figure 4 – Sample DLP Datacenter Deployment

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 Agents that are dispersed widely throughout the enterprise.

The DLP 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 four types of scan groups available: agent-scan groups for agent-based scans on desktops or laptops, grid-scan groups for grid scans on large data depositories, repository scan groups for file repositories, and repository scan groups for databases. 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 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 Enterprise Coordinator. The DLP 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 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 Enterprise Coordinator, which in turn forwards them to the DLP Enterprise Manager. The DLP Enterprise Manager displays the results to the administrator.

Repository scans are specialized types of grid scans which target the scanning of enterprise databases, such as SQL or Exchange, or file repositories such as document management systems like SharePoint or Documentum.

Two types identifying and detecting sensitive data in DLP Datacenter: described-content and fingerprinted-content. Described content detection is based on a set of rules that specify the nature of the sensitive content to be detected. This is typically used to identify specific strings or pattern matches within a file, such as a Social Security Number, or the word “Confidential”. Words, phrases, dictionaries, regular expressions, and heuristic programs all can be used in described-content scanning.

Fingerprinted-content detection involves identifying files or transmissions matching all or parts of known-sensitive content. This type is typically used in protecting content in which its location and sensitivity are known. For example, proprietary source code and binary data, Social Security Numbers and credit card numbers, or other confidential information that is stored in well-secured locations and must be monitored as it moves throughout the organization. Fingerprinting is performed by hashing sensitive files, parts of files, or database columns. Fingerprint crawlers create fingerprints on files and databases, and are installed on the DLP Datacenter Site Coordinator. Fingerprinted file/database contents are then analyzed and matched during normal DLP Datacenter Grid Worker or DLP Datacenter Agent scans.

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 over HTTPS. 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 events[7] and incidents[8], and view DLP documentation. The DLP Enterprise Manager stores and retrieves data to and from the Enterprise Results Database.

The DLP Enterprise Manager offers integration with partner products, such as Cisco IronPort Email Security Appliance, allowing TOE administrators to create and manage policies for external products. Policies for partner products provide Incident Handling, Escalation, and Notification rules as they do for native DLP policies. Partner product integration also provides administrators with methods for determining whether the policies are enabled or disabled on the TOE and the remote partner product. Policy bundles for partner products can be imported and exported into and out of the TOE using a standardized XML[9] format.

DLP Enterprise Manager integrates with an existing LDAP[10] directory, enabling TOE administrators to specify LDAP configurations which supply the TOE with user identity and credential attribute data. This information is used to support identification and authentication when configured to do so.

DLP Datacenter requires access credentials in order to deploy software to customer networks, read data from files or content repositories, and remediate files. As a result, the DLP Enterprise Manager includes a Credentials Management feature, which enables users to enter named credentials to enterprise resources, which are sent to the DLP Enterprise Coordinator during grid scans. Datacenter credentials are protected in the DLP Enterprise Manager database. Only authorized administrators can create or modify credentials. DLP Enterprise Manager restricts the ability to use credentials to users with sufficient role authorization.

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 TOE enforces the DLP Network Access Control SFP and Information Control SFP on network based activity, using rules composed of the following attributes:

- protocol characteristics, such as SMTP,
- words, phrases, or character patterns that match sensitivity criteria,
- transmission characteristics, such as sender or recipient,

[7] An "event" is any action or state detected by a TOE component that violates the security policy being enforced.
[8] "Incidents" are events or groups of events that require some sort of action to be taken by the TOE.
[9] XML – eXtensible Markup Language
[10] LDAP – Lightweight Directory Access Protocol

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

The TOE enforces the DLP Endpoint SFP on user actions, such as copying, moving, or saving files to various locations, printing, and network-based transfers, based on the following attributes:

- end-user ID or group,
- words, phrases, or character patterns that match sensitivity criteria,
- file attributes, such as file extensions, and
- file source and destination attributes, such as device type.

And for DLP Datacenter, the TOE enforces the DLP Datacenter SFP on data repositories using rules based on the following attributes:

- words, phrases, or character patterns that match sensitivity criteria,
- 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 encryption[11]

DLP Endpoint:

- Allow
- Audit only
- Notify and audit
- Justify and audit
- Block and audit
- Custom actions specified by an administrator

DLP Datacenter:

- Allow
- Audit only
- Apply RMS template[12]
- Grant permission
- Move to secure
- Quarantine

[11] 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.

[12] 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, or encrypting files. For more information, please see the *RSA DLP Datacenter v9.0 User Guide*.

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.

Applying RMS templates performs the actions designated in an RMS template, if the TOE is configured to use Active Directory RMS. The move to secure action places the files in the specified location. The grant permission action adds access control permissions to the file, granting rights to the specified end-user or group.

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

- DLP Network appliances;
- Customer-provided hardware for DLP Enterprise Manager, DLP Enterprise Coordinator, DLP Endpoint Site Coordinator, and DLP Datacenter Site Coordinator;
- Microsoft Internet Explorer 8 or Mozilla Firefox 7.0 web browser installed on the DLP Enterprise Manager server, or optionally a management workstation from which the TOE will be managed;
- Targeted customer workstations, servers, and laptops on which DLP Endpoint Agents, DLP Datacenter Agents, and DLP Datacenter Grid Workers will be installed;
- Microsoft Exchange Server on which the DLP Network Exchange Transport agent will be installed;
- Microsoft SQL[13] Server database to serve as the Enterprise Results Database;
- Microsoft Windows Active Directory RMS Server;
- Microsfot Windows Active Directory LDAP Server to support authentication of external users; and
- Proxy server for use with the DLP Network ICAP Server.

Table 2 lists the minimum hardware and software requirements for the TOE in the CC evaluated configuration:

[13] SQL – Structured Query Language

Table 2 – TOE Requirements

Component	Hardware Requirements	Software Requirements
TOE		

DLP Enterprise Manager	• Server-class computer, or VMware ESX (3.5, 4.0, or 4.1) host
	• 2 x 2 GHz[14] CPU[15]
	• 4 GB[16] RAM[17]
	• 1 GB Storage
		• Supported OS:
		  ○ 64-bit: Windows Server 2003 SP[18]2, R2 SP2, Windows Server 2008 SP2, R2
		  ○ 32-bit: Windows Server 2003 SP2, R2 SP2, Windows 2008 SP2
		• Evaluated OS:
		  ○ Microsoft Windows Server 2008 R2
		• Microsoft SQL Server 2005/2008 Command Line Query Utility
		• Microsoft SQL Server 2005/2008 Native Client
		• Supported Browsers:
		  ○ Microsoft Internet Explorer 7, 8, 9
		  ○ Mozilla Firefox 3.5.x, 3.6.x, 4.0 or greater
		• Evaluated Browsers:
		  ○ Microsoft Internet Explorer 8
		  ○ Mozilla Firefox 7.0
		• FIPS[19] Mode enabled[20]

DLP Datacenter Enterprise Coordinator	• Server-class computer, or VMware ESX (3.5, 4.0, or 4.1) host
	• 2 x 2 GHz CPU
	• 2 GB RAM
	• 20 GB Storage
		• Supported OS:
		  ○ 64-bit: Windows Server 2003 SP2, R2 SP2, Windows Server 2008 SP2, R2
		  ○ 32-bit: Windows Server 2003 SP2, R2 SP2, Windows 2008 SP2
		• Evaluated OS:
		  ○ Microsoft Windows Server 2008 R2
		• .NET Framework 2.0 SP2, 3.5 SP1
		• MDAC[21] 2.8 SP1
		• FIPS Mode enabled
		• Optional components required for database repository scanning (not evaluated):
		  ○ Oracle 10, 11, or 11g R2 OLEDB[22] driver
		  ○ IBM OLEDB Provider for DB2 or Microsoft OLEDB Provider for DB2
		  ○ Lotus Notes client v6.5.6, 8.0 and 8.5

[14] GHz - Gigahertz
[15] CPU – Central Processing Unit
[16] GB - Gigabyte
[17] RAM – Random Access Memory
[18] SP – Service Pack
[19] FIPS – Federal Information Processing Standard
[20] FIPS Mode must be enabled on all applicable components. For more information, please refer to the *Deploying RSA DLP in FIPS-Compliant Mode* technical note.
[21] MDAC – Microsoft Data Access Components
[22] OLEDB – Object Linking and Embedding, Database

Component	Hardware Requirements	Software Requirements

DLP Datacenter Site Coordinator	• Server-class computer, or VMware ESX (3.5, 4.0, or 4.1) host
	• 2 x 2 GHz CPU
	• 2 GB RAM
	• 40 GB Storage
		• Supported OS:
		  ○ 64-bit: Windows Server 2003 SP2, R2 SP2, Windows Server 2008 SP2, R2
		  ○ 32-bit: Windows Server 2003 SP2, R2 SP2, Windows 2008 SP2
		• Evaluated OS:
		  ○ Microsoft Windows Server 2008 R2
		• .NET Framework 2.0 SP2, 3.5 SP1
		• MDAC 2.8 SP1
		• FIPS Mode enabled
		• Optional components required for database repository scanning (not evaluated):
		  ○ Oracle 10, 11, or 11g R2 OLEDB driver
		  ○ IBM OLEDB Provider for DB2 or Microsoft OLEDB Provider for DB2
		  ○ Lotus Notes client v6.5.6, 8.0 and 8.5

DLP Datacenter Agent	• Workstation class computer, or VMware ESX (3.5, 4.0, or 4.1) host
	• 1 GB RAM
	• 250 MB[23] Storage
		• Supported OS:
		  ○ 64-bit: Windows Vista SP2, Windows Server 2003 SP2 and R2 SP2, Windows 7 Professional, Windows 7 Enterprise, Windows Server 2008 R2 and SP2
		  ○ 32-bit: Windows Vista SP2, Windows Server 2003 SP2 and R2 SP2, Windows 7 Professional, Windows 7 Enterprise, Windows Server 2008 SP2
		• Evaluated OS:
		  ○ Windows 7 (32-bit)
		• .NET Framework 2.0 SP2, 3.5 SP1
		• FIPS Mode enabled

[23] MB - Megabyte

Component	Hardware Requirements	Software Requirements

DLP Datacenter Grid Worker	• Workstation class computer, or VMware ESX (3.5, 4.0, or 4.1) host
	• 2 x 2 GHz CPU
	• 1 GB RAM
	• 20 GB Storage
		• Supported OS:
		  ○ 64-bit: Windows Vista SP2, Windows 7 Professional, Windows 7 Enterprise, Windows Server 2008 SP2, R2, Windows Server 2003 SP2, R2 SP2
		  ○ 32-bit: Windows Vista SP2, Windows Server 2003 SP2, R2 SP2, Windows 7 Professional, Windows 7 Enterprise, Windows Server 2008 SP2, Windows XP SP3
		• Evaluated OS:
		  ○ Windows 7 (32-bit)
		• .NET Framework 2.0 SP2, 3.5 SP1, or 4.0
		• MDAC 2.8 SP1
		• Optional components required for database repository scanning (not evaluated):
		  ○ Oracle 10, 11, or 11g R2 OLEDB Driver
		  ○ IBM OLEDB Provider for DB2 or Microsoft OLEDB Provider for DB2
		  ○ Lotus Notes client v6.5.6, 8.0 and 8.5
		• FIPS Mode enabled

DLP Endpoint Enterprise Coordinator	• Server-class computer, or VMware ESX (3.5, 4.0, or 4.1) host
	• 2 x 2 GHz CPU
	• 2 GB RAM
	• 20 GB Storage
		• Supported OS:
		  ○ 64-bit: Windows Server 2003 SP2, R2 SP2, Windows Server 2008 SP2, R2
		  ○ 32-bit: Windows Server 2003 SP2, R2 SP2, Windows 2008 SP2
		• Evaluated OS:
		  ○ Windows Server 2008 R2
		• .NET Framework 2.0 SP2, 3.5 SP1, or 4.0
		• FIPS Mode enabled

DLP Datacenter Site Coordinator	• Server-class computer, or VMware ESX (3.5, 4.0, or 4.1) host
	• 2 x 2 GHz CPU
	• 2 GB RAM
	• 40 GB Storage
		• Supported OS:
		  ○ 64-bit: Windows Server 2003 SP2, R2 SP2, Windows Server 2008 SP2, R2
		  ○ 32-bit: Windows Server 2003 SP2, R2 SP2, Windows 2008 SP2
		• Evaluated OS:
		  ○ Windows Server 2008 R2
		• .NET Framework 2.0 SP2, 3.5 SP1, or 4.0
		• FIPS Mode enabled

Component	Hardware Requirements	Software Requirements
DLP Datacenter Agent	• Workstation class computer, or VMware ESX (3.5, 4.0, or 4.1) host • 512 MB RAM • 250 MB Storage	• Supported OS: ○ 64-bit: Windows Vista SP2, Windows Server 2003 SP2 and R2 SP2, Windows 7 Professional, Windows 7 Enterprise, Windows Server 2008 R2 and SP2 ○ 32-bit: Windows Vista SP2, Windows Server 2003 SP2 and R2 SP2, Windows 7 Professional, Windows 7 Enterprise, Windows Server 2008 SP2 • Evaluated OS: ○ Windows 7 (32-bit) • .NET Framework 2.0 SP2, 3.5 SP1 • FIPS Mode enabled
DLP Network common appliance	• RSA Appliance • 2 x 2.53 GHz CPU • 32 GB RAM • 146 GB Storage	• TabOS based on CentOS v5.4 • FIPS Mode enabled
DLP Network Sensor appliance	• RSA Appliance • 2 x 2.53 GHz CPU • 8 GB RAM • 146 GB Storage	• TabOS based on CentOS v5.4 • FIPS Mode enabled
DLP Network Exchange Transport Agent	• Server-class computer • 64-bit processor • 8 GB RAM • 40 GB Storage	• Microsoft Windows Server 2008 R2 • Microsoft Exchange Server 2010 SP1
TOE Environment		
Enterprise Results Database	• Server-class computer • 2 x 2 GHz CPU • 2 GB RAM • 200 GB to 1 TB[24] Storage	• Supported OS: ○ 64-bit: Windows Server 2003 SP2, R2 SP2, Windows Server 2008 SP2, R2 ○ 32-bit: Windows Server 2003 SP2, R2 SP2, Windows Server 2008 SP2 • Evaluated OS: ○ Windows Server 2008 R2 • Supported database servers: ○ Microsoft SQL Server 2005 SP3 ○ Microsoft SQL Server 2008 SP1, R2 • Evaluated database server: ○ Microsoft SQL Server 2008 R2
LDAP Server	• Server-class computer or VMware ESX host • 2 GHz CPU • 2 GB RAM • 40 GB Storage	• Supported OS: ○ Windows Server 2003 SP2, R2 SP2, Windows Server 2008 SP2, R2 • Evaluated OS: ○ Windows Server 2003 SP2 • Active Directory Domain Controller role
Active Directory RMS Server	• Server-class computer or VMware ESX host • 2 GHz CPU • 2 GB RAM • 40 GB Storage	• Windows Server 2008 R2 • Active Directory RMS Server role
Proxy Server	• Varies	• Evaluated proxy server: ○ BlueCoat ProxySG (SGOS 5.x)

[24] TB - Terabyte

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 v9.0 software
- DLP Datacenter Enterprise Coordinator v9.0 software
- DLP Network Controller v9.0 software
- DLP Network Sensor v9.0 software
- DLP Network Interceptor v9.0 software
- DLP Network ICAP Server v9.0 software
- DLP Network Exchange Transport Agent v9.0 software
- DLP Endpoint Site Coordinator v9.0 software
- DLP Endpoint Agent v9.0 software
- DLP Datacenter Site Coordinator v9.0 software
- DLP Datacenter Agent v9.0 software
- DLP Datacenter Grid Worker v9.0 software.

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

- RSA DLP Network 9.0 User Guide
- RSA DLP Network 9.0 Deployment Guide
- RSA DLP Datacenter 9.0 User Guide
- RSA DLP Datacenter 9.0 Deployment Guide
- RSA DLP Endpoint 9.0 User Guide
- RSA DLP Endpoint 9.0 Deployment Guide
- RSA DLP 9.0 Release Notes
- RSA Data Loss Prevention Suite v9.0 Guidance Supplement, Document Version 0.1
- Deploying RSA DLP in FIPS-Compliant Mode Technical Note
- Guide to RSA DLP for Internal Email Technical Note
- Configuring Active Directory RMS for use with RSA DLP Technical Note

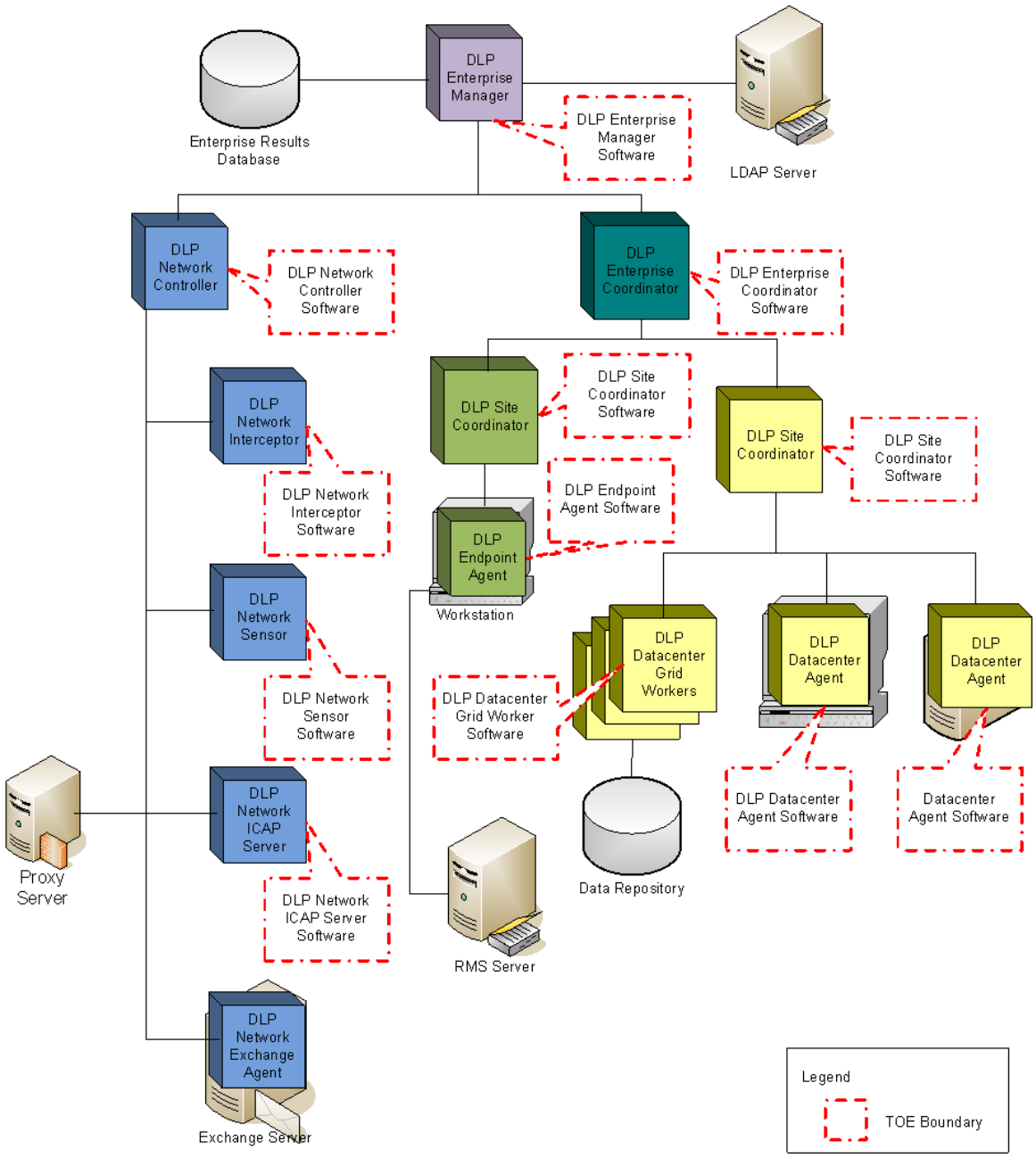

Figure 5 – Physical TOE Boundary

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
- 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.

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.

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.

Two FIPS 140-2 compliant cryptographic implementations are installed in the TOE Environment:

- RSA BSAFE Crypto-J 5.0 SSL-J 5.1.1.1 and Cert-J 5.2 (Certificate No. 1503)
  - installed on:
    - DLP Enterprise Manager,
    - DLP Datacenter Enterprise Coordinator,
    - DLP Datacenter Site Coordinator,
    - DLP Endpoint Enterprise Coordinator, and
    - DLP Endpoint Site Coordinator
- Red Hat Enterprise Linux 5 OpenSSL Cryptographic Module (Certificate No. 1320)
  - installed on:
    - DLP Network Controller,
    - DLP Network ICAP Server,
    - DLP Network Interceptor, and
    - DLP Network Sensor.

The TOE Environment implements the RSA BSAFE cryptographic modules for TLS support, which includes encryption/decryption (of Enterprise Manager HTTPS traffic between the TOE and the remote web browser used for management, as well as securing SMTP, SQL, and LDAP traffic); it also provides the cryptographic primitives for hashing, digital signature verification and generation, and message authentication.

The Red Hat OpenSSL module is used to secure management traffic, including SSH to the DLP Network appliance command line interfaces, as well as TLS protocol support for *stunnel*, which is used to secure management traffic between distributed DLP Network appliances. The OpenSSL module provides the cryptographic primitives necessary to perform cryptographic functions, including encryption/decryption, hashing, digital signature verification/generation, and message authentication.

In the evaluated configuration, only FIPS 140-2 validated algorithms are implemented. Each module performs self-tests of cryptographic algorithms during startup, and periodically during normal operation. The TOE is configured to operate in FIPS mode according to the guidance set forth in the *Deploying DLP in FIPS-Compliant Mode Technical Note* document.

For more information on the RSA BSAFE Crypto-J cryptographic implementation, please refer to the *RSA BSAFE Crypto-J v5.0 Product Documentation.* For more information on the Red Hat OpenSSL implementation, please refer to the *Red Hat Enterprise Linux – OpenSSL Module v1.0 FIPS 140-2 Security Policy*.

1.4.3 Product Physical/Logical Features and Functionality not included in the Evaluated Configuration of the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- Operating System
- Hardware

- Enterprise Results Database
- 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 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM[25] as of 2011/09/30 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.1)

[25] CEM – Common Evaluation Methodology

3 Security Problem

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[26] assets against which protection is required by the TOE or by the security environment. The 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 or 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 or 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.
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

[26] IT – Information Technology

Name	Description
	a security mechanism.
T.WEAKCIPHERS	An external attacker or malicious user may exploit weaknesses in cryptographic algorithms to expose TSF data.
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, along with all TSF-dependent services, including the LDAP server with which the TOE interfaces, reside in a physically controlled access facility that prevents unauthorized physical access.
A.NOEVIL	Authorized administrators who manage the TOE and systems in the IT Environment are non-hostile and are appropriately trained to use, configure, and maintain the TOE, and follow all guidance.
A.SECURECOMM	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:

Table 7 – IT Security Objectives

Name	Description
OE.TIMESTAMP	The TOE Environment must provide reliable timestamps for the TOE's use.

Name	Description
OE.LOG	The TOE Environment shall securely store logs of management operations performed on the TOE that are generated by the TOE.
OE.CRYPTO	The TOE Environment shall implement FIPS 140-2 approved algorithms and protocols for use in all cryptographic functions needed by the TOE.
OE.SECURECOMM	The TOE Environment shall provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote administrators.

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 or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 – Non-IT Security Objectives

Name	Description
NOE.NOEVIL	The TOE shall be operated by non-hostile administrators that are appropriately trained to use, configure, and maintain the TOE, and follow all guidance.
NOE.TRUSTED_ENV	The TOE shall reside in a physically secure location, safe from compromise by malicious insiders and outsiders.

5 Extended Components

This section defines the extended SFRs and extended 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 9 identifies all extended SFRs implemented by the TOE

Table 9 – 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_ARP: Incident automatic response was modeled after the CC family FAU_ARP: 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.

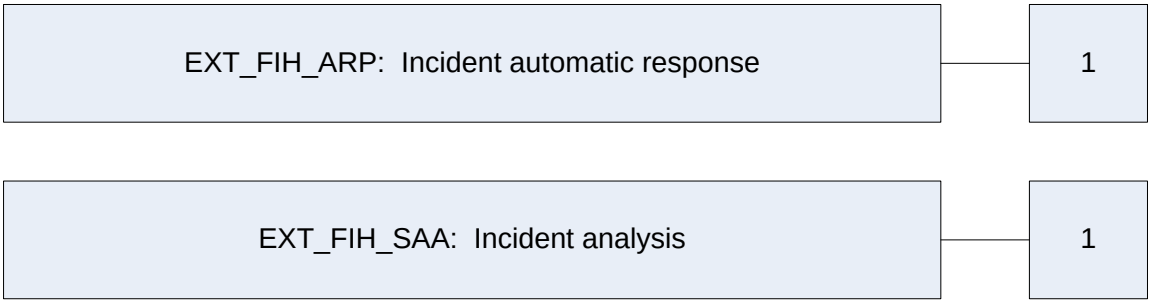

Figure 6 – EXT_FIH: Incident Handling Class Decomposition

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 7 – 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.

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 Incident alarms
Hierarchical to: No other components
EXT_FIH_ARP.1.1
The TSF shall take [assignment: *list of actions*] upon detection of a potential incident.
EXT_FIH_ARP.1.2
The TSF shall provide the incident data in a manner suitable for the user to interpret the information.
Dependencies: EXT_FIH_SAA.1 Incident analysis

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

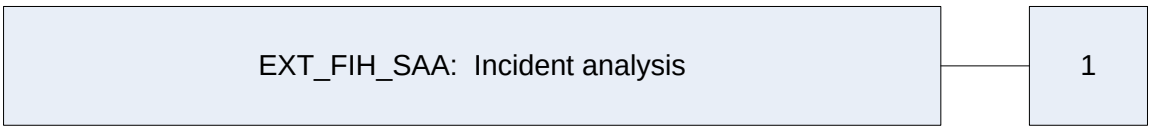

Figure 8 – Incident analysis family decomposition

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

- 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
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*].

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

5.2 Extended TOE Security Assurance Components

There are no extended SARs implemented by the TOE.

6 Security Requirements

This section defines the SFRs and 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 Part 2 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 text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF 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 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 – 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		✓		✓
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			✓	

Name	Description	S	A	R	I
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:*

- *Create, update, delete users;*
- *Create, update, delete groups;*
- *Create, update, delete roles;*
- *Create, update, delete credentials;*
- *Create, update, delete Network Controller configurations;*
- *Create, update, delete Enterprise Coordinator configurations;*
- *Create, update, delete Endpoint Agent groups;*
- *Create, update, delete content blades;*
- *Create, update, delete fingerprint crawlers;*
- *Successful login;*
- *Logout;*
- *Failed login;*
- *Create, update, delete, reorder, enable, disable policies;*
- *Delete, logically delete events;*
- *Delete, logically delete incidents;*
- *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 SFP*[27]] on
[
Subjects: users[28] *attempting to establish an interactive session with the TOE*
Objects: User Interface menu items, policies, incidents, events, reports, administrative management data, credentials
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*

].
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.

[27] SFP – Security Functional Policy
[28] "User" may refer to any individual attempting to access the TOE or the targeted TOE devices or data (administrators or end-users).

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. *Host/IP Address*
6. *Email address*
7. *URL*
8. *Protocol*
9. *DLP device detected by*

].

FDP_ACF.1.2(b)[29]

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)

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
[

[29] 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).

Subjects: End-Users
Objects: Data
Operations: Copy, paste, cut, move, 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"*
6. *Perform custom actions if defined by an administrator*

].

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

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"*
4. *Grant permissions on the data to an authorized end-user if the result of the evaluation is "grant permission"*
5. *Move the data to a specified location if the result of the evaluation is "move to secure"*
6. *Revoke all access permissions on the data and reclaim file ownership to an authorized administrator if the result of the evaluation is "quarantine"*

].

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. *Host/IP Address*
7. *Email address*
8. *URL*
9. *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"*[30]

].

FDP_IFF.1.3

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

FDP_IFF.1.4

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

FDP_IFF.1.5

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

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

[30] 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 11 below**] the functions [*See functions listed in Table 11 below*] to [*the roles listed in Table 11 below*].

Table 11 – Management of Security Functions Behavior

Security Function	Admin Role	Limited Admin Role
Management of Users, Groups, Credentials, and Roles	*Determine the behavior of* *Modify the behavior of*	*Determine the behavior of* *Modify the behavior of* ***(when given permission by the Admin Role)***
Management of DLP Network Configuration	*Determine the behavior of* *Modify the behavior of*	*Determine the behavior of* *Modify the behavior of* ***(when given permission by the Admin Role)***
Management of DLP Endpoint Configuration	*Determine the behavior of* *Modify the behavior of*	*Determine the behavior of* *Modify the behavior of* ***(when given permission by the Admin Role)***
Management of DLP Datacenter Configuration	*Determine the behavior of* *Modify the behavior of*	*Determine the behavior of* *Modify the behavior of* ***(when given permission by the Admin Role)***
Management of Content Blades	*Determine the behavior of* *Modify the behavior of*	*Determine the behavior of* *Modify the behavior of* ***(when given permission by the Admin Role)***
Management of Email Server Configuration	*Determine the behavior of* *Modify the behavior of*	*Determine the behavior of* *Modify the behavior of* ***(when given permission by the Admin Role)***
Management of Notification Templates	*Determine the behavior of* *Modify the behavior of*	*Determine the behavior of* *Modify the behavior of* ***(when given permission by the Admin Role)***
Management of Policies	*Determine the behavior of* *Modify the behavior of*	*Determine the behavior of* *Modify the behavior of* ***(when given permission by the Admin Role)***
Management of Reports	*Determine the behavior of* *Modify the behavior of*	*Determine the behavior of* *Modify the behavior of* ***(when given permission by the Admin Role)***
Management of Policy Templates	*Determine the behavior of* *Modify the behavior of*	*Determine the behavior of*
System Maintenance	*Determine the behavior of* *Modify the behavior of*	*Modify the behavior of*
Management of Incidents	*Determine the behavior of*	***(when given permission by the***

Security Function	Admin Role	Limited Admin Role
	Modify the behavior of	***Admin Role)***
Management of Events	Determine the behavior of Modify the behavior of	Determine the behavior of

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, Credentials*] to [*the Admin Role, authorized Limited Admin Roles*].
Dependencies: **[FDP_ACC.1(a) 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(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, host/IP address, email address, URL, 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(c)
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 Role*].
Dependencies: **[FDP_ACC.1(c) 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(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 or**

FDP_IFC.1 Subset information flow 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 12 below*] to provide [*[See default value listed in Table 12 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.

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

Table 12 – 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
Credentials	Restrictive	n/a	n/a	Restrictive
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
Host/IP address	n/a	Permissive	n/a	n/a
Email address	n/a	Permissive	n/a	n/a
URL	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

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 behavior, 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 of 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 the 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 13 – Assurance Requirements summarizes the requirements.

Table 13 – Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
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 Specification

This section presents information to detail how the TOE meets the functional 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 14 – 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
	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

TOE Security Function	SFR ID	Description
		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 and management of device credentials. 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 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, administrative management data, and device credentials 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[31], and which DLP device detected the violation. The resulting possible policy actions include: allow the transmission, record an event, block the transmission, encrypt the transmission[32], and quarantine the data transmitted. (Note that the DLP Network Access Control SFP is executed before the DLP Network Information Flow Control SFP.)

[31] URL – Uniform Resource Locator
[32] However, encryption is done by a third-party product, and is outside the scope of this CC evaluation.

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, record an event, apply RMS template, grant permission to a user, move to a secure location, or quarantine.

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), FDP_IFF.1, FDP_IFC.1.

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 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, credentials, 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 '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', 'move object to secure repository', 'quarantine the object', and 'delete the object'. Possible actions by DLP Endpoint are '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, policies, and assumptions to the security objectives are 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 15 – 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.
T.INFO_CAPTURE An external attacker or malicious insider may sniff the communication channel between	OE.SECURECOMM The TOE Environment shall provide a secure line of communication between separate	OE.SECURECOMM requires that information being transmitted between the TOE and TOE administrators never be modified

Threats	Objectives	Rationale
the TOE and a remote administrator in order to capture or modify information sent between the two.	parts of the TOE and between the TOE and trusted remote administrators.	or disclosed. This prevents external attackers and malicious insiders from capturing or modifying that data.
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.	OE.SECURECOMM The TOE Environment shall provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote administrators.	OE.SECURECOMM 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.
T.NO_AUDIT A threat agent may perform security-relevant operations on the TOE without being held accountable for it.	OE.TIMESTAMP The TOE Environment must provide reliable timestamps for the TOE's use.	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.
	OE.LOG The TOE Environment shall securely store logs of management operations performed on the TOE that are generated by the TOE.	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.
	O.LOG The TOE shall generate logs of management operations performed on the TOE.	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.
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.	O.INCIDENT The TOE shall analyze all events and generate incidents according to configured policies.	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.
	O.NOTIFICATION The TOE shall generate and deliver alerts according to configured policies upon generating an incident.	O.NOTIFICATION requires that the TOE generate and deliver alerts according to configured policies upon generating an incident. This alerts the administrator to policy violations involving the access or transmission of non-public or

Threats	Objectives	Rationale
		confidential information.
	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.	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.
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.	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 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.
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.	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 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.
	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 data of the TOE. This prevents unauthorized users from accessing the data collected and produced by the TOE.
T.WEAKCIPHERS An external attacker or malicious user may exploit weaknesses in cryptographic algorithms to expose TSF data.	OE.CRYPTO The TOE Environment shall implement FIPS 140-2 approved algorithms and protocols for use in all cryptographic functions needed by the TOE.	OE.CRYPTO mitigates this threat by requiring the TOE Environment to be operated in a secure mode of operation in accordance with the FIPS 140-2 standard, ensuring that only approved algorithms and protocols are implemented for use in cryptographic functionality.
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.	OE.SECURECOMM The TOE Environment shall provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote	OE.SECURECOMM requires that the information passing between separate parts of the TOE and between the TOE and trusted remote administrators be protected from unauthorized

Threats	Objectives	Rationale
	administrators.	disclosure and modification. This prevents unauthorized users from disclosing or modifying the data collected and produced by the TOE.
T.DATALOSS An unauthorized user may attempt to remove or destroy 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.
	OE.SECURECOMM The TOE Environment shall provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote administrators.	OE.SECURECOMM 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.

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 16 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.LOCATE The TOE, along with all TSF-dependent services, including the LDAP server with which the TOE interfaces, reside 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 and outsiders.	NOE.TRUSTED_ENV ensures that the TOE shall reside in a physically secure location, thereby preventing unauthorized physical access.
A.NOEVIL Authorized administrators who manage the TOE and systems in the IT Environment are non-hostile and are appropriately trained to use, configure, and maintain the TOE, and follow all guidance.	NOE.NOEVIL The TOE shall be operated by non-hostile administrators that are appropriately trained to use, configure, and maintain the TOE, and follow all guidance.	NOE.NOEVIL ensures that TOE administrators are non-hostile, appropriately trained, and follow all guidance.
A.SECURECOMM 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.	OE.CRYPTO The TOE Environment shall implement FIPS 140-2 approved algorithms and protocols for use in all cryptographic functions needed by the TOE.	OE.CRYPTO ensures that the TOE data in transit is protected using FIPS-validated cryptography.
	OE.SECURECOMM The TOE Environment shall provide a secure line of communication between separate parts of the TOE and between the TOE and trusted remote administrators.	OE.SECURECOMM ensures that the TOE Environment provides the necessary means for protecting sensitive data transmitted between distributed TOE components and end users.

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 17 – 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	The SFR meets the objective by

Objective	Requirements Addressing the Objective	Rationale
	Security roles	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 User identification before any action	The SFR meets the objective by requiring that TOE administrators be 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.
O.SEC_ACCESS The TOE shall ensure that only authorized administrators are granted access to the security functions, configurations, and associated data.	FDP_ACC.1(a) Subset access control	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.
	FDP_ACF.1(a) Security attribute based access control	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.
	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.1(b) Management of security attributes	The SFR meets the objective by requiring that only the Admin Role and authorized Limited

Objective	Requirements Addressing the Objective	Rationale
		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.
	FMT_MSA.1(c) 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 Endpoint policies, according to the DLP Endpoint 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	EXT_FIH_ARP.1	The SFR meets the objective by

Objective	Requirements Addressing the Objective	Rationale
The TOE shall generate and deliver alerts according to configured policies upon generating an incident.	Incident alarms	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 containing or accessing non-public or confidential information.	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 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

Objective	Requirements Addressing the Objective	Rationale
		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 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 satisfies all the requirement dependencies of the Common Criteria.
Table 18 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 18 – 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	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FDP_ACC.1(a)	✓	
FDP_ACC.1(b)	FDP_ACF.1(b)	✓	
FDP_ACF.1(b)	FDP_ACC.1(b)	✓	
	FMT_MSA.3	✓	
FDP_ACC.1(c)	FDP_ACF.1(c)	✓	
FDP_ACF.1(c)	FDP_ACC.1(c)	✓	
	FMT_MSA.3	✓	
FDP_ACC.1(d)	FDP_ACF.1(d)	✓	
FDP_ACF.1(d)	FDP_ACC.1(d)	✓	
	FMT_MSA.3	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FMT_MSA.3	✓	
	FDP_IFC.1	✓	
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_SMF.1	✓	
	FDP_ACC.1(a)	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(b)	FDP_ACC.1(b)	✓	
	FDP_IFC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(c)	FDP_ACC.1(c)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(d)	FDP_ACC.1(d)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FMT_MSA.3	FMT_MSA.1(a)	✓	
	FMT_MSA.1(b)	✓	
	FMT_MSA.1(c)	✓	
	FMT_MSA.1(d)	✓	
	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_ACF.1(c)	✓	
	FDP_ACF.1(b)	✓	
	FDP_ACC.1(d)	✓	
	FDP_ACC.1(c)	✓	
	FDP_ACC.1(b)	✓	
	FDP_ACF.1(d)	✓	

9 Acronyms and Terms

This section describes the acronyms and terms referenced within this document.

9.1 Acronyms

Table 19 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AOL	America Online
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
CPU	Central Processing Unit
DLP	Data Loss Prevention
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
HTTPS	Secure HTTP
ICAP	Internet Content Adaptation Protocol
ID	Identifier
IM	Instant Messaging
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MAPI	Messaging Application Protocol Interface
MB	Megabyte
MDAC	Microsoft Data Access Components
MSN	Microsoft Network
NAS	Network Attached Storage

Acronym	Definition
NPI	Non-Public Personal Information
OLEDB	Object Linking and Embedding, Database
OS	Operating System
OSP	Organizational Security Policy
PCI	Payment Card Industry
PII	Personally Identifiable Information
PP	Protection Profile
PRNG	Pseudo-Random Number Generator
PSS	Probabilistic Signature Scheme
RAM	Random Access Memory
RMS	Rights Management Services
RPC	Remote Procedure Call
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SP	Service Pack
SQL	Structured Query Language
ST	Security Target
TB	Terabyte
TOE	Target of Evaluation
TSF	TOE Security Functionality
URL	Uniform Resource Locator
XML	eXtensible Markup Language

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.

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com