Security Target

McAfee Data Loss Prevention 11.1 with ePolicy Orchestrator 5.10

Version 1.0

May 8, 2019

Prepared For:

McAfee, LLC.
2821 Mission College Blvd.
Santa Clara, CA 95054

Prepared By:

Primasec Ltd
Le Domaine de Loustalviel
11420 Pech Luna, France

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), McAfee Data Loss Prevention 11.1 with ePolicy Orchestrator 5.10. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

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

1.1 ST Reference

ST Title	Security Target: McAfee Data Loss Prevention 11.1 with ePolicy Orchestrator 5.10
ST Revision	1.0
ST Publication Date	May 8, 2019
Author	Primasec Ltd

1.2 TOE Reference

McAfee Data Loss Prevention 11.1 with ePolicy Orchestrator 5.10

1.3 TOE Type

The TOE is software only, and relates to Data Loss Prevention.

1.4 Document Organization

2 This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE.
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable.
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats.
5	Extended Components Definition	Describes extended components of the evaluation.

SECTION	TITLE	DESCRIPTION
6	Security Requirements	Contains the functional and assurance requirements for this TOE.
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.5 Document Conventions

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

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

4 Outside the SFRs, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.6 Document Terminology

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

TERM	
CC	Common Criteria version 3.1 (ISO/IEC 15408)
DBMS	DataBase Management System
DLP	Data Loss Prevention
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
FIPS	Federal Information Processing Standard

TERM	
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
ICAP	Internet Content Adaptation Protocol
I&A	Identification & Authentication
IMAP	Internet Message Access Protocol
IRC	Internet Relay Chat
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MTA	Message Transfer Agent
OS	Operating System
OSP	Organizational Security Policy
POP3	Post Office Protocol 3
PP	Protection Profile
RAM	Random Access Memory
SOCKS	Socket Secure
SFP	Security Function Policy
SFR	Security Functional Requirement
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SP	Service Pack
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy

Table 2 – Terms and Acronyms Used in Security Target

1.7 TOE Overview

6 The TOE is McAfee Data Loss Prevention 11.1 with ePolicy Orchestrator 5.10.

7 Data loss can occur when confidential or private information leaves an enterprise as a result of unauthorized communication through channels such as applications, physical devices, or network protocols. McAfee Data Loss Prevention (DLP) is a suite of products that identify and

protect data within the network. It provides an understanding of the types of data on a network, how the data is accessed and transmitted, and if the data contains sensitive or confidential information.

8 DLP is used to build and implement effective protection policies, while reducing the need for extensive trial and error.

9 DLP includes extensions for ePolicy Orchestrator (ePO) that add new management features and reports to its capabilities.

10 McAfee Agent is also employed to provide communications between ePO, DLP management components and DLP clients.

1.8 TOE Description

1.8.1 Physical Boundary

11 The TOE is a software TOE and includes:

- McAfee Data Loss Prevention **Endpoint** – Inspects and controls content and user actions on endpoints
- McAfee **Device Control** – Controls the use of removable media on endpoints
- McAfee Data Loss Prevention **Discover** – Scans file, Box[1], registered document and repositories to identify and protect sensitive data
- McAfee Data Loss Prevention **Prevent** – Works with a web proxy or MTA server to protect web and email traffic
- McAfee Data Loss Prevention **Monitor** – Passively scans unencrypted network traffic for potential data loss incidents
- McAfee DLP Capture – a function within DLP Monitor and DLP Prevent that allows capture of email, web and network traffic for later analysis
- McAfee **ePO** – Provides facilities to manage and monitor DLP
- Four McAfee ePO managed extensions related to DLP
    - DLP management
    - DLP appliance management
    - AME
    - Common UI
- **McAfee Agent** on each server and managed system
- McAfee Agent ePO policy and reporting extension

[1] Box is an online file sharing and content management service.

12 Note specifically that the hardware (including the DLP Capture Storage Array), operating systems and third party support software (e.g. DBMS) on each of the systems are excluded from the TOE boundary.

13 All TOE software and documentation is available for download from the McAfee website. Download of software requires a current Grant Number.

14 In order to comply with the evaluated configuration, the following hardware and software components must be used:

TOE COMPONENT	Product	File description	File name
TOE Software	All products	McAfee Data Loss Prevention management extension 11.1.100.16	DLP_Mgmt_11.1_Package.zip
	DLPe and Device Control 11.1	Client software Windows 11.1.100.232 Mac 11.1.100.8	MS Windows: HDLP_Agent_11_1_100_23.zip MacOS: DlpAgentInstaller.zip
	DLP Discover 11.1	Discover Server package 11.1.100.12 DLP Server	Discover_11_1_100_12.zip DLPServer_11_1_100_12.zip
	DLP Monitor 11.1 DLP Prevent 11.1	McAfee DLP Appliance Management ePO extension 11.1.0.122	dlp-appliance-management-app-11.1.0.122-extensions.zip
		DLP AME extension 11.1.100.163	11.1.000extensionbundle.zip
		Common UI extension 1.3.0.258	

TOE COMPONENT	Product	File description	File name
		Installation image 3525.100	Virtual appliance: McAfee-PS-11.1.100-3525.100.ova McAfee-MS-11.1.100-3525.100.ova Hardware appliance: McAfee-PS-11.1.100-3525.100.iso McAfee-MS-11.1.100-3525.100.iso
	ePolicy Orchestrator 5.10.0	ePO 5.10.0.Refresh 3, Update 2 McAfee Agent 5.5.1.388 5.5.1.342 MA ePO policy and reporting extension 5.5.1.124 McAfee Agent Help 5.5.1.010	EPO510_2428_10_R3.zip EPO5.10.0_Update2.zip MA551WIN.zip MA551MAC.zip EPOAGENTMETA.zip help_ma_551.zip
IT Environment	Specified in the following: • Table 4 – ePO Server System Requirements • Table 6 – Supported client platforms • Table 7 –Client platform hardware requirements		

Table 3 – Evaluated Configuration for the TOE

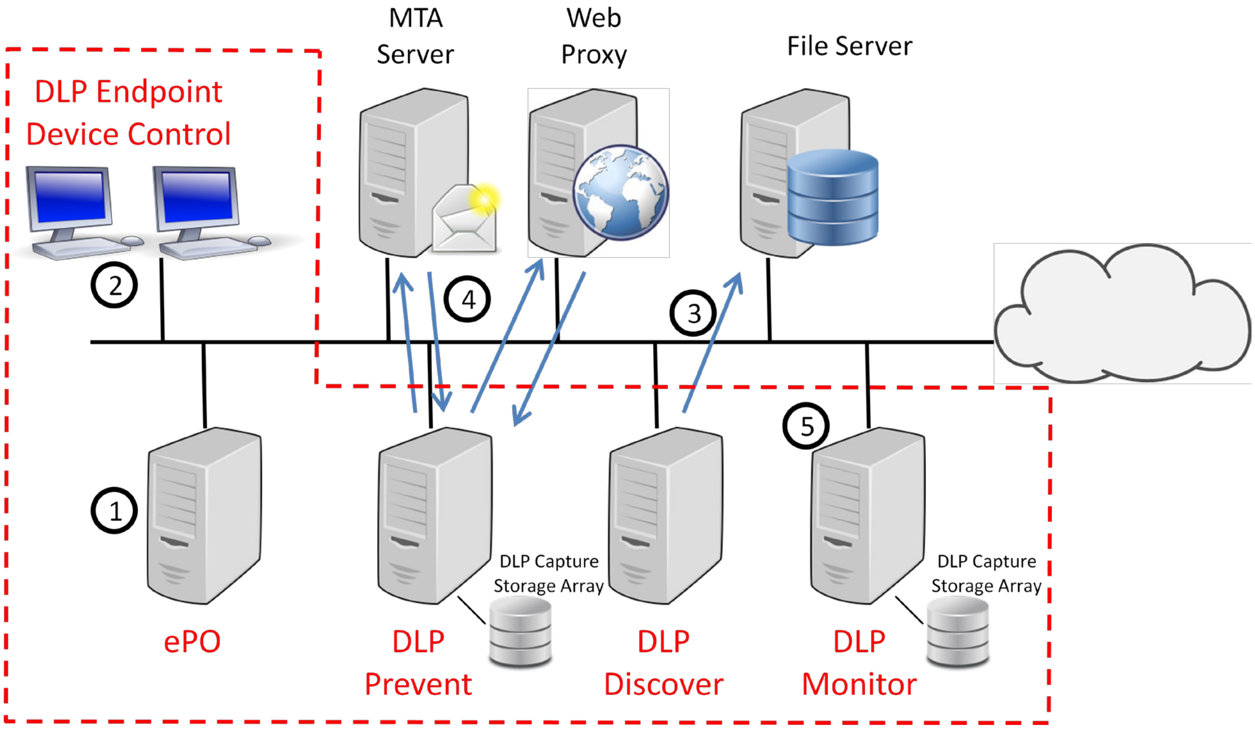
15 The evaluated configuration consists of a single instance of the management system (with ePO, the DLP extensions and the McAfee Agent extension), Discover, Prevent, Monitor, and one or more instances of managed systems (with McAfee Agent, Endpoint client and Device Control).

16 ePO supports authentication of user account credentials either by Windows or ePO itself (ePO by default). Both are supported in the evaluated configuration. User accounts (other than the password) are still required to be defined in ePO so that attributes and permissions can be associated with the account.

17 The ePO, server and Prevent must be installed in FIPS mode (as detailed in *McAfee Data Loss Prevention 11.1 with ePolicy Orchestrator 5.10 Common Criteria Evaluated Configuration Guide*

and *McAfee ePolicy Orchestrator 5.10.0 Product Guide)* to ensure that cryptographic services used by the TOE are FIPS validated.

18 The following figure presents an example of an operational configuration. The area enclosed by the red dotted line in the figure represents the TOE boundary.


MTA Server
Web Proxy
File Server
DLP Endpoint Device Control
2
4
3
5
1
ePO
DLP Prevent
DLP Capture Storage Array
DLP Discover
DLP Monitor
DLP Capture Storage Array

Reference	Description	Data vector
1	ePO handles policy configuration and incident management for all McAfee DLP products.	Not applicable
2	DLP Endpoint and Device Control monitor and restrict users' data use. McAfee DLP Endpoint also scans endpoint file systems and email.	Data in use Data at rest
3	DLP Discover scans files from local or cloud repositories to find sensitive information.	Data at rest

Reference	Description	Data vector
4	DLP Prevent receives email from MTA servers. It analyzes the messages, adds appropriate headers based on configured policy, and sends the emails to a single MTA server, also known as the *Smart Host*. DLP Prevent receives web traffic from web proxy servers encapsulated in an ICAP request. It analyzes the web traffic, determines if the traffic should be allowed or blocked, and sends an ICAP response back to the connecting web proxy server. The DLP Capture feature can be enabled to store content for later analysis on an external DLP Capture Storage Array.	Data in motion Data at rest
5	DLP Monitor connects to either a Switched Port Analyzer (SPAN) port or a network tap to passively monitor live traffic. DLP Monitor captures, analyzes, and stores live network traffic, but does not take any blocking or preventive actions. Data collected by DLP Monitor is used to determine who sends what kind of data through the network, and where the data is sent. The DLP Capture feature can be enabled to store content for later analysis on an external DLP Capture Storage Array.	Data in motion Data at rest

Figure 1 - TOE components

19 Note that the data stored within the DBMS for ePO are part of the TOE, but the third party DBMS software is not.

20 The following specific ePO/MA configuration options apply to the evaluated configuration:

1. Incoming connections to McAfee Agents are only accepted from the configured address of the ePO server.
2. The repository is where ePO stores software and signatures for distribution to network platforms. The only software and update repository supported is the ePO server (see section 1.7.10.3).
3. The DLP Capture feature is enabled within Prevent and Monitor.

21 The diagram below shows the scope of the TOE.

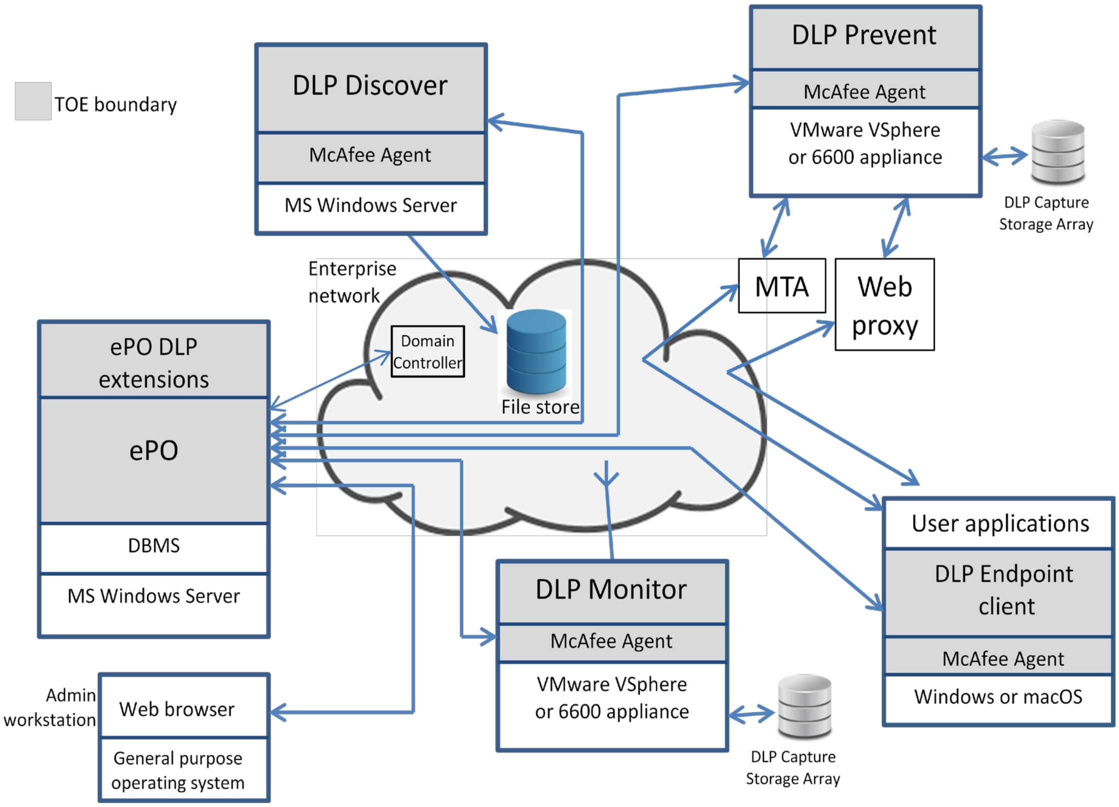


Figure 2 – Scope of the TOE

1.8.2 Hardware and Software Supplied by the IT Environment

22 The TOE consists of a set of software applications. The hardware, operating systems and all third party support software (e.g., DBMS, Active Directory server) on the systems on which the TOE executes are excluded from the TOE boundary.

23 The platform on which the ePO and DLP extensions are installed must be dedicated to functioning as the management system. The ePO server operates as a distribution system and management system for a client-server architecture offering components for the server part of the architecture (not the clients).

24 The TOE requires the following hardware and software configuration.

1.8.2.1 ePO

25 The ePO server system requirements are:

Component	Minimum Requirements
Processor	64-bit Intel Pentium D or higher 2.66 GHz or higher
Memory	8 GB available RAM recommended minimum
Free Disk Space	20 GB — Recommended minimum
Monitor	1366x768, 256-color, VGA monitor or higher

Component	Minimum Requirements
Operating System	Windows Server 2016
DBMS	Microsoft SQL Server 2012 (Required – installed automatically)
Network Card	Ethernet, 100Mb or higher
Disk Partition Formats	NTFS
Domain Controllers	The system must have a trust relationship with the Primary Domain Controller (PDC) on the network
Miscellaneous	Microsoft updates Microsoft Visual C++ 2010 and 2015 Redistributable Packages (Required – installed automatically) MSXML 3.0 and 6.0 (Required – installed automatically)

Table 4 – ePO Server System Requirements

26 The ePO management system is accessed from remote systems via a browser. The browser used to access the ePO management system in this evaluation was:

- Microsoft Internet Explorer 11.0.

27 The TOE relies on ePO or Windows to authenticate user credentials during the logon process. User accounts must be defined within ePO in order to associate permissions with the users.

1.8.2.2 DLP Discover

28 DLP Discover installed on Microsoft Windows Server 2016 with compatible hardware platform.

Component	Minimum Requirements
CPU	Intel Core 2 64-bit, minimum 2 CPUs
RAM	4 GB minimum
Free disk space	100 GB minimum

Table 5 –DLP Discover hardware requirements

1.8.2.3 DLP Prevent

29 DLP Prevent installed on VMware vSphere using VMware vCenter server 6.7, VMware ESXi 6.7, and compatible hardware platform, or a Model 6600 appliance hardware platform with DLP Capture Storage Array[2].

[2] The DLP Capture feature can be used on a virtual appliance when deployed using a capture enabled virtual machine.

1.8.2.4 DLP Monitor

30 DLP Monitor installed on VMware vSphere using VMware vCenter server 6.7, VMware ESXi 6.7, and compatible hardware platform, or a Model 6600 appliance hardware platform with DLP Capture Storage Array.

1.8.2.5 DLPe client platforms

31 McAfee Agent, DLP Endpoint and Device Control execute on one or more systems that are to be monitored. The client platforms within the scope of the evaluation are:

SUPPORTED OS FOR CLIENTS	PLATFORM
Windows 10 version 1809	X64 platforms
Windows 2016 Server	X64 platforms
Apple macOS 10.14	X64 platforms

Table 6 – Supported client platforms

32 The minimum hardware requirements for the client platforms are specified in the following table:

COMPONENT	MINIMUM HARDWARE REQUIREMENTS
CPU	Intel Pentium IV 1GHz or higher
Memory	1GB minimum (2GB recommended)
Free Disk Space	300 MB minimum (500MB recommended)
Network Card	Minimum 100 megabit LAN

Table 7 –Client platform hardware requirements

1.8.3 TOE Guidance

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

- *McAfee Data Loss Prevention 11.1.x Product Guide*
- *McAfee Data Loss Prevention Monitor 11.1.x Installation Guide*
- *McAfee Data Loss Prevention Monitor 11.1.x Hardware Guide*
- *McAfee Data Loss Prevention Prevent 11.1.x Installation Guide*
- *McAfee Data Loss Prevention Prevent 11.1.x Hardware Guide*
- *McAfee Data Loss Prevention Discover 11.1.x Installation Guide*
- *McAfee Data Loss Prevention Endpoint 11.1.x Installation Guide*
- *McAfee Data Loss Prevention 11.1.x Interface Reference Guide*
- *McAfee ePolicy Orchestrator 5.10.0 Product Guide*
- *McAfee ePolicy Orchestrator 5.10.0 Installation Guide*
- *McAfee Agent 5.5.1 Product Guide*

- *McAfee Data Loss Prevention 11.1 with ePolicy Orchestrator 5.10 Common Criteria Evaluated Configuration Guide*

34 All documentation is supplied for download in .pdf format, and is also available online at https://docs.mcafee.com.

1.8.4 Logical Boundary

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

TSF	DESCRIPTION
Security Audit	The TOE's Audit Security Function provides auditing of management actions performed by administrators. Authorized users may review the audit records via ePO.
User Data Protection	The TOE enforces DLP policies on managed systems and audits end-user action against those policies. DLP events are stored in the database (the DBMS is in the IT Environment), and reports based upon completed policy audits may be retrieved via the GUI interface. Data from Prevent and Monitor can also be stored for analysis using the DLP Capture function.
Identification & Authentication	On the ePO management system, the TOE requires administrative users to identify and authenticate themselves before accessing the TOE software. User accounts must be defined within ePO, but authentication of the user credentials is performed either by ePO or by Windows. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that define the functionality the user is allowed to perform.
Security Management	The TOE's Management Security Function provides support functionality that enables users to configure and manage TOE components. Management of the TOE may be performed via the GUI. Management privileges are defined per-user.
Cryptographic Support	The TOE makes use of the cryptographic services provided by RSA BSAFE Crypto-C Micro Edition v4.0.1 (for McAfee Agent), and OpenSSL v1.0.2p library with FIPS module v2.0.16 (for ePO). These services include encryption/decryption, key generation and key destruction.
Protection of the TSF	The TOE provides TLS v1.2 protection of all communication between the McAfee Agent and ePO. The TOE may be configured to import information about systems to be managed from Active Directory (LDAP servers) or domain controllers. This functionality ensures that all the defined systems in the enterprise network are known to the TOE and may be configured to be managed.

Table 8 –Logical boundary descriptions

36 Seamless integration with McAfee ePolicy Orchestrator (ePO) eases deployment of components that reside on the clients, and allows policy management, and reporting. ePO provides the user interface for the TOE via a GUI accessed from remote systems using web browsers. Custom reports can be fully automated, scheduled, or exported. ePO requires users to identify and authenticate themselves before access is granted to any data or management functions. Audit log records are generated to record configuration changes made by ePO users. The audit log records may be reviewed via the GUI. Users can review the results of policy application via ePO. Access to this information is controlled by per-user permissions.

37 The following sections provide a summary of the specific TOE sub-components.

1.8.5 DLP Endpoint

38 DLP Endpoint inspects users' actions on sensitive content on client computers.

39 Device Control prevents unauthorized use of removable media devices. DLP Endpoint includes all Device Control functionality, and, in addition, protects against data loss through a broad set of potential data-loss channels.

40 The following paragraphs outline the key features of DLP Endpoint.

41 Device Control:

- Controls what data can be copied to removable devices, or controls the devices themselves. It can block devices completely or make them read-only;
- Blocks executables on removable media from running. Exceptions can be made for required executables such as virus protection;
- Provides protection for USB drives, smartphones, Bluetooth devices, and other removable media.

42 DLP Endpoint protects against data loss from:

- Clipboard software
- Cloud applications
- Email (including email sent to mobile devices)
- Network shares
- Printers
- Screen captures
- Specified applications and browsers
- ▪ Web posts

43 The DLP classification engine applies definitions and classification criteria that define the content to be protected, and where and when the protection is applied. Protection rules apply the classification criteria and other definitions to protect the sensitive content.

44 McAfee DLP Endpoint safeguards sensitive enterprise information:

- Applies policies that consist of definitions, classifications, rule sets, endpoint client configurations, and endpoint discovery schedules;
- Monitors the policies and blocks actions on sensitive content, as needed;

- Encrypts sensitive content before allowing the action;
- Creates reports for review and control of the process, and can store sensitive content as evidence.

1.8.6 DLP Discover

45 McAfee DLP Discover runs on Microsoft Windows servers and scans network file systems to identify and protect sensitive files and data.

46 DLP Discover can be used for:

- Detecting and classifying sensitive content;
- Moving or copying sensitive content;
- Integrating with Microsoft Rights Management Service to apply protection to files;
- Automating IT tasks such as finding blank files, determining permissions, and listing files that changed within a specified time range.

47 ePO is used to perform configuration and analytics tasks such as:

- Displaying available Discover servers;
- Configuring and scheduling scans;
- Configuring policy items such as definitions, classifications, and rules;
- Reviewing data analytics and inventory results;
- Reviewing incidents generated from remediation scans.

48 DLP Discover supports local and cloud repositories: Box, Common Interface File System and Sharepoint (2010, 2013 and 2016).

49 DLP Discover supports four scan types: inventory, classification, remediation and registration.

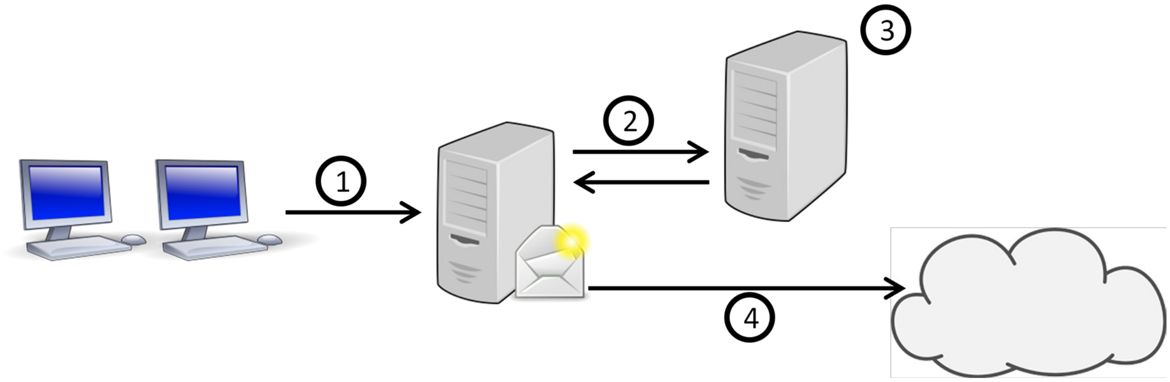
- **Inventory scans** give a high-level view of what types of files exist in the repository. This scan collects only metadata, and the files are not fetched. DLP Discover sorts scanned metadata into different content types and analyzes attributes such as file size, location, and file extension.
- **Classification scans** help to understand the data that exists in the targeted repository. By matching scanned content to classifications such as text patterns or dictionaries, data patterns can be analyzed to create optimized remediation scans.
- **Remediation scans** find data that is in violation of a policy. It is possible to monitor, apply a Rights Management policy, copy, or move files to an export location. All actions can produce incidents that are reported to the Incident Manager in ePO.
- **Registration scans** extract content from files based on selected fingerprint criteria, and save the data to a signature database. The registered documents can define classification and remediation scans, or policies for DLP Prevent and DLP Monitor.

1.8.7 DLP Prevent

50 DLP Prevent integrates with an MTA server or web proxy to monitor email and web traffic and prevent potential data loss incidents.

1.8.7.1 Protecting email traffic

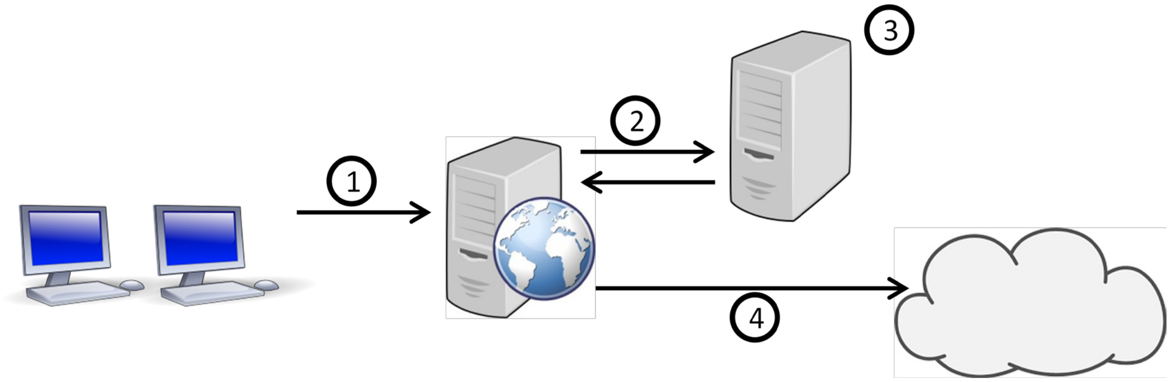
51 DLP Prevent integrates with any MTA[3] that supports header inspection. IT interacts with email traffic, generates incidents, and records the incidents in ePO for subsequent case review.



Step	Description
1	Users – Incoming /outgoing messages to/from the MTA server
2	MTA server forwards the email messages to DLP Prevent
3	DLP Prevent receives SMTP connections from the MTA server and: • Decomposes the email message into its component parts • Analyzes the email message to detect policy violations • Adds an X-RCIS-Action header • Sends the message back to the original MTA (or a second MTA).
4	MTA server – acts on the email message based on the information it gets from the X-RCIS-Action header

Figure 3 – DLP Prevent mail flow

1.8.7.2 Protecting web traffic



[3] The configuration can include 2 MTAs: a source and destination. The evaluated configuration uses a single MTA.

Step	Description
1	Users send web traffic to the web proxy server
2	Web proxy server forwards the email messages to DLP Prevent
3	DLP Prevent inspects the web traffic, and returns a response to the web proxy server to allow traffic through to the destination server or deny access.
4	Web proxy server sends the inspected web traffic to the appropriate destinations.

Figure 4 – DLP Prevent web traffic flow

1.8.8 DLP Monitor

52 DLP Monitor performs passive deep packet inspection on Ethernet frames to reassemble application-level data. Application of a rule engine allows evidence to be stored, and end users to be notified. Stored information can be used for analysis and reporting.

53 It can decapsulate the following protocols: SMTP, IMAP, POP3, HTTP, FTP, LDAP, Telnet, IRC and SMB. The application data may be embedded in SOCKS traffic.

54 Data that is not a recognized protocol or that is known to be encrypted is ignored.

55 DLP Monitor can apply one of the following DLP protection rules to network traffic:

Email Protection – By default, DLP Monitor inspects SMPT traffic using email protection rules that incorporate protocol specific information such as sender and recipient email addresses;

Web Protection – By default, DLP Monitor inspects HTTP and FTP traffic using web protection rules that incorporate protocol specific information such as the URL;

Network Communication Protection – DLP Monitor can inspect all supported traffic using network communication protection rules that do not incorporate any protocol specific information.

56 The placement of DLP Monitor determines what data is analyzed. DLP Monitor can connect to any switch in a network, using, for example, a SPAN port or network tap. Typically it connects to the LAN switch before the WAN router. This placement ensures that it analyzes all connections entering or leaving the network.

1.8.9 DLP Capture

57 DLP Prevent and DLP Monitor appliances that have the DLP Capture feature enabled:

- Capture content for later analysis for keywords, user activity, or file name to identify potential data loss incidents missed by active email protection, web protection, or network communication protection rules.
- Allow customization of email, web or network communication protection rules for testing using the DLP Capture database.

1.8.10 McAfee Agent

58 McAfee Agent is a vehicle of information and enforcement between the ePO server and each managed system. McAfee Agent deploys McAfee products, retrieves updates, runs client tasks, distributes policies, and forwards events from each managed system (endpoint) back to ePO. McAfee Agent uses a secure channel (using TLS v1.2) to transfer data from/to the ePO server.

1.8.11 ePolicy Orchestrator

59 ePolicy Orchestrator (ePO) provides a platform for centralized policy management and enforcement of DLP policies on managed systems. It uses the System Tree to organize managed systems into units for monitoring, assigning policies, scheduling tasks, and taking actions. The System Tree is a hierarchical structure that allows administrators to combine managed systems into groups. Policies can then be applied to groups of managed systems, rather than individually.

60 Management permissions are defined per-user. The TOE maintains two types of roles:

- Where users are assigned to the “administrator” permission set, which is a superset of all other permission sets. This includes the default “admin” user account created when ePO is installed. Users assigned to this permission set are known as “Administrator”.
- Where Users are assigned to selected permission sets. Users assigned to permission sets (excluding the administrator permission) set are known as “Users with Selected Permissions”.

61 This ST uses the term “administrator” to refer generally to an ePO user, unless, for example when defining SFRs, a more precise term is required. When using the term in this sense the possession of necessary ePO permissions is assumed.

62 ePO allows administrators to manage the targeted systems from a single location through the combination of product policies and client tasks. Policies ensure that the DLP features are configured correctly.

63 Within the TOE configuration the ePO software is comprised of the following components.

1.8.11.1 ePO Server

64 The ePO server deploys DLP software to DLP servers and managed systems (via the McAfee agent) and controls DLPe agent, DLP Monitor, DLP Prevent and DLP Discover updates. It creates DLP policies and distributes them to the managed systems, and processes the events for all the DLP servers and managed systems. It includes the following subcomponents:

- **Policy Catalog**
  The ePO policy catalog stores the DLP policies and allows an ePO user to edit, delete, duplicate or create new DLP policies. The types of DLP policies are:
  - *DLP Policy* – contains rule sets and endpoint and DLP Discover discovery scans;
  - *Client Configuration* – contains settings to control the DLP software on servers and managed systems;
  The policy is the entity that is distributed to managed systems to enforce the DLP rules.
- **DLP Classifications**
  Defines the content classification options (e.g. PCI, PHI, HIPAA) and the classification criteria

and the definitions used to configure them. It also sets up registered document repositories and user authorization for manual tagging.

- **DLP Policy Manager**
  Defines the data protection rules, device control rules, endpoint discovery rules, and the definitions used to configure them. Multiple rules are grouped into a rule set, and multiple rule sets can be assigned to a DLP Policy.
- **DLP Incident Manager**
  Events resulting from policy violations, sent to the DLP Event Parser, are displayed in the DLP Incident Manager, a GUI accessed from the ePolicy Orchestrator Reporting console. All events can be filtered and sorted based on criteria such as protection rule types, severity, date, time, user, computer name, or policy version. Events can be labeled by the administrator for tracking purposes.
- **DLP Operational Events**
  Displays administrative events, such as deployments, policy updates and operational errors (such as DLPe agent could not copy evidence file to evidence share – no sufficient space)
- **Application server**
  This includes the Automatic Response[4] functionality, Registered Servers (see below), and the user interface.
- **Agent handler**
  Distributes network traffic generated by agent-to-server communications responsible for communicating policies, tasks, and properties.
- **Event parser**
  This parses events received from deployed DLP software and inserts them into the ePO DBMS.
- **Registered servers** - used to register different server types in ePO (e.g. LDAP, SNMP, Ticketing servers, MS-RMS server).

1.8.11.2 Database

65 The database is the central storage component for all data created and used by ePO. The database can be housed on the ePO server, or on a separate server, depending on the specific needs of the organization. However, the evaluated configuration only supports the database housed on the same server as ePO.

1.8.11.3 Master Repository

66 The Master Repository is the central location for all McAfee software and signatures, and it resides on the ePO server. The Master Repository retrieves user-specified software updates and signatures from McAfee or from user-defined source sites.

[4] Automatic Responses functionality allows administrators to create rules for responding to events that are specific to the managed business environment, such as sending email notifications or SNMP traps, or creating issues for use with integrated third-party ticketing systems.

1.8.12 Features not part of the evaluated TOE

67 In addition to the platforms given in Table 4, ePO can also be installed on the following operating system platforms that have not been tested during the evaluation:

- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 SP1
- Windows 2012 R2

68 Additional supported browsers for access to the ePO management interface that have not been tested during the evaluation are:

- Internet Explorer 8.0 and later
- Firefox 10.0 and later
- Chrome 17 and later
- Safari 6.0 and later

69 In addition to the platforms given in Table 6, DLPe can also be installed on the following operating system platforms that have not been tested during the evaluation:

- Windows 7 SP1 all editions (32-bit and 64-bit)
- Windows 8 and 8.1 all editions (32-bit and 64-bit)
- Windows 10 (32-bit)
- Windows Server 2008 SP2 (32-bit and 64-bit)
- Windows Server 2008 R2
- Windows Server 2012

70 In addition to the platforms given in section 1.7.2.2, DLP Discover can also be installed on the following operating system platform that has not been tested during the evaluation:

- Windows Server 2008 R2 SP1 or later
- Windows Server 2012
- Windows Server 2012 R2

71 In addition to the platforms given in sections 1.7.2.3 and 1.7.2.4, DLP Prevent and DLP Monitor can also be installed on the following platforms that have not been tested during the evaluation:

- Model 5500 appliance
- VMware vSphere using VMware vCenter server 6.7, and VMware ESXi versions 6.0 and 6.5
- VMware Hyper-V using Windows Server 2012 or 2016

1.9 DLP workflows

72 The following workflow provides general guidance on working with DLP products:

- **Understand the data** — Detect and identify what data is on the network.

1. Use McAfee DLP to passively monitor the data and user actions on the network. Predefined rules can be used, or a basic policy can be created.
2. Review incidents and analyze scan results to see potential policy violations. Use this information to begin creating an effective policy.

- **Configure policy** — Use rules to react to violations to protect data.

1. Classify and define sensitive data by configuring classifications and definitions.
2. Track sensitive data and files with content fingerprinting and registered documents.
3. Protect data with scans and rules. Configure the action to take when sensitive data is discovered, accessed, or transmitted.

- **Monitor results** — Monitor incidents and create reports.

1. Review incidents for false positives and genuine policy violations.
2. Group related incidents into cases, which can be escalated to other departments, such as legal or Human Resources.

- **Refine policy** — Fine-tune the policy as needed. Continue monitoring incidents.

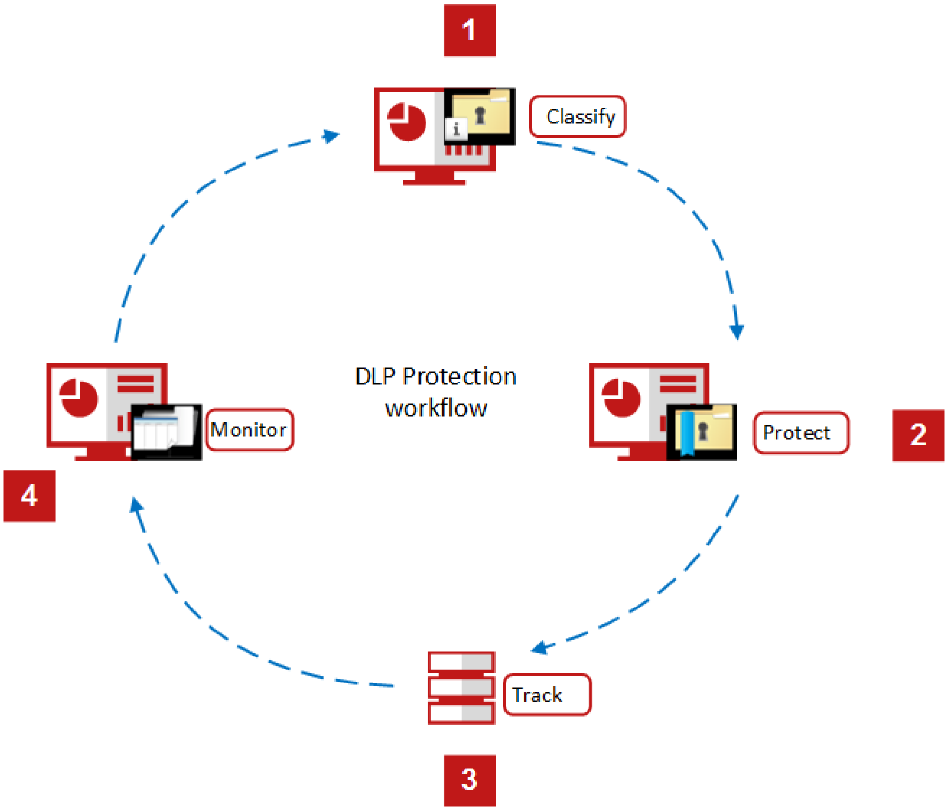


Figure 5 – DLP protection process

1 Create classifications with the McAfee DLP extension **Classification** console.

2 Protect sensitive data by applying rules with the **DLP Policy Manager**.

3 Track how and where the files containing sensitive content are used with tags or registered documents.

4 Monitor results with **DLP Incident Manager**, **DLP Case Management**, and **DLP Operations**. Create reports with McAfee ePO dashboards and queries.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

73 The TOE is Common Criteria Version 3.1 Revision 5 (April 2017) Part 2 extended and Part 3 conformant at Evaluation Assurance Level 2 and augmented by ALC_FLR.2 – Flaw Reporting Procedures.

2.2 Protection Profile Conformance Claim

74 The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

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

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

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

3.1 Threats

77 The following are threats identified for the TOE and the IT systems that the TOE monitors. The TOE is responsible for addressing threats to the environment in which it resides, and there are also threats related to the TOE itself. The assumed level of expertise of the attacker for all the threats is unsophisticated.

78 The TOE addresses the following threats:

THREAT	DESCRIPTION
T.DATA_LOSS	Users may store or transmit sensitive data in a manner that is inconsistent with a defined organizational policy, leading to loss of confidentiality. Such data may include, for example, intellectual property, trade secrets, or financial information.

Table 9 – Threats in the TOE environment

THREAT	DESCRIPTION
T.CONF_COMP	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.INT_COMP	An unauthorized user may attempt to modify the data collected and produced by the TOE by bypassing a security mechanism.
T.CH_CONFIG	An unauthorized user may inappropriately modify the configuration of the TOE causing potential data loss to go undetected.
T.NO_HALT	An unauthorized user may attempt to compromise the continuity of the system’s collection and analysis functions by halting execution of the TOE.
T.CONFLICT	Policy rules may include contradictions that may both explicitly permit and deny certain actions leading to unpredictable results in policy enforcement.

THREAT	DESCRIPTION
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.ACCOUNT	Users may not be accountable for their actions when administering the TOE; and consequently errors and omissions may go undetected, leading to failures in policy enforcement.

Table 10 - Threats against the TOE

3.2 Organizational Security Policies

79 This section describes the Organizational Security Policies that the TOE is designed for use with.

POLICY	DESCRIPTION
P.CRYPTO	When providing cryptographic services to protect the integrity of data in transit the TOE must use cryptographic modules that have been validated to FIPS 140.

Table 11 – Organizational Security Policies

3.3 Assumptions

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

ASSUMPTION	DESCRIPTION
A.ACCESS	The TOE has appropriate access to the systems it is intended to manage.
A.MTA	The MTA is configured to route email traffic via DLP Prevent, and to act on the header strings that DLP Prevent adds to the email messages.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to authorized users.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTECT	The hardware on which the TOE and the IT environment software are installed will be protected from unauthorized physical modification[5].

[5] Whilst this would be considered normal practice for server components of the TOE in an enterprise environment, it should be acknowledged that managed systems will often not have the same level of protection.

ASSUMPTION	DESCRIPTION
A.PLATFORM	The hardware, operating system, and other software on which the TOE depends, operate correctly.

Table 12 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

81 The IT security objectives for the TOE are listed below:

OBJECTIVE	DESCRIPTION
O.DLP	The TOE must be able to take defined actions upon detection of the access, transmission, printing, or copying of sensitive files or data from managed systems.
O.DISCOVER	The TOE must be able to scan files stored on a network to detect content defined to be sensitive, to classify files according to defined attributes, and to take defined actions.
O.MONITOR	The TOE must be able to monitor, at the application level, data passing across a network, and be able to provide notification and evidence of defined traffic.
O.CAPTURE	The TOE must be able to capture email, web and network communications traffic for later data loss analysis.
O.AUDIT	The TOE must record events generated by its data loss prevention activity, and must audit use of the TOE functions on the management system.
O.AUDIT_PROTECT	The TOE must provide the capability to protect the confidentiality and integrity of audit information generated by the TOE.
O.AUDIT_REVIEW	The TOE must provide the capability for authorized administrators to review DLP records and audit information generated by the TOE.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data on the management system.
O.ACCESS	The TOE must restrict user access to only those TOE functions and data for which they are authorized.
O.CONTRADICT	The TOE must consistently interpret contradictory policy rules data.
O.CRYPTO	The TOE must use only cryptographic modules that have been validated to FIPS 140 when providing cryptographic services to protect the integrity of data in transit.

Table 13 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

82 The security objectives for the operational environment are listed below:

OBJECTIVE	DESCRIPTION
OE.PHYSICAL	Those responsible for the TOE must ensure that the hardware on which the TOE and IT environment software are installed is protected from any physical attack.
OE.PLATFORM	The hardware, operating system, and other software on which the TOE depends, must operate correctly.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is installed, managed, and operated in a manner which is consistent with provided guidance.
OE.IDAUTH	The IT environment must also be able to identify and authenticate user credentials on the management systems when requested by the TOE.
OE.INTEROP	The TOE must be interoperable with the managed systems that it monitors.
OE.PERSON	Personnel working as authorized administrators must be carefully selected and trained for proper operation of the system.
OE.DATABASE	Those responsible for the TOE must ensure that access to the database via mechanisms outside the TOE boundary (e.g., DBMS) is restricted to authorized users only.
OE.STORAGE	The IT environment must manage the storage and retrieval of TOE data in the databases as directed by the TOE.
OE.TIME	The IT Environment must provide reliable timestamps to the TOE.
OE.LDAP	The IT environment must maintain confidentiality and integrity for data transferred between the TOE and the LDAP server.

Table 14 – Operational Environment Security Objectives

Application Note: With regard to OE.PHYSICAL it should be noted that different levels of protection will be appropriate for different hardware platforms. Whereas, to avoid large scale compromise of the TOE, it may be appropriate to protect the ePO server, DLP servers and DBMS hardware in server rooms with limited access, this may not be appropriate for managed PCs and laptops. For such managed computers network users should provide protection appropriate to the data being stored and processed, and no special measures would be expected.

4.3 Security Objectives Rationale

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

OBJECTIVE THREAT / ASSUMPTION	O.DLP	O.DISCOVER	O.MONITOR	O.CAPTURE	O.AUDIT	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.EADMIN	O.IDAUTH	O.ACCESS	O.CONTRADICT	O.CRYPTO	OE.PHYSICAL	OE.PLATFORM	OE.CREDEN	OE.INSTALL	OE.IDAUTH	OE.INTEROP	OE.PERSON	OE.DATABASE	OE.STORAGE	OE.TIME	OE.LDAP
T.DATA_LOSS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓							✓						
T.CONF_COMP					✓		✓		✓	✓			✓		✓		✓			✓			
T.INT_COMP					✓		✓		✓	✓			✓		✓		✓			✓			
T.CH_CONFIG					✓		✓		✓	✓			✓		✓		✓			✓			
T.NO_HALT									✓	✓			✓		✓		✓						
T.CONFLICT											✓												
T.PRIVIL									✓	✓					✓		✓			✓			✓
T.ACCOUNT					✓	✓	✓															✓	
P.CRYPTO												✓				✓							
A.ACCESS																		✓					
A.MTA																✓							
A.DATABASE													✓							✓			
A.NOEVIL													✓		✓	✓			✓				
A.PROTECT													✓										✓
A.PLATFORM														✓							✓		

Table 15 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

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

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.DATA_LOSS	*Users may store or transmit sensitive data in a manner that is inconsistent with a defined organizational policy, leading to loss of confidentiality. Such data may include, for example, intellectual property, trade secrets, or financial information.* O.DLP states the need for the TOE to be configurable to monitor access to sensitive data, and to define actions to be taken when access in conflict with defined policy is detected. This includes monitoring of email and web traffic, and export to external storage. O.DISCOVER addresses analysis of data at rest. O.MONITOR addresses examination of application traffic on a network. O.CAPTURE requires that the TOE be capable of storing email, web and network communications traffic for later data loss analysis. O.AUDIT covers the recording of information gathered and policy violations. O.AUDIT_PROTECT requires that the collected information is protected, and O.AUDIT_REVIEW requires that is can be reviewed by authorized administrators. O.IDAUTH, OE.IDAUTH and O.ACCESS control access to the stored records. O.EADMIN addresses the need for an effective set of management functions that allow data loss policy to be specified, applied, and its implementation monitored.
T.CONF_COMP	*An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.* O.IDAUTH and OE.IDAUTH require that administrators be identified and authenticated before access is granted, thus inhibiting unauthorized users from gaining access to TOE data. O.ACCESS further restricts the actions of authenticated users. OE.PHYSICAL aims to prevent access to the TOE platforms by those aiming to access TOE data. OE.CREDEN specifies that administrators must protect their access credentials against disclosure. OE.DATABASE aims to prevent access directly to the data stored in the database that bypasses TOE mechanisms. O.AUDIT specifies that all management actions are audited, allowing any such access to be monitored using O.AUDIT_REVIEW.

T.INT_COMP	*An unauthorized user may attempt to modify the data collected and produced by the TOE by bypassing a security mechanism.* O.IDAUTH and OE.IDAUTH require that administrators be identified and authenticated before access is granted, thus inhibiting unauthorized users from gaining access and modifying TOE data. O.ACCESS further restricts the actions of authenticated users. OE.PHYSICAL aims to prevent access to the TOE platforms by those aiming to modify TOE data. OE.CREDEN specifies that administrators must protect their access credentials against disclosure. OE.DATABASE aims to prevent access directly to the data stored in the database that bypasses TOE mechanisms. O.AUDIT specifies that all management actions are audited, allowing any such changes to be monitored using O.AUDIT_REVIEW.
T.CH_CONFIG	*An unauthorized user may inappropriately modify the configuration of the TOE causing potential data loss to go undetected.* O.IDAUTH and OE.IDAUTH require that administrators be identified and authenticated before access is granted, thus inhibiting unauthorized users from gaining access and modifying the TOE configuration. O.ACCESS further restricts the actions of authenticated users. OE.PHYSICAL aims to prevent access to the TOE platforms by those aiming to change its configuration. OE.CREDEN specifies that administrators must protect their access credentials against disclosure. OE.DATABASE aims to prevent access directly to the configurations stored in the database that bypasses TOE mechanisms. O.AUDIT specifies that all management actions are audited, allowing any such changes to be monitored using O.AUDIT_REVIEW.
T.NO_HALT	*An unauthorized user may attempt to compromise the continuity of the system's collection and analysis functions by halting execution of the TOE.* O.IDAUTH and OE.IDAUTH require that users of the management system be identified and authenticated before access is granted, thus inhibiting unauthorized users from gaining access and halting TOE execution. O.ACCESS further restricts the actions of authenticated users. OE.PHYSICAL aims to prevent access to the TOE platforms by those aiming to disable its operation. OE.CREDEN specifies that administrators must protect their access credentials against disclosure.
T.CONFLICT	*Policy rules may include contradictions that may both explicitly permit and deny certain actions leading to unpredictable results in policy enforcement.* O.CONTRADICT specifies that the TOE must predictably interpret rules that are in conflict (e.g. rules to explicitly permit and deny an action).

T.PRIVIL	*An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.* The O.IDAUTH and OE.IDAUTH objectives provide for identification and authentication of users prior to any TOE data access. OE.IDAUTH provides the same for when the TOE is configured to use the operational environment for identification and authentication. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by only permitting users to access TOE functions for which they are authorized. OE.DATABASE aims to prevent access directly to the database that bypasses TOE mechanisms. OE.CREDEN specifies that administrators must protect their access credentials. OE.LDAP specifies that communications with the LDAP server must be protected.
T.ACCOUNT	*Users may not be accountable for their actions when administering the TOE; and consequently errors and omissions may go undetected, leading to failures in policy enforcement.* O.AUDIT states that the actions of administrators must be recorded, allowing them to be held to account. O.AUDIT_PROTECT states the intent to protect the confidentiality and integrity of that information. O.AUDIT_REVIEW requires the capability for an authorized administrator to review the audit data. OE.TIME requires the environment to provide reliable time stamps for the audit data.
P.CRYPTO	*When providing cryptographic services the TOE must use cryptographic modules that have been validated to FIPS 140.* The TOE addresses this through O.CRYPTO, and the requirement that where options exist the correct modes are chosen on installation is addressed through OE.INSTALL.
A.ACCESS	*The TOE has appropriate access to the systems it is intended to manage.* The OE.INTEROP objective ensures the TOE is interoperable with the systems that is monitors, and therefore can gain access to the system and user data required to carry out monitoring activities.
A.MTA	*The MTA is configured to route email traffic via DLP Prevent, and to act on the header strings that DLP Prevent adds to the email messages.* This is addressed through OE.INSTALL, requiring that the operational environment, including the MTA, is installed, managed and operated in line with provided guidance. The provided guidance covers the requirements in the assumption.
A.DATABASE	*Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.* The OE.DATABASE objective ensures that access to any mechanisms outside the TOE boundary that may be used to access the database is configured by the administrators such that only authorized users may utilize the mechanisms. Direct access to the TOE is restricted through the OE.PHYSICAL objective.

A.NOEVIL	*The administrators assigned to manage the TOE are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.* The OE.INSTALL objective ensures that the TOE is properly installed and operated, and the OE.PHYSICAL objective provides for physical protection of the TOE and its operational environment by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data. The OE.PERSON objective supports this by requiring careful selection and training of administrators.
A.PROTECT	*The hardware on which the TOE and the IT environment software are installed will be protected from unauthorized physical modification.* The OE.PHYSICAL objective provides for the physical protection of the hardware on which the TOE and IT environment software are installed.OE.LDAP specifies that communications with the LDAP server must be protected.
A.PLATFORM	*The hardware, operating system, and other software on which the TOE depends, operate correctly.* The OE.PLATFORM objective provides for the correct operation of the hardware, operating system and other software on which the TOE depends. OE_STORAGE covers the correct operation of the software used to sore and manage the TOE databases.

Table 16 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

85 This section provides a definition for the extended components used within this ST.

5.1 Class FDP: User data protection

5.1.1 FDP_DSC_EXT Object discovery

Family Behaviour

86 The requirements of this family ensure that the TSF will have the ability to identify operational environment user data that exhibit certain characteristics, and take some action based on this identification.

Component levelling

87 There is only one component in this family, FDP_DSC_EXT.1. FDP_DSC_EXT.1, Object Discovery, requires the TSF to search the Operational Environment for data that meets some criteria and take action based upon discovery of such data. The primary purpose of this requirement is for use in mandatory access control (MAC) or similar environments so that the TSF can identify data that is not in a location allowed by its associated attributes and subsequently take some form of corrective action based on this.

88 The FDP_DSC_EXT.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to examine and act upon an observation made of the operational environment.

Management: FDP_DSC_EXT.1

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

a) Management of the conditions for objects to be discovered, and the actions to be taken.

Audit: FDP_DSC_EXT.1

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

a) Minimal: the detection of objects meeting the conditions, and changes to the conditions for objects to be discovered;

b) Basic: the action taken on detection of an object meeting the conditions, and changes to the actions to be taken.

FDP_DSC_EXT.1 Object discovery

Hierarchical to: No other components

Dependencies: No dependencies

FDP_DSC_EXT.1.1 The TSF shall be able to discover objects in the operational environment based on the following criteria: [assignment: *list of conditions that indicate that data residing in the Operational Environment should be catalogued by the TSF*]].

FDP_DSC_EXT.1.2 The TSF shall be able to take the following actions upon discovery of an object meeting the specified conditions: [selection: *record, encrypt, move, copy, classify, quarantine, content fingerprint, apply rights management policy*].

5.1.2 FDP_STG_EXT User data storage

Family Behaviour

89 The requirements of this family ensure that stored user data will be retained for the maximum time allowed by the configured storage.

Component levelling

90 There is only one component in this family, FDP_STG_EXT.1 Action in event of possible user data loss, which specifies actions to be taken if user data to be stored exceeds the available storage.

Management: FDP_STG_EXT.1

91 No management actions are foreseen.

Audit: FDP_STG_EXT.1

92 There are no auditable events foreseen.

FDP_STG_EXT.1 Action in event of possible user data loss

Hierarchical to: No other components

Dependencies: No dependencies

FDP_STG_EXT.1.1 The TSF shall [assignment: *actions to be taken in case of possible user data storage failure*] if the [assignment: *data storage repository*] is full.

6 Security Requirements

93 The security requirements for the TOE are specified in this section.

6.1 Security Functional Requirements

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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
User data protection	FDP_DSC_EXT.1	Object discovery
	FDP_STG_EXT.1	Action in event of possible user data loss
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and authentication	FIA_ATD.1	User attribute definition
	FIA_UID.2	User identification before any action
	FIA_UAU.2	User authentication before any action
	FIA_USB.1	User-subject binding
Security management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_TDC.1	Inter-TSF basic TSF data consistency

Table 17 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

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

c) [*The events identified in Table 18 – Audit Events and Details*].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*the information detailed in Table 18 – Audit Events and Details*].

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

SFR	EVENT	ADDITIONAL DETAILS RECORDED
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to the TOE and system data	Object IDs, Requested access
FAU_SAR.1	Reading of information from the audit records.	
FAU_SAR.2	Reading of information from the audit records. Note: Unsuccessful attempts to read information from the audit records do not occur because the TOE does not present that capability to users that are not authorized to read the audit records.	
FDP_DSC_EXT.1	Detection of user data that meets criteria specified in a rule. Action taken on detection of data that meets criteria specified in a rule.	Data at rest: Location of data, rule being applied Data in motion: Rule being applied, presumed address of source and destination

SFR	EVENT	ADDITIONAL DETAILS RECORDED
FDP_IFF.1	All decisions on requests for information flow.	The presumed address of the source and destination subject
FIA_ATD.1	All changes to TSF data (including passwords) result in an audit record being generated.	
FIA_UID.2	All use of the user identification mechanism	Location
FIA_UAU.2	All use of the user authentication mechanism	Location
FIA_USB.1	Successful binding of attributes to subjects is reflected in the audit record for successful authentication. Unsuccessful binding does not occur in the TOE design.	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_MSA.1	All modifications to security attributes	
FMT_SMF.1	Use of the management functions.	Function used
FMT_SMR.1	Modifications to the group of users that are part of a role	

Table 18 – Audit Events and Details

Application Note: The audit events as defined in this ST cover both the ePO management events that are audited, and the DLP events that are identified through application of DLP policies that are reported back to ePO from DLP servers and managed systems.

6.1.1.2 FAU_GEN.2 User Identity Association

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

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [*Administrators or users assigned to the Global reviewer permission set*] with the capability to read [*all information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*sorting and filtering*] of audit data based on [*the fields listed in the table below*].

Event type	Field	Filter/Sort
ePO Operational Events	Action	Sort
	Completion time	Filter, Sort
	Details	Sort
	Priority	Sort
	Start Time	Filter, Sort
	Success	Filter, Sort
	User Name	Sort
DLP Event Manager	Event type	Filter
	Date seen	Filter
	File hash	Filter
	System id	Filter
	Rule name	Filter

Table 19 – Selectable audit review fields

6.1.1.6 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

6.1.2 User data protection (FDP)

6.1.2.1 FDP_DSC_EXT.1 Object discovery

FDP_DSC_EXT.1.1 The TSF shall be able to discover objects in the operational environment based on the following criteria: [*document properties, file information, file creating application, objects containing specified words, objects containing data matching specified patterns, location*].

FDP_DSC_EXT.1.2 The TSF shall be able to take the following actions upon discovery of an object meeting the specified conditions: [record, encrypt, move, copy, classify, quarantine, content fingerprint, apply rights management policy].

Application note: FDP_DSC_EXT.1 is not applicable to DLP Endpoint on Apple macOS.

Application note: FDP_DSC_EXT.1 is applicable both to real time analysis, and to the analysis of traffic data stored by the TOE.

6.1.2.2 FDP_STG_EXT.1 User data storage

FDP_STG_EXT.1.1 The TSF shall [*delete older captured data*] if the [*storage available for captured data*] is full.

6.1.2.3 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [*DLP Information flow control SFP*] on [

Subjects: *Endpoint user and external IT entities attempting to transfer or transmit data*

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

Operations: *Copy (to a different destination), upload (to web/ftp destination), send to printer, send by email*].

Application Note: The following table gives examples of subject/information/object relationships on which the DLP Information Flow Control SFP is enforced (items 2, 3, 4 and 6 are not applicable to DLP Endpoint on Apple macOS):

	Subject	***Operation***	***Information***
1	*an endpoint user at managed workstation*	*copying to a USB device*	*a file*
2	*an endpoint user, using email client on managed workstation*	*sending an email*	*with an attachment*
3	*an endpoint user at managed workstation*	*sending to a printer*	*a document*
4	*an endpoint user using ftp client on managed workstation*	*uploading to a FTP server*	*a file*
5	*an endpoint user at managed workstation*	*copying to a different file server*	*a file*
6	*an endpoint user at a managed workstation*	*access web address*	*web page contents*
7	*an endpoint user at a managed workstation*	*access to an application file*	*application files*

6.1.2.4 FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [*DLP Information Flow Control SFP*] based on the following types of subject and information security attributes:

[*Subject: Context*

- *User identity or membership in AD Group*
- *Managed system*
- *Application performing the copy / transmission action/protocol*

Information Security Attributes: Content Classification

- *Dictionary*
- *File Extension*
- *Source IP address*
- *Destination IP address*
- *Registered document repository*[6]
- *Text Pattern*
- *Whitelisted text (to reduce false positive detection)*
- *Email Destination (recipients)*
- *Printer to which the information is transmitted*
- *Web Destination to where the file is uploaded or sent*
- *Destination File server to where the file is copied (e.g. copying of sensitive information to the public share is not allowed)*]

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: [*unless an explicit DLP data protection rule is enabled to deny the information flow (see FDP_IFF.1.5 below)*].

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

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

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*a DLP data protection rule is enabled for the subject and information attributes and has a block reaction configured*].

Application note: *For example, block send email if the sender is member of the finance (AD group) and the information contains more than 1 social security number (text patterns) and more than 1 credit card number (text pattern) and email is sent to email recipients outside the corporate domain.*

[6] This refers to a set of confidential documents that are manually selected by DLP administrators and uploaded to the DLP management console in order create fingerprints of these documents. The fingerprints are distributed to all DLP endpoint clients, and allow DLP endpoint client to detect fragments of text from these confidential documents and block (or report) the copy or transmission of content from these files by FTP, email or web-upload.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 User Attribute Definition

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

a) ePO User name;

b) *Authentication configuration (either Windows authentication or local ePO password);*

c) *Permission Sets*].

6.1.3.2 FIA_UID.2 User Identification before any action

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

6.1.3.3 FIA_UAU.2 User authentication before any action

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

Application Note: The TOE performs identification on the management system, and then, depending on the configuration of the user account, either relies upon Windows for authentication or performs authentication based on the local ePO password. Hence, authentication on the management system is the responsibility of the operating environment when Windows authentication is configured.

6.1.3.4 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [

a) ePO user name; and

b) Permissions].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [*user security attributes are bound upon successful login with a valid ePO User Name*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [*user security attributes do not change during a session*].

Application Note: The TOE binds security attributes to subjects for ePO sessions. Windows binds security attributes to subjects for workstation sessions. Permissions are determined by the union of all permissions in any permission set associated with a user. If the security attributes for a user are changed while that user has an active session, the new security attributes are not bound to a session until the next login.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [DLP *Information flow control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*content classification*] to [*an Administrator or a user with permissions*].

6.1.4.2 FMT_MSA.3 Static attribute initialisation

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

FMT_MSA.3.2 The TSF shall allow the [*Administrator or a user with specific permission*] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.3 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [query, modify, delete, clear, [*create, view, copy, export, access, assign and use*]] the [*TSF data identified in Table 20 – TSF Data Access Permissions*] to [*an Administrator or a user with permissions*].

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
Agent Handler	View Agent Handlers	View
	Edit Agent Handlers, Create and Edit Agent Handler Groups, Create and Edit Agent Handler Assignments	View, create, modify, delete agent handlers, agent handler groups and agent handler assignments
Appliance Management	View Health and Statistics	View
	View, Create and Change Database Tasks	View, create, modify, delete
Appliance Management Common Policy	View Policy and Task Settings	View
	View and Change Policy and Task Settings	View, modify
Audit Log	View Audit log	View
	View and purge audit log	View, delete
Automatic Response	View Responses, View Response Results in the Server Task Log	View
	Create, Edit. Review and Cancel Responses, View Response Results in the Server Task Log	Create, view, modify, delete responses, view response results
Client Events	View Client Events	View
	View, Delete and Purge Client Events	View, delete
Contacts	Use Contacts	View
	Create and Edit Contact Entries	Create, view,, modify, delete
Dashboards	Use public dashboards	View public dashboards
	Use public dashboards, create and edit private dashboards	View public dashboards, create and modify private dashboards

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
	Use public dashboards, create and edit private dashboards, make private dashboards public	View public dashboards, create, delete and modify private dashboards, make private dashboards public
DLP Policy Catalog	View Any DLP Policy	View
DLP Discover	Full permissions	All
DLP Policy Manager	Rule Sets Access Control: Use Permissions, View and Use Permissions, Full Permissions	Create, view, modify, delete
	Override Permissions for Specific Rule Sets	View, modify, delete
	Rule Types: Data Protection, Device Control, Discovery	Create, view, modify, delete
DLP Classifications	Classification Actions: Manage Manual Classifications	Create, view, modify, delete
	Registered Documents and Whitelisted Text	Create, view, modify, delete
	Use Permissions	Copy
	View and Use Permissions	View
	Full Permissions	Create, view, modify, delete
	Override Permissions for Specific Classifications	View, modify, delete
DLP Definition Permissions	Use Permissions	Use items of this type in classification criterions, discovery scans and DLP protection rules.
	View and Use Permissions	- Use items of this type in classification criterions, discovery scans and DLP protection rules. - View the content of a definition item.
DLP Incident Management	Incident Access by Type: Data Protection, Device Control, Endpoint Discovery, Network Discovery	View
	Incident Access by Reviewer: View Incidents Assigned to User, View Incidents Assigned to permission Set, View All Incidents	View, set reviewer, add comments, set severity, set resolution
	Incident Data Redaction: Supervisor Permission, Obfuscate Sensitive Incidents Data	View

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
	Incident Tasks: Create a Mail Notification Task, Create a Purge Notification Task, Create a Set Reviewer Task	View, create, delete, modify
DLP Operational Events	Operational Reviewer: View Operations Events Assigned to User, View Operations Events Assigned to Permission Set, View All Operational Events	View, set reviewer, add comments, set severity, set resolution
	Operational Tasks: Create a Mail Notification Task, Create a Purge Notification Task, Create a Set Reviewer Task	View, create, delete, modify
DLP Case Management	View Cases Assigned to User	View
	View Cases Assigned to Permission Sets	View
	View All Cases	View
DLP Settings Tabs	General, Advanced	Use
	Incident Manager	Use
	Operations Center	Use
	Case Management	Use
	Backup and Restore	Use
DLP Capture	Search List	Create, view, modify, delete
	Search Results	View
	Datasets	Create, view, modify, delete, use
	Definitions	Create, view, modify, delete
DLP Appliance Management Policy	View Policy and Task Settings	View
	View and Change Policy and Task Settings	View, modify
DLP Event Notifications	Registered Executable: View Registered Executable, Create and Edit Registered Executables	Create, view, modify, delete
	View My Organization	Create, view, modify, delete rules and notifications
Helpdesk Actions	Generate Client Uninstall Key	Create
	Generate Bypass Client Key	Create
	Generate Release from Quarantine Key	Create

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
	Generate Master Response Key for the Keys Above	Create
Issue Management	View Issues	View
	Create Issues and Edit, View and Purge Issues Created By or Assigned To Me	Create, view, modify, delete for user
	Create, Edit, View and Purge Issues	Create, view, modify, delete
LDAP	Browse registered servers	View, modify, delete
McAfee Agent	View Policy Settings	View
	View and Change Policy Settings	View, modify
	View Task Settings	View
	View and Change Task Settings	View, modify
McAfee Labs	View McAfee Labs Portal	View
Multi-Server Roll-Up Data	Run and Edit Queries Based on Roll-Up Data	View, query
	Run and Edit Queries Based on Roll-Up Data, Schedule Roll-Up Data Tasks, Purge Roll-Up Data	View, query, delete
Policy Assignment Rule	View Rules	View
	View and Edit Rules	Create, view, modify, delete
Product Investment Program	View Policy and Task Settings	View
	View and Change Policy and Task Settings	View, modify
Queries and Reports	Use public groups	Query and use public groups
	Use public groups; create and edit private queries/reports	Query and use public groups; create and modify private queries/reports
	Edit public groups; create and edit private queries/reports; make private queries/reports public	Query, delete, modify and use public groups; create, delete and modify (including make public) private queries/reports
Registered Servers	Database Server: View Registered Servers, View, Create and Edit Registered Servers	Create, view, modify, delete
	LDAP Server: View, Create and Edit Registered Servers	Create, view, modify, delete
	View Registered Servers: View, Create and Edit Registered Servers	Create, view, modify, delete

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
	ePO: View Registered Servers, View, Create and Edit Registered Servers	Create, view, modify, delete
	SNMP Server: View Registered Servers, View, Create and Edit Registered Servers	Create, view, modify, delete
Server Tasks	View Scheduler Tasks, View Scheduler Task Results in the Server Log	View
	Create, Edit, Run, View and End Scheduler Tasks, View Scheduler Task Results in the Server Log	Create, view, modify, use, delete
Software	Master Repository: View Packages, Add, Remove and Change Packages, Perform Pull Tasks	Create, view, delete
	Distributed Repositories: View Repositories, Add, Remove and Change Repositories, Perform Pull Tasks	Create, view, delete
Software Manager	View List of Available Products	View
Systems	System Tree: View "System Tree" Tab, Wake Up Agents, View Agent Activity Log, Edit System Tree Groups and Systems, Deploy Agents	View, modify, delete
System Tree access	My Organization	View, modify, delete

Table 20 – TSF Data Access Permissions

6.1.4.4 FMT_SMF.1 Specification of Management Functions

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

a) *ePO user account management,*

b) *Permission set management,*

c) *Audit log management,*

d) *DLP policy and rules management and monitoring, Incidents access control, DLP incidents data redaction, Incident task creation, Operational events,*

e) *Registered servers management,*

f) *Systems and system tree access,*

g) *Query and report management,*

h) *Dashboard management*].

6.1.4.5 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: [*Administrator and User with Selected Permissions*].

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

Application Note: In ePO a role is called a permission set.

6.1.5 Cryptographic Support (FCS)

6.1.5.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*see table below*] and specified cryptographic key sizes [*see table below*] that meet the following*: [list of standards -see table below*].

Component	Purpose	Algorithm	Key size	Standard
ePO	TLS	CTR_DRBG for deterministic random bit generation	256 (AES), 2048 (RSA)	NIST Special Publication 800-90 (CAVP DRBG algorithm certificate #1451)
MA	TLS	HMAC_DRBG for random number generation	256 (AES), 2048 (RSA)	NIST Special Publication 800-90A (CAVP DRBG algorithm certificate #191)

Table 21 - Key generation

6.1.5.2 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 level 1*].

6.1.5.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [*encryption/decryption, digital signature services, hashing services and keyed hash message authentication services to support TLS 1.2*] in accordance with a specified cryptographic algorithm [*see table below*] and cryptographic key sizes [*see table below*] that meet the following: [*list of standards - see table below]*.

Cryptographic operation	Cryptographic algorithm	Key sizes (bits)	Standards
Key Transport	RSA encrypt/decrypt	2048	Allowed in FIPS mode (CAVP RSA algorithm certificates: ePO #2444, MA #1046)
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (operating in CBC mode)	256	FIPS 197 (CAVP AES algorithm certificates: ePO #4469, MA #2017)
Secure Hashing	SHA-256	Not Applicable	FIPS 180-3 (CAVP SHS algorithm certificates: ePO #3681, MA #1767)

Table 22 - Cryptographic operations

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from [<u>disclosure and modification</u>] when it is transmitted between separate parts of the TOE.

6.1.6.2 FPT_TDC.1 Inter-TSF Basic TSF Data Consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [*authentication information*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [*the rules listed below*] when interpreting the TSF data from another trusted IT product.

a) For Active Directory (LDAP servers), the data is interpreted according to the LDAP version 3 protocol.

b) For NT Domains, the data is interpreted according to the NetBIOS protocol.

c) When conflicting information is received from different sources, highest priority is given to information learned from the McAfee Agent, then to Active Directory, and finally to NT Domains.

6.2 Security Assurance Requirements

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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	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
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 23 – Security Assurance Requirements at EAL2

6.3 CC Component Hierarchies and Dependencies

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

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components	FPT_STM.1	Satisfied by OE.TIME in the environment
FAU_GEN.2	No other components	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied by FIA_UID.2
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components	FAU_SAR.1	Satisfied

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_SAR.3	No other components	FAU_SAR.1	Satisfied
FAU_STG.1	No other components	FAU_GEN.1	Satisfied
FDP_DSC_EXT.1	No other components	None	n/a
FDP_STG_EXT.1	No other components	None	n/a
FDP_IFC.1	No other components	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components	FDP_IFC.1 FMT_MSA.3	Satisfied
FIA_ATD.1	No other components	None	n/a
FIA_UID.2	FIA_UID.1	None	n/a
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2
FIA_USB.1	No other components	FIA_ATD.1	Satisfied
FMT_MSA.1	No other components	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1, FMT_SMF.1	Satisfied by FDP_IFC.1, FMT_SMR.1 and FMT_SMF.1
FMT_MSA.3	No other components	FMT_MSA.1, FMT_SMR.1	Satisfied
FMT_MTD.1	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components	None	n/a
FMT_SMR.1	No other components	FIA_UID.1	Satisfied by FIA_UID.2
FCS_CKM.1	No other components	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Satisfied by FCS_COP.1 and FCS_CKM.4
FCS_CKM.4	No other components	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	Satisfied by FCS_CKM.1

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FCS_COP.1	No other components	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Satisfied by FCS_CKM.1 and FCS_CKM.4
FPT_ITT.1	No other components	None	n/a
FPT_TDC.1	No other components	None	n/a

Table 24 – TOE SFR Dependency Rationale

6.4 Security Requirements Rationale

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

6.4.1 Security Functional Requirements for the TOE

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

OBJECTIVE SFR	O.DLP	O.DISCOVER	O.MONITOR	O.CAPTURE	O.AUDIT	O. AUDIT_PROTECT	O. AUDIT_REVIEW	O. EADMIN	O. IDAUTH	O.ACCESS	O.CONTRADICT	O.CRYPTO
FAU_GEN.1		✓	✓		✓							
FAU_GEN.2					✓							
FAU_SAR.1							✓			✓		
FAU_SAR.2							✓			✓		
FAU_SAR.3							✓					
FAU_STG.1					✓	✓						
FDP_DSC_EXT.1		✓	✓	✓								
FDP_STG_EXT.1				✓								
FDP_IFC.1	✓										✓	
FDP_IFF.1	✓										✓	
FIA_ATD.1									✓	✓		
FIA_UID.2									✓	✓		
FIA_UAU.2									✓	✓		
FIA_USB.1										✓		
FMT_MSA.1	✓	✓	✓	✓				✓				
FMT_MSA.3	✓							✓		✓	✓	
FMT_MTD.1	✓	✓	✓	✓			✓	✓	✓	✓		
FMT_SMF.1	✓	✓	✓	✓			✓	✓	✓	✓		
FMT_SMR.1		✓	✓	✓			✓	✓	✓	✓		
FCS_CKM.1												✓
FCS_CKM.4												✓

OBJECTIVE SFR	O.DLP	O.DISCOVER	O.MONITOR	O.CAPTURE	O.AUDIT	O. AUDIT_PROTECT	O. AUDIT_REVIEW	O. EADMIN	O. IDAUTH	O.ACCESS	O.CONTRADICT	O.CRYPTO
FCS_COP.1												✓
FPT_ITT.1	✓	✓	✓		✓	✓		✓				
FPT_TDC.1			✓		✓				✓			

Table 25 – Mapping of TOE SFRs to Security Objectives

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

OBJECTIVE	RATIONALE
O.DLP	*The TOE must be able to take defined actions upon detection of the access, transmission, printing, or copying of sensitive files or data from managed systems.* Rules can be specified and applied to control the flow of sensitive data (IFC.1, IFF.1). Restrictive defaults are applied to rule creation (FMT_MSA.3). The ability to define and distribute policy is restricted to authorized users (FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1). Policies must be protected during distribution (FPT_ITT.1).
O.DISCOVER	*The TOE must be able to scan files stored on a network to detect content defined to be sensitive, to classify files according to defined attributes, and to take defined actions.* Policy for scanning data at rest on the network must be defined (FDP_DSC_EXT.1), and securely distributed (FPT_ITT.1). The results of scanning activity and associated actions must be recorded (FAU_GEN.1). The ability to define and distribute policy is restricted to authorized users (FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1).
O.MONITOR	*The TOE must be able to monitor, at the application level, data passing across a network, and be able to provide notification and evidence of defined traffic.* Policy for scanning data in transit on the network must be defined (FDP_DSC_EXT.1), and securely distributed (FPT_ITT.1). The results of scanning activity must be recorded (FAU_GEN.1). The ability to define and distribute policy is restricted to authorized users (FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1).

OBJECTIVE	RATIONALE
O.CAPTURE	*The TOE must be able to capture email, web and network communications traffic for later data loss analysis.* Policy for scanning captured data must be defined (FDP_DSC_EXT.1), and securely distributed (FPT_ITT.1). Captured traffic data must be protected in the event of allocated storage exhaustion (FDP_STG_EXT.1). The results of scanning activity must be recorded (FAU_GEN.1). The ability to define and distribute policy is restricted to authorized users (FMT_MSA.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1).
O.AUDIT	*The TOE must record events generated by its data loss prevention activity, and must audit use of the TOE functions on the management system.* Security-relevant events must be defined and auditable for the TOE (FAU_GEN.1). The user associated with the events must be recorded (FAU_GEN.2). The TOE does not provide any mechanism for users to modify or delete audit records other than via configuration of the data retention timeframe, and that functionality is limited to administrators (FAU_STG.1). Audit data can be securely moved around the network (FPT_ITT.1, FTP_ITC.1).
O.AUDIT_PROTECT	*The TOE must provide the capability to protect the confidentiality and integrity of audit information generated by the TOE.* The TOE is required to protect the stored audit records from unauthorized deletion or modification at rest (FAU_STG.1) and in transit (FPT_ITT.1).
O.AUDIT_REVIEW	*The TOE must provide the capability for authorized administrators to review DLP records and audit information generated by the TOE.* The TOE provides the capability to review stored audit records relating both to DLP events and to administrative actions (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3). The permitted access to audit data by the roles and permissions is defined (FMT_MTD.1, FMT_SMF.1, FMT_SMR.1).
O.EADMIN	*The TOE must include a set of functions that allow effective management of its functions and data.* The functions and roles required for effective management are defined (FMT_SMF.1, FMT_SMR.1), and the specific access privileges for the roles and permissions is enforced (FMT_MSA.1, FMT_MTD.1). Secure default values are assigned to security attributes (FMT_MSA.3).

OBJECTIVE	RATIONALE
O.IDAUTH	*The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data on the management system.* Security attributes of subjects used to enforce the security policy of the TOE must be defined (FIA_ATD.1). Users authorized to access the TOE are determined using an identification process (FIA_UID.2) and an authentication process (either that provided by the TOE or ensuring that provided by the operational environment is applied) (FIA_UAU.2). Management of the identification and authentication process is restricted to Administrators (FMT_MTD.1, FMT_SMF.1, FMT_SMR.1). If Windows authentication is configured secure exchange with external servers must be supported (FPT_TDS.1).
O.ACCESS	*The TOE must restrict user access to only those TOE functions and data for which they are authorized.* Security attributes of subjects used to enforce the security policy of the TOE must be defined (FIA_ATD.1). Users authorized to access the TOE are determined using an identification process (FIA_UID.2) and an authentication process (either enforcing its own authentication process or ensuring that provided by the operational environment is applied) (FIA_UAU.2). Upon successful I&A, the security attributes for the user are bound to the subject so that proper access controls can be enforced (FIA_USB.1). The permitted access to TOE data by the roles and permissions is defined (FMT_MTD.1, FMT_SMF.1, FMT_SMR.1). Secure default values are assigned to security attributes (FMT_MSA.3). The audit log records may only be viewed by authorized users (FAU_SAR.1, FAU_SAR.2).
O.CONTRADICT	*The TOE must consistently interpret contradictory policy rules data.* In order for policy to be applied in a consistent manner the TOE must be able to define a set of monitoring and control rules that will be capable of resolving inconsistencies in a predictable manner (FDP_IFC.1, FDP_IFF.1).
O.CRYPTO	*The TOE must use only cryptographic modules that have been validated to FIPS 140 when providing cryptographic services to protect the integrity of data in transit.* The TOE uses cryptographic standards that are accepted for validation under (FCS_CKM.1, FCS_CKM.4, FCS_COP.1).

Table 26 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Rationale for TOE Assurance Requirements Selection

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

101 The general level of assurance for the TOE is:

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

6.5 TOE Summary Specification Rationale

102 This section demonstrates that the Security Functions provided by the TOE (as described in the TOE Summary Specification in section 7 below) completely and accurately meet the TOE SFRs.

103 The following tables provide a mapping between the Security Functions provided by the TOE and the SFRs and the rationale.

Security Function SFR	Policy Creation	Policy Enforcement	Identification & Authentication	Management	Audit	System Information Import	TSF Data Protection
FAU_GEN.1		✓			✓		
FAU_GEN.2					✓		
FAU_SAR.1		✓			✓		
FAU_SAR.2		✓			✓		
FAU_SAR.3		✓			✓		
FAU_STG.1		✓			✓		
FDP_DSC_EXT.1	✓	✓					
FDP_STG_EXT.1		✓					
FDP_IFC.1	✓	✓					
FDP_IFF.1	✓	✓					
FIA_ATD.1			✓				
FIA_UID.2			✓				
FIA_UAU.2			✓				
FIA_USB.1			✓				
FMT_MSA.1				✓			
FMT_MSA.3				✓			
FMT_MTD.1				✓		✓	

Security Function SFR	Policy Creation	Policy Enforcement	Identification & Authentication	Management	Audit	System Information Import	TSF Data Protection
FMT_SMF.1				✓		✓	
FMT_SMR.1				✓			
FCS_CKM.1							✓
FCS_CKM.4							✓
FCS_COP.1							✓
FPT_ITT.1		✓					✓
FPT_TDC.1						✓	

Table 27 – SFR to Security Functions Mapping

SFR	SECURITY FUNCTION AND RATIONALE
FAU_GEN.1	**Security Audit –** ePO user actions are audited according to the events specified in the table with the SFR. **Policy Enforcement -** In addition to the ePO audit data, the TOE also stores event data concerning potential data loss identified on the network.
FAU_GEN.2	**Security Audit –** The audit log records include the associated user name when applicable.
FAU_SAR.1	**Security Audit –** Audit log records are displayed in a human readable table form from queries generated by authorized users. **Policy Enforcement –** DLP event data are displayed in a human readable form in reports and from queries generated by authorized users.
FAU_SAR.2	**Security Audit –** Only authorized users have permission to query audit log records. **Policy Enforcement –** Only authorized users have permission to query DLP event data
FAU_SAR.3	**Audit –** The TOE provides functionality to sort and filter audit and DLP event data. **Policy Enforcement –** The TOE provides functionality to report on DLP events.

SFR	SECURITY FUNCTION AND RATIONALE
FAU_STG.1	**Security Audit –** The only mechanism provided by the TOE to cause audit records to be deleted is configuration of the data retention timeframe, which is restricted to administrators. The TOE does not provide any mechanism for users to modify audit records. **Policy Enforcement –** The TOE protects stored DLP event data against unauthorized deletion within the ePO database.
FDP_DSC_EXT.1	**Policy Creation –** An authorized ePO user can define policy for object discovery, and the actions to be taken. **Policy Enforcement -** The defined policy is deployed to managed systems and the Discovery server, to carry out searches according to defined schedules.
FDP_STG_EXT.1	**Policy Enforcement –** The TOE ensures that the most recent captured data is retained in the event of captured data storage exhaustion.
FDP_IFC.1	**Policy Creation –** An authorized ePO user specifies policy rules for managed systems. **Policy Enforcement** – The TOE implements data classification to identify/track sensitive data and protection rules to act when sensitive data is handled inappropriately.
FDP_IFF.1	**Policy Creation –** An authorized ePO user specifies policy rules for managed systems. **Policy Enforcement** – The TOE implements data classification to identify/track sensitive data and protection rules to act when sensitive data is handled inappropriately.
FIA_ATD.1	**Management** – User security attributes are associated with the ePO user account via ePO User Account management.
FIA_UID.2	**Identification & authentication** - The TSF requires users to identify and themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TOE. No action can be initiated before proper identification.
FIA_UAU.2	**Identification & authentication** - The TSF requires users to authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TOE. No action can be initiated before proper authentication.
FIA_USB.1	**Identification & authentication** - Upon successful login, the TOE binds the Administrator permission set or the union of all the permissions from the permission sets that are assigned to the user account configuration to the session.

SFR	SECURITY FUNCTION AND RATIONALE
FMT_MSA.1	**Management** – The Administrator permission set and user permission sets determine the access privileges of the user to security attributes.
FMT_MSA.3	**Management –** The TOE defines restrictive default values.
FMT_MTD.1	**Management** – The Administrator permission set and user permission sets determine the access privileges of the user to TOE data. **System Information Import –** A user with the necessary permissions can import system information to populate the system tree.
FMT_SMF.1	**Management** – The management functions that must be provided for effective management of the TOE are defined and described. **System Information Import –**System information can be imported to populate the system tree.
FMT_SMR.1	**Management** – The TOE provides the roles specified in the SFR. When a user account is created or modified, the role is specified by assigning one or more ePO permission sets for the user.
FCS_CKM.1	**TSF Data Protection** – The TOE provides cryptographic services to protect the TSF data while it is in transit.
FCS_CKM.4	**TSF Data Protection** – The TOE provides cryptographic services to protect the TSF data while it is in transit.
FCS_COP.1	**TSF Data Protection** – The TOE provides cryptographic services to protect the TSF data while it is in transit.
FPT_ITT.1	**Policy Enforcement –** Policies are protected during distribution to managed systems. Event data is protected during transport to storage in the ePO database. **TSF Data Protection –** The TOE protects TSF data while in transit between ePO and MA.
FPT_TDC.1	**System Information Import** – The TOE provides the functionality to import asset authentication data information from Active Directory (LDAP servers) or NT Domains and correctly interpret the information.

Table 28 – SFR to Security Function Rationale

7 TOE Summary Specification

104 The TOE monitors and protects sensitive information from being disclosed through various channels, including email, print, upload to the web or copy to an external storage device. Protection rules control the flow of data by defining the action taken when an attempt is made to transfer or transmit sensitive data. Protection rules link actions with definitions, content classification, and end-user groups.

105 Using DLP software involves the following tasks:

- Defining policy – creating classifications and definitions; using them to create data protection, device and discovery rules.
- Assigning rule sets to DLP policies. For Discover, create scan definitions.
- Assign and deploy the policies in the System Tree. For McAfee DLP Discover, apply policy to the Discover servers.
- Monitoring events — using the DLP Incidents Manager to view, filter, and sort events in the enterprise network.
- Performing administrative maintenance — Keeping the DLP Agents up-to-date and generating agent override, agent uninstall, and quarantine release keys as required.

7.1 Policy creation

106 A DLP policy consists of rules, grouped into rule sets. Rules use classifications and definitions to specify what McAfee DLP detects. Rule reactions determine the action to take when data matches the rule. An authorized ePO user must first specify DLP policy rules for the managed systems. This is done using the ePO policy catalog. After creating the rules required for the enterprise, these must be enforced by assigning the policy to managed computers.

7.1.1.1 Classify

107 Content is classified by defining *classifications* and *classification criteria*. Classification criteria define the conditions on how data is classified. Methods to define criteria include advanced pattern matching, dictionaries, file types and source/destination location.

7.1.1.2 Track

108 DLP can track content based on storage location or the application used to create it. DLP Endpoint for Windows users can also create manual classifications that can be used to track any file. The mechanisms used to track content are:

- Content fingerprinting – supported on DLP Endpoint (for Windows);
- Registered documents – supported on DLP Endpoint (for Windows) and DLP Prevent;
- Manual classifications – created only by DLP Endpoint users, but supported on all McAfee DLP products.

Content fingerprinting

109 Content fingerprinting is a content tracking technique unique to the DLP Endpoint product. The administrator creates a set of content fingerprinting criteria that define either the file location or the application used to access the file, and the classification to place on the files. The DLP

Endpoint client tracks any file that is opened from the locations, or by the applications, defined in the content fingerprinting criteria and creates fingerprint signatures of these files in real time when the files are accessed. It then uses these signatures to track the files or fragments of the files.

Registered documents

110 The registered documents feature is based on pre-scanning all files in specified repositories (such as the engineering SharePoint) and creating signatures of fragments of each file in these repositories. These signatures are then distributed to all managed endpoints. The DLP Endpoint client is then able to track any paragraph copied from one of these documents, and to classify it according to the classification of the registered document signature.

Manual classification

111 Users working with manual classification have the option of applying content fingerprints or content classifications to their files. Manually applied content fingerprinting is identical to the automatically applied fingerprinting described previously. Manually applied content classifications embed a physical tag in the file which can be used to track the file wherever it is copied, but do not create signatures, so content copied from these files into other files can't be tracked.

7.1.1.3 Protect

112 Rules are created to identify sensitive data and take appropriate action. Protection rules define the action taken when an attempt is made to transfer or transmit tagged data. The protection rule specifies the transfer method, content classification name(s) to protect, a set of specific conditions related to the transfer method (such as email recipients, printer names or network shares), and how the system should react to the event. Each event is given a severity level, and options for responding to the event. In some cases, protection rules merely log the event. In other cases, the protection rules prevent transfer of data, and notify the user of the violation. Protection rules can be applied to specific users by setting the rule conditions to apply only for specific end-user groups.

113 Rules are comprised of conditions, exceptions, and actions. Conditions contain multiple parameters, such as classifications, to define the data or user action to identify. Exceptions specify parameters to exclude from triggering the rule. Actions specify how the rule behaves when a rule is triggered, such as blocking user access, encrypting a file or creating an incident.

Data Protection rules

114 Data protection rules are used by DLP Endpoint, Device Control and DLP Prevent to prevent unauthorized distribution of classified data. When a user tries to copy or attach classified data, DLP intercepts the attempt and uses the data protection rules to determine what action to take. For example, DLP Endpoint can halt the attempt and display a dialog to the end user. The user inputs the justification for the attempt, and processing continues.

115 DLP Prevent uses web and email protection rules to monitor and take action on communication from an MTA server or web proxy server.

116 DLP Monitor can apply the network communication protection, email protection, or web protection rules to analyze supported traffic on a network.

117 McAfee Device Control uses only removable storage data protection rules.

Device Control rules

118 Device Control rules monitor and potentially block the system from loading physical devices such as removable storage devices, Bluetooth, Wi-Fi, and other plug-and-play devices. Device Control rules consist of device definitions and reaction specifications, and can be assigned to specific end-user groups by filtering the rule with end-user group definitions.

Application Control rules

119 Application control rules monitor and block user access to websites. For example, a web application control rule blocks a specified URL, either by name or reputation.

Discovery rules

120 Discovery rules are used by DLP Endpoint and DLP Discover for file and data scanning.

121 Endpoint Discovery is a crawler that runs on managed computers. It scans the local endpoint file system and the local email (cached) inbox and PST files. Local file system and email storage discovery rules define whether the content is to be quarantined, tagged, or encrypted. These rules can also define whether the classified file or email is reported as an incident, and whether to store the file or email as evidence included in the incident. File system scans are not supported on server operating systems.

122 DLP Discover scans repositories and can move or copy files, apply Rights Management policies to files, and create incidents.

Rule sets

123 Rules are organized into rule sets. A rule set can contain any combination of rule types.

Policies

124 Policies contain active rule sets and are deployed from ePO to the DLP Endpoint client software, Discovery server, or DLP Prevent appliance. DLP Endpoint policies also contain policy assignment information and definitions.

ACTIONS RULES	Apply RM Policy	Block	Set classification tag	Report Incident	Notify User	Quarantine	Read Only	Request Justification	Store Evidence
Plug and Play device rules (2)		✓		✓	✓				
Removable storage device rules (3)		✓		✓	✓		✓		
Removable Storage File Access rule		✓		✓	✓				
Citrix XenApp Device rule (3)		✓							
Fixed Hard Drive rule (3)		✓		✓	✓		✓		
TrueCrypt Device rule (3)		✓		✓	✓		✓		

ACTIONS RULES	Apply RM Policy	Block	Set classification tag	Report Incident	Notify User	Quarantine	Read Only	Request Justification	Store Evidence
Application file access protection rules		✓		✓	✓				✓
Clipboard protection rules		✓		✓	✓				✓
Cloud protection rules	✓	✓		✓				✓	✓
Email protection rules (3)		✓		✓	✓			✓	✓
Network communication protection rules (3)		✓		✓	✓				
Network share protection rules				✓	✓			✓	✓
Printing protection rules (3)		✓		✓	✓			✓	✓
Removable storage protection rules		✓		✓	✓			✓	✓
Screen capture protection rules (3)		✓		✓	✓				✓
Web post protection rules (3)		✓		✓	✓			✓	✓
Local file system discovery rules (3)	✓		✓	✓	✓ (1)	✓			✓
Local email storage discovery rule (3)			✓	✓	✓ (1)	✓			✓

Table 29 – Rules and their actions

(1) Since discovery rules run at-rest and not as result of a user action, the user may not notice the "user notification" hence the "user notification" action in discovery rules is not showing a popup dialog to the end-user: instead it logs the event in the DLP endpoint console, and also leaves a "placeholder" file instead of a file if the file is quarantined.

(2) For DLP Endpoint for Mac Plug and Play rules relate to USB only.

(3) Rules marked (3) in the above table are not implemented on DLP Endpoint for Mac.

125 After creating the rules and definitions required for the enterprise, they must be enforced by assigning the policy to managed computers. Once the policy is in place, the DLP Incident Manager is used to monitor the state of the enterprise's sensitive information.

TOE Security Functional Requirements Satisfied: User Data Protection (FDP_DSC_EXT.1, FDP_IFC.1, FDP_IFF.1)

7.2 Policy Enforcement

126 The McAfee DLP classification engine applies definitions and classification criteria that define the content to be protected, and where and when the protection is applied. Protection rules apply the classification criteria and other definitions to protect the sensitive content.

127 Monitoring functions include:

- **Incident management** — Incidents are sent to the McAfee ePO Event Parser and stored in a database. Incidents contain the details about the violation, and can optionally include evidence information. Incidents and evidence can be viewed as they are received in the **DLP Incident Manager** console.
- **Case management** — Group related incidents into cases for further review in the **DLP Case Management** console.
- **Operational events** — View errors and administrative events in the **DLP Operations** console.
- **Evidence collection** — For rules that are configured to collect evidence, a copy of the data or file is saved and linked to the specific incident. This information can help determine the severity or exposure of the event.
- **Hit highlighting** — Evidence can be saved with highlighting of the text that caused the incident. Highlighted evidence is stored as a separate encrypted HTML file.
- **Reports** — DLP Endpoint can create reports, charts, and trends for display in ePO dashboards.

128 The table below shows the predefined ePO dashboards and available functions for the Policy Enforcement TSF:

NAME	DESCRIPTION
Agent version	Displays the distribution of agents in the enterprise. Used to monitor agent deployment progress.
Agent Status	Displays the status of agents in the enterprise. Used to monitor how many agents running and enforcing rules, how many installations failed and how many have no policies.
Policy Distribution	Displays the number of endpoint per DLP policy instance. For example: 2,500 systems with the DLP Japan policy and 15,000 with DLP EMEA policy.
Bypassed agents	Displays how many DLPe nodes are in policy bypass mode. This is a real-time view that refreshes when a bypass begins or expires.
Agent Operations Mode	Displays how many agents are in device control mode and how many are enforcing data protection & device control.
Enforced Rule sets	Displays the number of computers enforcing each rule set.
Privileged Users	Displays how many DLPe sessions are running by a privileged user mode. Policy rules with a block action will not block and simply report an incident if running on a system with a logged on privileged user (e.g. Senior VP, CFO).
Policy Revision Distribution	Displays the number of endpoint enforcing each DLP policy revision. Used to monitor progress when deploying a new policy. Example: ePO has 2 DLP policies (Japan, EMEA) and some machines might not get the latest revision of the Japan policy (because they were disconnected from network for long time).

Table 30 – Predefined DLP Dashboards

7.2.1 DLP Endpoint

129 The McAfee DLP Endpoint client software is deployed as a McAfee Agent plug-in, and enforces the policies defined in the McAfee DLP policy. The McAfee DLP Endpoint client software audits user activities to monitor, control, and prevent unauthorized users from copying or transferring sensitive data. It then generates *events*.

130 Events generated by the McAfee DLP Endpoint client software are sent to the McAfee ePO Event Parser, and recorded in tables in the McAfee ePO database. Events are stored in the database for further analysis and used by other system components.

131 Different device and protection rules can be applied, depending on the endpoint Operating System (Windows or macOS), and whether the managed computer is *online* (connected to the enterprise network) or *offline* (disconnected from the network). Some rules also allow differentiation between computers within the network and those connected to the network by VPN.

132 The endpoint console was designed to share information with the user and to facilitate self-remediation of problems. On Windows-based computers, the console is activated from the icon in the System Tray. On Mac endpoints, the console is activated from the McAfee menulet on the status bar.

7.2.2 DLP Discover

133 DLP Discover runs on Microsoft Windows servers and scans network file systems to identify and protect sensitive files and data.

134 ePO uses McAfee® Agent to install and deploy the McAfee DLP Discover software to a Discover server — a designated Windows server. ePO applies the scan policy to Discover servers, which scan the repository at the scheduled time. The data collected and the actions applied to files depend on the scan type and configuration.

7.2.3 DLP Prevent

135 DLP Prevent interacts with email traffic, generates incidents, and records the incidents in McAfee ePO for subsequent case review. It also receives ICAP connections from a web proxy server, analyzes the content, and determines if the traffic should be allowed or blocked.

7.2.4 DLP Monitor

136 DLP Monitor acts passively to monitor network traffic, and does not enforce policy other than to monitor and report on traffic as directed.

7.2.5 DLP Capture

137 The DLP Capture feature allows storage of email, web and network data that has been analyzed by Prevent and Monitor appliances with the feature enabled. Content in the DLP Capture database can then be searched, and rules and classification settings tuned. This permits the content to be searched for data loss events that may have been missed during real

time analysis, and allows rules and classifications to be tuned to reduce false positives without affecting live analysis of the data.

138 By default, captured data is removed automatically from storage after 28 days, but this limit can be modified by an authorized administrator. If captured data storage nears capacity before the specified limit is reached then older data is automatically removed to provide space.

139 The ability to tune rules and search captured data is controlled using the Capture permission set.

140 Datasets to be searched can be based on the following criteria:

a) Appliance,

b) Incident triggered,

c) Protocol,

d) Subject of an email message,

e) Time range,

f) URL to which data was uploaded,

g) VLAN (Monitor only),

h) Email recipient and/or sender,

i) Destination and/or source address,

j) Destination and/or source port,

k) Destination and/or source user,

l) Keywords or phrases.

141 Configured searches and the results of searches can be viewed using ePO using the Search List. The results of searches can also be exported.

TOE Security Functional Requirements Satisfied: Security Audit (FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1), User Data Protection (FDP_DSC_EXT.1, FDP_STG_EXT.1, FDP_IFC.1, FDP_IFF.1), Protection of the TSF (FPT_ITT.1)

7.3 Identification and Authentication

142 Users must log in to ePO with a valid user name and password supplied via a GUI before any access is granted by the TOE to TOE functions or data. When the credentials are presented by the user, ePO determines if the user name is defined and enabled. If not, the login process is terminated and the login GUI is redisplayed.

143 If Windows authentication is enabled, the supplied password is passed to Windows for validation, otherwise it is validated against ePO's internal password store. If authentication is successful, the TOE grants access to additional TOE functionality. If the validation is not successful, the login GUI is redisplayed. Note that all the Windows I&A protection mechanisms (e.g., account lock after multiple consecutive login failures) that may be configured still apply since Windows applies those constraints when performing the validation.

144 Upon successful login, the union of all the permissions from the permission sets from the user account configuration are bound to the session (if a user account is assigned as an "Administrator", no other permissions sets can be bound to that account). Those attributes remain fixed until the user refreshes their session by logging out and logging back in.

TOE Security Functional Requirements Satisfied: Identification and Authentication) FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1

7.4 Management

145 The TOE's Management Security Function provides administrator support functionality that enables an administrator or user with selected permissions to configure and manage TOE components. Management of the TOE is performed via the ePO GUI. Management permissions are defined per- ePO user.

146 The TOE provides functionality to manage the following:

1. ePO User Accounts,
2. Permission Sets,
3. Audit Log,
4. DLP Policy and rules,
5. Registered Servers,
6. Systems and System Tree access,
7. Queries and Reports,
8. Dashboards.

147 Each of these items is described in more detail in the following sections.

7.4.1 ePO User Account Management

148 Each user authorized for login to ePO must be defined with ePO. Only ePO Administrators may perform ePO user account management functions (create, view, modify and delete). For each defined account, the following information is configured:

1. User name;
2. Enabled or disabled;
3. Whether authentication for this user is to be performed by ePO or Windows;
4. Permission sets granted to the user.

149 One or more permission sets may be associated with an account. ePO Administrators are only granted permission as "Administrator" and have access to everything in ePO.

150 Permissions exclusive to ePO administrators (i.e., not granted via permission sets) include:

1. Create and delete user accounts.
2. Create, delete, and assign permission sets.

7.4.2 Permission Set Management

151 A permission set is a group of permissions that can be granted to any users by assigning it to those users' accounts. ePO provides the following predefined permission sets:

- Executive Reviewer
- Global Reviewer
- Group Admin
- Group Reviewer

152 When a user account is created, the user can be assigned to either a permission set (pre-defined or administrator defined) or assigned as an "Administrator". If the new user account is assigned to a permission set they are considered to be an "ePO user", whereas if they are assigned to "Administrator" they are considered to be an "Administrator".

153 One or more permission sets can be assigned to any users who are not ePO administrators (ePO administrators can only be assigned as an Administrator).

154 Permission sets only grant rights and access — no permission ever removes rights or access. When multiple permission sets are applied to a user account, they aggregate. For example, if one permission set does not provide any permissions to registered servers, but another permission set applied to the same account grants all permissions to registered servers, that account has all permissions to registered servers.

155 When a new ePO product extension (e.g., DLP) is installed into ePO it may add one or more groups of permissions to the permission sets. Initially, the newly added section is listed in each permission set as being available but with no permissions yet granted. The Administrators can then grant permissions to users through existing or new permission sets.

156 Administrators may create, view, modify and delete permission sets. Each permission set has a unique name so that it can be appropriately associated with ePO users.

157 When a permission set is created or modified, the permissions granted via the permission set may be specified by an Administrator.

7.4.3 Audit Log Management

158 An ePO Administrator may view and purge events in the audit log. A user with the appropriate permissions may view only, or view and purge events in the audit log.

7.4.4 DLP Policy and rules

159 A product policy is a collection of settings that are created, configured, and then enforced. Product policies ensure that McAfee Agent and DLP components are configured and perform accordingly on DLP servers and managed systems. Different policy rules for the same product may be configured for different groups. When product policy settings are reconfigured, the new settings are delivered to, and enforced on, the managed systems at the next agent-server communication.

160 The permissions associated with product policy management are:

1. Policy - This permission can be used to grant the ability to view and save policies.
2. Rule Sets – this permission can be used to grant the ability to view, create, modify and delete rule sets
3. Classifications – this permission can be used to grant the ability to view, create, modify and delete classifications, classification criterions and tagging criterions
4. Manage manual classification – this permission can be used to grant the ability to define which end-users will be allowed to manually classify files.
5. Manage registered documents and whitelisted text – this permission can be used to grand the ability to upload files to be indexed and registered as well as upload and register whitelisted text snippets.
6. Definitions – this permission can be used to grant the ability to view, create, modify and delete different types of definitions, such as Text Patterns, Dictionaries, Email lists, URL lists and end-user groups as well as many other definition types.
7. Incidents Access Control - This permission grants the ability to view incidents.
8. Incidents data redaction - This permission grants the ability control whether data is redacted or in clear text.
9. Incident task creation - This permission grants the ability to view, create, delete and modify mail notification tasks, purge tasks or set a reviewer task.
10. Operational events - This permission grants the ability to view, create, delete and modify operational events.

161 Product policies are applied to any group or system by one of two methods, inheritance or assignment. Inheritance determines whether the product policy settings for a group or system are taken from its parent. By default, inheritance is enabled throughout the System Tree. When this inheritance is broken by assigning new product policies anywhere in the System Tree, all child groups and systems that are set to inherit the product policy from this assignment point do so. An ePO Administrator can assign any product policy in the Policy Catalog to any group or system. Assignment allows the definition of product policy settings once for a specific need and then the application of this product policy to multiple locations.

162 All product policies are available for use by any user, regardless of who created the product policy. To prevent any user from modifying or deleting other users' named product policies, each product policy is assigned an owner — the user who created it. Ownership provides that no one can modify or delete a product policy except its creator or an ePO administrator. When a product policy is deleted, all groups and systems where it is currently applied inherit the product policy of their parent group.

163 Once associated with a group or system, enforcement of individual product policies may be enabled and disabled by an ePO Administrator.

7.4.5 Registered Servers Management

164 Registered servers allows for integration of ePO with other external servers. For example an LDAP server may be registered to facilitate connection to an Active Directory server for

synchronization of active directory system and user data with ePO. ePO Administrators may create, view, modify and delete registered servers. Servers may be registered as:

- McAfee ePO – additional McAfee ePO servers for use with the main ePO server to collect or aggregate data,
- LDAP – as above, to synchronize directory system and user data,
- SNMP – to receive SNMP traps,
- Database servers – to retrieve data from a database server.

165 ePO Users can only be granted permission to view registered server settings by assigning the “View registered servers” permission from the Registered Servers permission set.

7.4.6 Systems and System Tree Access

166 The System Tree organizes managed systems in units for monitoring, assigning policies, scheduling tasks, and taking actions. The System Tree is a hierarchical structure that allows organization of systems within units called groups.

167 Groups have these characteristics:

1. Groups can be created by ePO administrators or users with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.
2. A group can include both systems and other groups.
3. Groups are modified or deleted by a ePO administrator or user with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.

168 The System Tree root includes a Lost&Found group. Depending on the methods for creating and maintaining the System Tree, the server uses different characteristics to determine where to place systems. The Lost&Found group stores systems whose locations could not be determined. The Lost&Found group has the following characteristics:

1. It can't be deleted.
2. It can't be renamed.
3. Its sorting criteria can't be changed (although sorting criteria for subgroups can be created)
4. It always appears last in the list and is not alphabetized among its peers.
5. All users with view permissions to the System Tree can see systems in Lost&Found.
6. When a system is sorted into Lost&Found, it is placed in a subgroup named for the system’s domain. If no such group exists, one is created.

169 Child groups in the System Tree hierarchy inherit policies set at their parent groups. Inheritance is enabled by default for all groups and individual systems that are added to the System Tree. Inheritance may be disabled for individual groups or systems by an ePO Administrator. Inheritance can be broken by applying a new policy at any location of the System Tree (provided a user has appropriate permissions). Users can lock policy assignments to preserve inheritance.

170 Groups may be created manually or automatically (via synchronization with Active Directory or NT Domains). Systems may be deleted or moved between groups by a Global Administrator or user with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.

7.4.7 Queries and Reports Management

171 Users may create, view, modify, use and delete queries/reports based upon their permissions. Permissions associated with queries/reports are:

1. Use public groups — Grants permission to use any groups that have been created and made public.
2. Use public groups; create and edit private queries/reports — Grants permission to use any groups that have been created and made public by users with the same permissions, as well as the ability to create and edit personal queries/reports.
3. Edit public groups; create and edit private queries/reports; make personal queries/reports public — Grants permission to use and edit any public queries/reports, create and modify any private queries/reports, as well as the ability to make any private query/reports available to anyone with access to public groups.

7.4.8 Dashboard Management

172 User-specific dashboards may be configured to display data of interest to each user; these chart-based displays are updated at a configured rate to keep the information current. Permissions relevant to dashboards are:

1. Use public dashboards
2. Use public dashboards; create and edit personal dashboards
3. Edit public dashboards; create and edit personal dashboards; make personal dashboards public

TOE Security Functional Requirements Satisfied: Identification and Authentication (FIA_ATD.1), Security Management (FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1)

7.5 Security Audit

7.5.1 ePO audit log

173 The Audit Log maintains a record of ePO user actions. The auditable events are specified in Table 18 – Audit Events and Details.

174 The Audit Log entries display in a sortable table. For added flexibility, the log can be filtered so that it only displays failed actions, or only entries that are within a certain age. The Audit Log displays seven columns:

1. Action — The name of the action the ePO user attempted.
2. Completion Time — The date and time the action finished.
3. Details — More information about the action.

4. Priority — Importance of the action.
5. Start Time — The date and time the action was initiated.
6. Success — Specifies whether the action was successfully completed.
7. User Name — User name of the logged-on user account that was used to take the action.

175 Audit Log entries can be queried by an ePO Administrator or users assigned to the Global reviewer permission set. The ePO Administrator can select to purge Audit Log entries. No mechanisms are provided for modification of audit log entries, or for ePO Users to delete entries. The audit log entries are stored in the database; if space is exhausted, new entries are discarded.

7.5.2 DLP events

176 DLP events that are recorded as a result of the application of DLP policies are also treated as audit data, but are stored separately in the ePO database. Recent events can be viewed via the Incident Management page in ePO.

177 The TOE provides the following DLP Information Flow Control SFP events:

NAME	DESCRIPTION
Number of Incidents per day	Displays the number of incidents that were triggered each day.
Local file system scan status	Display the number of endpoint systems per each status of local file system scan (i.e. running, completed, unknown, no scan defined)
Operational events per type	Display the number of operational events per type of operation issue
Incidents by Incidents Type	Displays the number of DLP incidents for each event type
Number of operational events per day	Displays the number of incidents that were triggered each day.
Incidents per Rule Set	Displays the number of incidents for each rule set.
Incidents by Severity	Displays the number of DLP incidents for each severity level.
Local email storage scan status	Display the number of endpoint systems per each status of local file system scan (i.e. running, completed, unknown, no scan defined)
Undefined Device Classes	Lists and shows a bar graph of the devices whose device class cannot be determined.

Table 31 – Predefined DLP Event Reports

178 DLP agents inspect all end-user attempts to transmit/copy/email/print/etc. data, but record only those attempts that violate a DLP rule (that is included in the policy). DLP agents record the violation only if the rule is configured to record the incident. The TOE can be configured to

block the action without recording the incident, although the default is to record. This information is recorded in the DLP Incidents Manager (not in ePO audit log), and can be reviewed there using filters.

TOE Security Functional Requirements Satisfied: Security Audit (FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1)

7.6 System Information Import

179 ePO offers integration with both Active Directory and Windows domains as a source for systems, and even (in the case of Active Directory) as a source for the structure of the System Tree.

180 Active Directory synchronization can be used to create, populate, and maintain part or all of the System Tree with Active Directory synchronization. Once defined, the System Tree is updated with any new systems (and sub-containers) in Active Directory.

181 There are two types of Active Directory synchronization (systems only and systems and structure) that can be used based on the desired level of integration with Active Directory.

182 With each type, the following synchronization options are available:

1. Deploy agents automatically to systems new to ePolicy Orchestrator.
2. Delete systems from ePolicy Orchestrator (and remove their agents) when they are deleted from Active Directory.
3. Prevent adding systems to the group if they exist elsewhere in the System Tree.
4. Exclude certain Active Directory containers from the synchronization. These containers and their systems are ignored during synchronization.

183 The System Tree can be populated with the systems in the Windows domain. When synchronizing a group to a Windows domain, all systems from the domain are put in the group as a flat list. Those systems can be managed in a single group or via subgroups for more granular organizational needs.

184 When systems are imported, their placement in the System Tree may be automatically determined by criteria-based sorting of two forms. IP address sorting may be used if IP address organization coincides with the management needs for the System Tree. Tag based sorting may be used to sort systems based on tags associated with them.

185 The server has three modes for criteria-based sorting:

1. Disable System Tree sorting
2. Sort systems on each agent-server communication — Systems are sorted again at each agent-server communication. When the sorting criteria on groups is changed, systems move to the new group at their next agent-server communication.
3. Sort systems once — Systems are sorted at the next agent-server communication and marked to never be sorted again.

4. **TOE Security Functional Requirements Satisfied:** Security Management (FMT_MTD.1, FMT_SMR.1, FMT_SMF.1), Protection of the TSF (FPT_TDC.1)

7.7 TSF Data protection

186 Communications between McAfee Agents and ePO take the form of XML messages. Communications can include policies to implement, properties collected from the DLP servers or managed systems, event data gathered by the DLP components, or tasks to be run on the servers or managed systems. The messages are transferred via HTTPS. The TOE protects these transmissions between the ePO and the McAfee Agent from disclosure and modification by encrypting the transmissions under TLS, using AES operating in CBC mode, with 256 bit key size (by default the cipher used by ePO and McAfee Agent is TLS_DHE_RSA_WITH_AES_256_CBC_SHA256).

187 In FIPS mode, ePO uses OpenSSL v1.0.2p with FIPS module v2.0.16 (FIPS 140-2 certificate #2398) for TLS 1.2. Key generation uses CTR_DRBG for deterministic random bit generation, following NIST Special Publication 800-90 (CAVP DRBG algorithm certificate #1451). Zeroisation of cryptographic keys and other sensitive data is carried out before memory is deallocated.

188 McAfee Agent uses RSA BSAFE Crypto-C Micro Edition v4.0.1 (FIPS 140-2 certificate #2097) to provide cryptographic services for this link. Key generation uses HMAC_DRBG for deterministic random bit generation, following NIST special Publication 800-90 (CAVP DRBG algorithm certificate #191). Zeroisation of cryptographic keys and other sensitive data is carried out before memory is deallocated.

189 McAfee affirms that the cryptographic modules have been implemented in accordance with their FIPS 140 security policies, and when the TOE is configured in FIPS mode the cryptographic functions operate as intended.

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards	CAVP Cert #
Key Transport	RSA encrypt/decrypt	2048	Allowed in FIPS mode	OpenSSL #2444 BSAFE #1046
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (operating in CBC mode)	256	FIPS 197	OpenSSL #4469 BSAFE #2017
Secure Hashing	SHA-256	Not Applicable	FIPS 180-3	OpenSSL #3681 BSAFE #1767

Table 32 - Cryptographic operations ePO/MA

TOE Security Functional Requirements Satisfied: Cryptographic Services (FCS_CKM.1, FCS_CKM.4, FCS_COP.1), Protection of the TSF (FPT_ITT.1)