Security Target

McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2

Document Version 1.8

April 17, 2017

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

38North Security, LLC

2020 Pennsylvania Ave NW, Suite 254

Washington, DC 20006

www.38northsecurity.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

1 Introduction 6
1.1 ST Reference 6
1.2 TOE Reference 6
1.3 Document Organization 6
1.4 Document Conventions 7
1.5 Document Terminology 7
1.6 TOE Overview 8
1.7 TOE Description 9
1.7.1 McAfee Endpoint Security (ENS) Client 9
1.7.2 McAfee Agent 10
1.7.3 McAfee ePolicy Orchestrator (ePO) 10
1.7.4 Physical Boundary 11
1.7.5 Hardware and Software Supplied by the IT Environment 14
1.7.6 Logical Boundary 15
1.7.7 TOE Data 17
1.8 Rationale for Non-bypassability and Separation of the TOE 19

2 Conformance Claims 21
2.1 Common Criteria Conformance Claim 21
2.2 Protection Profile Conformance Claim 21

3 Security Problem Definition 22
3.1 Threats 22
3.2 Organizational Security Policies 23
3.3 Assumptions 23

4 Security Objectives 25
4.1 Security Objectives for the TOE 25
4.2 Security Objectives for the Operational Environment 25
4.3 Security Objectives Rationale 26

5 Extended Components Definition 32
5.1 Anti-Malware (FAM) Class of SFRs 32
5.1.1 FAM_ACT_(EXT).1 Anti-Malware Actions 32
5.1.2 FAM_ALR_(EXT).1 Anti-Malware Alerts 33
5.1.3 FAM_SCN_(EXT).1 Anti-Malware Scanning 34
5.2 Extended Component – Audit Data Generation 34
5.2.1 FAU_GEN_EXT.1 Audit Data Generation (Extended) 35

6 Security Requirements 36
6.1 Security Functional Requirements 36
6.1.1 Security Audit (FAU) 36
6.1.2 Anti-Malware (Explicitly Stated) 38
6.1.3 Cryptographic Support (FCS) 40
6.1.4 Information Flow Control (FDP) 41
6.1.5 Identification and Authentication (FIA) 43
6.1.6 Security Management (FMT) 44

6.1.7 Protection of the TSF (FPT) 49
6.2 Security Assurance Requirements *50*
6.3 CC Component Hierarchies and Dependencies *50*
6.4 Security Requirements Rationale *51*
6.4.1 Security Functional Requirements for the TOE 51
6.4.2 Security Assurance Requirements 54
6.5 TOE Summary Specification Rationale *55*
7 TOE Summary Specification 59
7.1 Client Threat Prevention *59*
7.1.1 Viruses 60
7.1.2 Access Point Violations 60
7.1.3 Potentially Unwanted Code and Programs 61
7.1.4 Buffer Overflow Exploits 61
7.2 Client Communications Protection *61*
7.3 Client Web Protection *63*
7.4 Identification & Authentication *64*
7.5 Management *65*
7.5.1 User Account Management 65
7.5.2 Permission Set Management 66
7.5.3 Audit Log Management 66
7.5.4 Event Log Management 66
7.5.5 System Tree Management 67
7.5.6 Query Management 68
7.5.7 Dashboard Management 68
7.5.8 Endpoint Security Common Module Management 68
7.5.9 Client Threat Prevention Policy Management 68
7.5.10 Client Communications Protection Policy Management 69
7.5.11 Client Web Protection Policy Management 69
7.6 Audit *70*
7.6.1 Audit and Server Task Logs 70
7.6.2 Threat Event Log 71
7.7 Protected System Data Transfer *71*

List of Tables

Table 1 – ST Organization and Section Descriptions 7
Table 2 – Terms and Acronyms Used in Security Target 8
Table 3 – Evaluated Configuration for the TOE 12
Table 4 – ePO Management System Component Requirements 14
Table 5 – Supported ENS Client and Agent Platforms 14
Table 6 – Supported Internet browsers for Web Control Functionality 15
Table 7 – Logical Boundary Descriptions 17

Table 8 – ePO TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information) 17
Table 9 – Client Threat Prevention TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information) 18
Table 10 – Client Communications Protection TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information) 19
Table 11 – Client Web Protection TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information) 19
Table 12 – Threats Addressed by the TOE and Operational Environment (Management System) 22
Table 13 – Threats Addressed by the TOE (Managed Systems) 23
Table 14 – Organizational Security Policies 23
Table 15 – Assumptions 24
Table 16 – TOE Security Objectives 25
Table 17 – Operational Environment Security Objectives 26
Table 18 – Mapping of Assumptions, Threats, and OSPs to Security Objectives 27
Table 19 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives 31
Table 20 – TOE Functional Components 36
Table 21 – Audit Events and Details 37
Table 22 – Cryptographic Operations 41
Table 23 – Management of TSF Behavior and Associated Permissions 44
Table 24 - TSF Data Access Permissions for ePO TOE Data 46
Table 25 - TSF Data Access Permissions for Client Threat Prevention 47
Table 26 - TSF Data Access Permissions for Client Communications Protection 47
Table 27 - TSF Data Access Permissions for Client Web Protection 48
Table 28 – Security Assurance Requirements at EAL2 50
Table 29 – TOE SFR Dependency Rationale 51
Table 30 – Mapping of TOE SFRs to Security Objectives 52
Table 31 – Rationale for Mapping of TOE SFRs to Objectives 54
Table 32 – Security Assurance Rationale and Measures 55
Table 33 – SFR to TOE Security Functions Mapping 56
Table 34 – SFR to TSF Rationale 58

List of Figures

Figure 1 – TOE Boundary 13

1 Introduction

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

1.1 ST Reference

ST Title	Security Target: McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2
ST Revision	1.8
ST Publication Date	April 17, 2017
Author	38North Security

1.2 TOE Reference

TOE Reference

- McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2, with these extensions installed:
  - Endpoint Security Platform 10.5.0 Extension, including:
    - Threat Prevention Extension 10.5.0
    - Firewall Extension 10.5.0
    - Web Control Extension 10.5.0
- McAfee Endpoint Security Client 10.5.0, including:
  - Threat Prevention Client 10.5.0
  - Firewall Client 10.5.0
  - Web Control Client 10.5.0
- McAfee Agent Version 5.0.4

TOE Type Anti-Malware, Client Firewall, Web Control

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE

SECTION	TITLE	DESCRIPTION
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

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

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by *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 <u>underlined</u> 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.

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

1.5 Document Terminology

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

TERM	DEFINITION
ASSC	Agent-server secure communication (ASSC)
CC	Common Criteria

TERM	DEFINITION
CM	Configuration Management
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
Exception	Defines a set of attributes that instructs the Agent to not enforce a rule or policy, resulting in an Event not being generated.
GUI	Graphical User Interface
HIP	Host Intrusion Prevention
I&A	Identification and Authentication
IPS	Intrusion Prevention System
IT	Information Technology
JRE	Java Runtime Environment
OS	Operating System
OSP	Organizational Security Policy
PDC	Primary Domain Controller
PP	Protection Profile
SFR	Security Functional Requirement
Signature	Signatures are patterns that indicate a potential security violation.
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

McAfee Endpoint Security (ENS) is a comprehensive security management solution that runs on Windows-based computers (clients) to identify and stop threats automatically. These threats include malware, suspicious communications, unsafe websites, and downloaded files. ENS intercepts threats, monitors overall system health, and reports detection and status information. While multiple management options are available, the TOE must be managed by McAfee ePolicy Orchestrator (ePO).

Security functionality is enforced on client computers through three integrated modules[1] working in tandem to protect systems from a wide range of threats from software, communications, and websites:

- McAfee Endpoint Security Threat Prevention (Threat Prevention) - Checks for viruses, spyware, unwanted programs, and other threats by scanning items automatically when users access them or on demand. Threat Prevention detects threats, then takes the actions that have been configured to protect systems.

[1] Adaptive Threat Protection (formerly named Threat Intelligence) is an optional ENS module that analyzes content from your enterprise and decides what to do based on file reputation, rules, and reputation thresholds. It is not part of the evaluated configuration.

- McAfee Endpoint Security Firewall (Firewall) - Monitors communication between the computer and resources on the network and the Internet. Intercepts suspicious communications.
- McAfee Endpoint Security Web Control (Web Control) - Displays safety ratings and reports for websites during online browsing and searching. Blocks access to websites based on safety rating or content.

Together, these modules are referred to as the McAfee Endpoint Security Client. In addition to the three integrated client modules, the TOE requires the installation of the McAfee Agent on each host to be protected. ENS software is operating system specific; only the Windows version is included in this evaluation.

The management capabilities for ENS are provided by ePO which manages McAfee Agents and ENS software residing on client (managed) systems. A centralized but distributed architecture allows the ENS software to be centrally managed and yet decrease network traffic required to manage clients. ePO provides the management interface and functionality for the administrators of the TOE. It also provides centralized audit collection and review functionality.

Communication between the distributed components of the TOE (i.e. Client/Agent and ePO server) is protected from disclosure and modification by cryptographic functionality provided by the TOE.

1.7 TOE Description

The TOE consists of both client and management software. Client software is installed on each host to be protected and comprises of the three integrated ENS modules (i.e. Threat Prevention, Firewall, and Web Control) and the McAfee Agent. Management software is installed on a dedicated server and is provided by ePO.

1.7.1 McAfee Endpoint Security (ENS) Client

The McAfee ENS Client is comprised of the Threat Prevention, Firewall and Web Control integrated modules as discussed in section 1.6. The ENS Client protects systems with regular upgrades, continuous monitoring, and detailed reporting. It does this through:

1. Silently monitoring all file input and output, downloads, program executions, inbound and outbound communications, visits to websites, and other activities on managed systems, then:
    - Deletes or quarantines detected viruses.
    - Removes potentially unwanted programs, such as spyware or adware.
    - Blocks or warns of suspicious activity, depending on product settings.

- Indicates unsafe websites with a color‐coded button or icon in the browser window or search results page. These indicators provide access to safety reports that detail site-specific threats.
- Blocks or warns of unsafe websites, depending on product settings.

2. Regularly connecting to the McAfee ePO server or directly to a site on the Internet to check for:
   - Updates to content files, which contain information that ENS uses to detect threats. These files are updated as new threats are discovered to ensure that systems are always protected against the latest threats.
   - Upgrades to software components.
   - If new versions are available, the client software downloads them.
3. Logging security information for each managed system, including protection status and details about detections. Security information is sent to the ePO server via the McAfee Agent for analysis, reporting and, if necessary, further administrator action.
4. Regularly communicating with the ePO management server via the McAfee Agent to:
   - Send logged security information.
   - Receive new policy assignments.

1.7.2 McAfee Agent

A software agent residing on each managed system which provides secure communication between the ENS Clients and the ePO server. The McAfee Agent is a vehicle of information and enforcement between the ePO server and each managed (client) system. It performs the following functions:

- Gathers information and events from managed systems and sends them to the ePO server.
- Installs the ENS Client on the managed systems.
- Provides the monitoring policies to the ENS client installed on the managed systems.
- Updates security content such as the policies enforced by the ENS Client.

1.7.3 McAfee ePolicy Orchestrator (ePO)

An application executing on a dedicated server which manages and securely communicates with all installed ENS Clients via the McAfee Agent. Administrators of the TOE use ePO to deploy software on client computers, manage detections, and configure security rules, called policies, that determine how product features work. The ePO server provides:

- The management interface and functionality for the administrators of the TOE.

- Centralized audit collection and review functionality, including the ability to run queries and reports on event data received from the managed systems.
- ENS-specific functions for administering policy management for the Threat Prevention, Firewall and Web Control integrated modules.

The ePO server software utilizes an external database to store all data collected, created and used by ePO, including: system properties, policy information, directory structure, threat events (information about detections), and all other relevant data that the server needs to keep managed systems up to date.

Agent-server secure communication (ASSC) occurs at regular intervals between the managed systems and the ePO server. The ePO server sends any available new policy assignments or product updates for ENS Client to the managed systems. This communication occurs shortly after the client software is installed and at regular intervals thereafter.

1.7.4 Physical Boundary

The TOE is software-only and includes:

1. The ENS Client software on each host to be protected;
2. The McAfee Agent executing on each host to be protected; and
3. The ePO application executing on a dedicated server.

The physical components of the TOE include the software that is installed during installation of ENS Client, McAfee Agent and ePO. The TOE software is installed on a centralized ePO server and on protected hosts (i.e. Windows-based client workstations and/or servers).

The hardware, operating systems and all third party support software (e.g., Internet browsers) on the systems on which the TOE executes are excluded from the TOE boundary. The database used by the ePO server is not part of the TOE.

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

TOE COMPONENT	VERSION/MODEL NUMBER

TOE COMPONENT	VERSION/MODEL NUMBER

TOE Software	• McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2, with these extensions installed:
	  o Endpoint Security Platform 10.5.0 Extension, including:
	  ▪ Threat Prevention Extension 10.5.0
	  ▪ Firewall Extension 10.5.0
	  ▪ Web Control Extension 10.5.0
	• McAfee Endpoint Security Client 10.5.0, including:
	  o Threat Prevention Client 10.5.0
	  o Firewall Client 10.5.0
	  o Web Control Client 10.5.0
	• McAfee Agent Version 5.0.4

IT Environment	Specified in the following: • Table 4 – ePO Management System Component Requirements • Table 5 – Supported ENS Client and Agent Platforms • Table 6 – Supported Internet browsers for Web Control Functionality
TOE Guidance Documentation	The guidance for the TOE is described in the following documentation: • Security Target: McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2 (this document) • Product Guide: McAfee Endpoint Security 10.5 • Installation Guide: McAfee Endpoint Security 10.5.0 • Product Guide: McAfee ePolicy Orchestrator 5.3.0 Software • Installation Guide: McAfee ePolicy Orchestrator 5.3.0 Software • Product Guide: McAfee Agent 5.0.3 • Operational User Guidance and Preparative Procedures Supplement: McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2

Table 3 – Evaluated Configuration for the TOE

The evaluated configuration consists of a single instance of the management system (with ePO) and one or more instances of managed systems (with McAfee Agent and the ENS Client).

ePO supports ePO authentication, Windows authentication and certificate-based authentication of user account credentials. The evaluated configuration requires the use of ePO authentication only.

The following figure presents an example of an operational configuration. The shaded elements in the boxes at the top of the figure represent the TOE components.

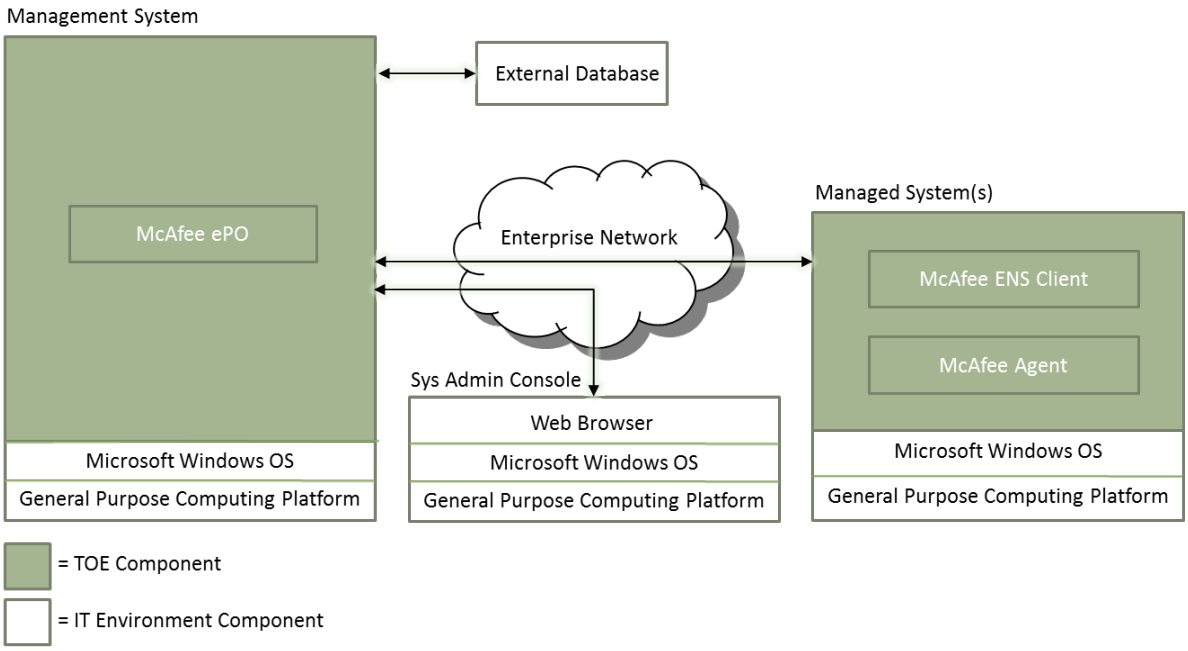

Figure 1 – TOE Boundary

The following specific configuration options apply to the evaluated configuration:

1. Adaptive Threat Protection[2] has been excluded from the evaluated configuration.
2. Self-managed systems (i.e. when a local system user installs the client software, customizes the features, and manages detections) have been excluded from the evaluation.
3. Management of the TOE via the McAfee ePO Cloud and the McAfee SecurityCenter have been excluded from the evaluation.
4. The IT Environment provides an external database for event storage, and other system data, used by the ePO server.
5. The ENS Client interface must be locked with self-protection enabled.
6. Certificate, Windows and LDAP user authentication methods to the ePO server have been excluded from the evaluated configuration.
7. The utilization of syslog servers, Windows event logs, XML API, email or Twitter accounts to send events and/or system messages has been excluded from the evaluated configuration.
8. Updates to the TOE software are not permitted in the evaluated configuration.
9. Running the McAfee ePO server in cluster mode is not permitted in the evaluated configuration.
10. The protection of TSF data transmitted between the administrator's web browser and the ePO server has been excluded from the evaluation.

[2] Adaptive Threat Protection (formerly named Threat Intelligence) is an optional ENS module that analyzes content from your enterprise and decides what to do based on file reputation, rules, and reputation thresholds. It is not part of the evaluated configuration.

11. The protection of TSF data transmitted between the ePO server and the external database has been excluded from the evaluation.

1.7.5 Hardware and Software Supplied by the IT Environment

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

The platform on which the ePO software is installed must be dedicated to functioning as the management system. ePO 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). The TOE requires the following hardware and software configuration on this platform:

Component	Minimum Requirements
Processor	64-bit Intel Pentium D or higher; 2.66GHz or higher
Memory	4 GB available RAM recommended minimum
Free Disk Space	5 GB — Recommended minimum
Operating System (64-bit)	Windows Server 2008 R2 Enterprise with Service Pack 1 Windows Server 2008 R2 Standard with Service Pack 1 Windows Server 2008 R2 Datacenter with Service Pack 1
DBMS	Microsoft SQL Server 2008 R2 Enterprise with Service Pack 1 Microsoft SQL Server 2008 R2 Express with Service Pack 1 Microsoft SQL Server 2008 R2 Standard with Service Pack 1 Microsoft SQL Server 2008 R2 Workgroup with Service Pack 1
Required Software	Microsoft .NET Framework 2.0 or later Microsoft Visual C++ 2005 SP1 Redistributable Microsoft Visual C++ 2008 Redistributable Package (x86) Microsoft XML Core Services (MSXML) 6.0
Internet Browser (required for management)	Google Chrome 17.0 or later

Table 4 – ePO Management System Component Requirements

The McAfee Agent and ENS Client execute on one or more managed systems. The supported platforms for these components are both client and server Windows-based operating systems:

OS TYPE	SUPPORTED AGENT OS	PLATFORM
Client	Windows 8.1 with Update 1 (all editions)	X64 platform
	Windows 8 (all editions)	X64 platform
	Windows 7 with SP1 (all editions)	X64 platform
Server	Windows Server 2012 (all editions)	X64 platform
	Windows Server 2008 R2 (all editions)	X64 platform

Table 5 – Supported ENS Client and Agent Platforms

In addition, the Web Control module of ENS is supported on one of these browsers (in conjunction with a reliable Internet connection):

SUPPORTED INTERNET BROWSERS FOR WEB CONTROL
Microsoft Internet Explorer 11
Mozilla Firefox 52
Google Chrome 57

Table 6 – Supported Internet browsers for Web Control Functionality

A full list of unevaluated supported operating systems can be found at the McAfee Knowledge Center, Technical Article ID: KB82761, located on the McAfee Service portal – URL: https://kc.mcafee.com/corporate/index?page=content&id=KB82761

1.7.6 Logical Boundary

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

TSF	DESCRIPTION
Client Threat Prevention	The TOE checks for malware (including viruses, trojan horses, adware, spyware, keyloggers, unwanted programs, etc), and other threats by scanning items (such as files, the registry and processes (programs) resident in memory) automatically when users access them or on demand. The TOE detects and reports (alerts) on threats, then takes the actions that have been configured to protect systems. Actions for detected malware include automatic quarantine, cleaning, and deletion from the affected system. Scans are configured as either “on-access” or “on-demand.” On-access scans will scan files as they first enter the system and deliver notifications to the user and management server when detections occur. On-demand scans are executed by the user manually or pre-defined by the administrator at a scheduled time, or at system startup. During either scan, files must meet predefined criteria to indicate a potential threat. Suspected threats are then compared against signatures for a possible match. Unwanted changes to managed systems are prevented by restricting access to specified items including ports, files, shares, the registry and keys. Rules can be created to report or block access to these items. The TOE compares a requested action against the list of rules and takes the action specified by the rule. The execution of potentially unwanted programs can also be blocked by the TOE. The execution of arbitrary code (such as buffer overflows) on managed systems is prevented by monitoring user-mode API calls to recognize when

TSF	DESCRIPTION
	they occur. When a detection occurs, information is recorded in the activity log, alerted on the client system, and sent to the management server.
Client Communications Protection	The TOE implements a firewall that scans all incoming and outgoing traffic on managed systems (i.e. clients). As it reviews arriving or departing traffic, the Firewall checks its list of rules, which is a set of criteria with associated actions. If the traffic matches all criteria in a rule, the Firewall acts according to the rule, blocking or allowing traffic through the Firewall. Firewall options and rules define how the Firewall works. Firewall Option settings enable the administrator to also block incoming and outgoing traffic from a network connection that McAfee Global Threat Intelligence (GTI)[3] rates as high risk. Rule groups organize firewall rules to simplify management. Information about threat detections is saved for reports that notify the user and administrator of any security issues for the managed system.
Client Web Protection	The TOE implements a Web Control feature that displays safety ratings and reports for websites during online browsing and searching. Websites are assigned a color-coded safety rating based on analysis and test results from McAfee. The software uses the test results to notify the user about web-based threats they might encounter while visiting the site. The safety rating is also present on search engine results pages. The administrator creates policies for Web Control on managed systems to control access to sites, pages, and downloads based on their safety rating or type of content. Sites may be blocked or allowed based on URLs and domains. The administrator can monitor and regulate browser activity on network computers, and create detailed reports about websites. The administrator can also control user access to Web Control features and configuration settings.
Identification and Authentication	The TOE requires administrative users to identify and authenticate themselves before accessing the TOE software or before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that defines the functionality the user is allowed to perform.

[3] McAfee GTI is a global Internet reputation intelligence system that determines what is good and bad behavior on the Internet. McAfee GTI uses real-time analysis of worldwide behavioral and sending patterns for email, web activity, malware, and system-to-system behavior. Using data obtained from the analysis, McAfee GTI dynamically calculates reputation scores that represent the level of risk to your network when you visit a webpage. The result is a database of reputation scores for IP addresses, domains, specific messages, URLs, and images.

TSF	DESCRIPTION
Management	The TOE's Management Security Function provides administrator functionality that enables a human user to configure and manage TOE components. Configuration functionality includes enabling a user to modify TSF Data. Management functionality includes invocation of TOE functions that effect security functions and security function behavior.
Audit	The TOE generates audit records upon detection of a potential security violation or system configuration events. The audit records can be viewed by an authorized user.
Protected Data Transfer	The TOE consists of distributed components. ePO server to McAfee Agent communication relies upon cryptographic functionality provided by the TOE to protect the information exchanged from disclosure or modification.

Table 7 – Logical Boundary Descriptions

1.7.7 TOE Data

TOE data consists of both TSF data and user data (information). TSF data consists of authentication data, security attributes, and other generic configuration information. Security attributes enable the TOE to enforce the security policy. Authentication data enables the TOE to identify and authenticate users.

1.7.7.1 ePO TOE Data

TSF Data	Description	AD	UA	GE
Audit Log	History list of all user actions on the ePO server.			✓
Dashboards	Collections of chart-based queries that are refreshed at a user-configured interval.			✓
ePO User Accounts	ePO user name, role, authentication type, logon status, and permission set for each user authorized to access TOE functionality on the management system.	✓		
Groups	Node on the hierarchical System Tree that may contain subordinate groups or systems.			✓
Permission	A privilege to perform a specific function.		✓	
Permission Set	A group of permissions that can be granted to any users by assigning it to those users' accounts.		✓	
Queries and Reports	Configurable objects that retrieve and display data from the database.			✓
Server Settings	Control how the ePolicy Orchestrator server behaves.			✓
System Information	Information specific to a single managed system (e.g. internet address) in the System Tree.			✓
System Tree	A hierarchical collection of all of the systems managed by ePolicy Orchestrator.			✓
Threat Event Log	Lists all threat events generated by the managed systems.			✓
User Interface Policies	Policies that control the access users have to the Endpoint Security client interface on the managed systems.			✓

Table 8 – ePO TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information)

1.7.7.2 Client Threat Prevention TOE Data

TSF Data	Description	AD	UA	GE
Access Protection Policies	Policies used to restrict access to specified ports, files, shares, registry keys, and registry values on the client systems.			✓
AMCore	A content file which contain the latest signatures by Threat Prevention on the client systems.			✓
Application Protection Lists	A list of applications that are protected by Exploit Prevention.			✓
Extra.DAT files	A temporary content file which contains information that Threat Prevention uses to handle new malware to be included in the next AMCore file update.			✓
Exclusions	An item to be excluded from an on-demand scan, or a process to be excluded from exploit prevention/access protection policies.			✓
Exploit Prevention Content	A content file containing memory protection signatures (for Generic Buffer Overflow Protection) and the Application Protection List.			✓
Exploit Prevention Policies	Policies used to prevent buffer overflows on the client systems.			✓
On-Access Scan Policies	Policies that enable and define when on-access scans are performed and the actions taken upon detection on the client systems. Also configures the settings and actions for standard, low and high risk processes.			✓
On-Demand Scan Policies	Policies that enable and configure the operation of on-demand scanning on the client systems, including full scans, quick scans, and right-click scanning.			✓
On-Demand Scan Tasks	Tasks that define the configuration of on-demand scans that may be invoked on the client systems.			✓
Options Policies	Policies that specify the quarantine settings, exclusions, and unwanted program detections on the client systems.			✓
Quarantine Policies	Policies that specify where quarantined files are stored on the client systems and how long they are kept.			✓
Quarantined Files	Collection of files on a client system that have been quarantined by Threat Prevention.			✓
Unwanted Programs	A list of undesirable programs to be detected on the client systems.			✓

Table 9 – Client Threat Prevention TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information)

1.7.7.3 Client Communications Protection TOE Data

TSF Data	Description	AD	UA	GE

TSF Data	Description	AD	UA	GE
Options Policies	Used to turn firewall protection on and off, enable Adaptive mode, and configure other Firewall options. Also used to create a list of domain names to block connections to the IP addresses resolving to those domain names.			✓
Rules	Firewall rules determine how to handle network traffic. Each rule provides a set of conditions that traffic must meet and an action to allow or block traffic.			✓
Rule Groups	A collection of firewall rules used to simplify management.			✓

Table 10 – Client Communications Protection TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information)

1.7.7.4 Client Web Protection TOE Data

TSF Data	Description	AD	UA	GE
Browser Activity	Collection of user browser events (including websites visited) on the managed systems.			✓
Options Policies	Used to configures general Web Control settings, which includes enabling, specifying action enforcement, Secure Search, event logging, web gateway settings, and email annotations.			✓
Safety Ratings	A color-coded safety rating button or icon indicating the level of trust of a specific website.			✓
Web Control Policies	Used to control user access to sites, pages, and downloads based on their safety rating or type of content. Sites may be blocked or allowed based on URLs and domains.			✓

Table 11 – Client Web Protection TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information)

1.8 Rationale for Non-bypassability and Separation of the TOE

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment. TOE components are software only products and therefore the non-bypassability and non-interference claims are dependent upon hardware and OS mechanisms. The TOE runs on top of the IT Environment supplied operating systems.

The TOE ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: the interfaces are well defined and insure that the access restrictions are enforced. Non-security relevant interfaces do not interact with the security functionality of the TOE. The TOE depends upon OS mechanisms to direct the system calls and network packets to the TOE for examination.

The TOE is implemented with well-defined interfaces that can be categorized as security relevant or non-security relevant. The TOE is implemented such that non-security relevant interfaces have no means of impacting the security functionality of the TOE. Unauthenticated users may not perform any actions within the TOE. The TOE tracks multiple users by sessions and ensures the access privileges of each are enforced.

The server hardware provides virtual memory and process separation, which the server OS utilizes to ensure that other (non-TOE) processes may not interfere with the TOE; all interactions are limited to the defined TOE interfaces. The OS and DBMS restrict access to TOE data in the database to prevent interference with the TOE via that mechanism.

The TOE consists of distributed components. Communication between the components relies upon cryptographic functionality provided by the TOE to protect the information exchanged from disclosure or modification.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 4 (September 2012) 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

The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

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

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

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

3.1 Threats

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

The following table identifies threats to the management system (ePO):

THREAT	DESCRIPTION
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data

Table 12 – Threats Addressed by the TOE and Operational Environment (Management System)

The following table identifies threats to the managed systems (user workstations) that may be indicative of vulnerabilities in or misuse of IT resources:

THREAT	DESCRIPTION
T.ASPOOF	An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising identification data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.

THREAT	DESCRIPTION
T.BADURL	The TOE may fail to identify an unsafe website or domain requested by the workstation user.
T.MALWARE	A malicious agent may attempt to introduce malware onto a workstation via network traffic or removable media to compromise data on that workstation, or use that workstation to attack additional systems.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE manages.

Table 13 – Threats Addressed by the TOE (Managed Systems)

3.2 Organizational Security Policies

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

POLICY	DESCRIPTION
P.ACCACT	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.MANSCAN	The authorized users of the workstations shall initiate manual anti-virus scans of removable media (e.g., floppy disks, CDs) introduced into the workstation before accessing any data on the removable media.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

Table 14 – Organizational Security Policies

3.3 Assumptions

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

ASSUMPTION	DESCRIPTION
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the number of IT Systems the TOE manages.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE manages.

ASSUMPTION	DESCRIPTION
A.GTI	Managed systems will securely download reputation values for URLs and domains and safety ratings for websites in real-time through the McAfee GTI service.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.SECDBASE	The external database will utilize SSL communication with the ePO server to protect system data.
A.SECMGMT	Management sessions will utilize HTTPS communication between the authorized administrator's web browser and the Epo web server to protect management session data.
A.SECUPDTE	Administrators will implement secure mechanisms for receiving and validating updated signature files from McAfee, and for distributing the updates to the central management systems.

Table 15 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
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.
O.MEDIAT	The TOE must mediate the flow of all information between client workstations and other users and/or IT entities located on internal and external networks governed by the TOE.
O.EXPORT	When any TOE component makes its data available to another TOE component, the TOE will ensure the confidentiality of the TOE data.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.MALWARE	The TOE will detect and take action against known malware introduced to the workstation via network traffic or removable media.

Table 16 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
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.GTI	Administrators shall ensure that managed systems receive reputation values for URLs and domains and safety ratings for websites from the McAfee GTI service in real-time via secure mechanisms.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.INTROP	The TOE is interoperable with the IT System it monitors.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

OBJECTIVE	DESCRIPTION
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data via mechanisms outside the TSC.
OE.SECURE_UPDATES	Enterprises using the TOE shall ensure that signature file updates are received from McAfee via secure mechanisms, the updates are validated before being used, and the updates are distributed to central management systems with the Enterprise via secure mechanisms.
OE.SECURE_STORAGE	The IT Environment will securely store TOE data in the external database and securely retrieve it when directed by the TOE.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE

Table 17 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

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

OBJECTIVE / THREAT / ASSUMPTION	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.MEDIAT	O.EXPORT	O.PROTCT	O.MALWARE	OE.AUDIT_PROTECTION	OE.CREDEN	OE.GTI	OE.INSTAL	OE.INTROP	OE.PERSON	OE.PHYCAL	OE.PROTECT	OE.SD_PROTECTION	OE.SECURE_UPDATES	OE.SECURE_STORAGE	OE.TIME
A.ACCESS													✓							
A.ASCOPE													✓							
A.DYNMIC													✓	✓						
A.GTI											✓									
A.LOCATE															✓					
A.MANAGE														✓						
A.NOEVIL										✓		✓			✓					
A.PROTCT															✓					
A.SECDBASE																	✓		✓	
A.SECMGMT																	✓			
A.SECUPDTE																		✓		
P.ACCACT		✓		✓																✓
P.ACCESS	✓			✓			✓		✓								✓			
P.INTGTY						✓	✓		✓							✓	✓		✓	
P.MANAGE	✓		✓				✓			✓		✓		✓						
P.MANSCAN			✓					✓												

OBJECTIVE / THREAT / ASSUMPTION	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.MEDIAT	O.EXPORT	O.PROTCT	O.MALWARE	OE.AUDIT_PROTECTION	OE.CREDEN	OE.GTI	OE.INSTAL	OE.INTROP	OE.PERSON	OE.PHYCAL	OE.PROTECT	OE.SD_PROTECTION	OE.SECURE_UPDATES	OE.SECURE_STORAGE	OE.TIME
P.PROTCT						✓									✓	✓			✓	
T.ASPOOF					✓															
T.BADURL					✓															
T.COMDIS	✓			✓		✓	✓									✓				
T.COMINT	✓			✓			✓									✓				
T.FACCNT	✓	✓		✓																
T.IMPCON	✓		✓	✓								✓								
T.LOSSOF	✓			✓			✓													
T.MALWARE								✓												
T.MEDIAT					✓															
T.PRIVIL	✓			✓			✓													
T.SCNVUL								✓												

Table 18 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

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

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions. The OE.INTROP objective ensures the TOE has the needed access.
A.ASCOPE	The TOE is appropriately scalable to the number of IT Systems the TOE manages. The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT Systems the TOE manages. The OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will be managed appropriately.
A.GTI	Managed systems will securely download reputation values for URLs and domains and safety ratings for websites in real-time through the McAfee GTI service. The OE.GTI objective ensures that managed systems receive reputation values for URLs and domains and safety ratings for websites from the McAfee GTI service in real-time via secure mechanisms.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The OE.PHYCAL objective provides for the physical protection of the TOE hardware and software.
A.SECDBASE	The external database will utilize SSL communication with the ePO server to protect system data. The OE.SECURE_STORAGE objective requires the IT Environment to provide secure storage and retrieval mechanisms for System data for use by the TOE. The OE.SD_PROTECTION objective provides for the capability to protect system data via mechanisms outside the TSC. The use of SSL communication between the external database and the ePO server is a mechanism outside the TSC.
A.SECMGMT	Management sessions will utilize HTTPS communication between the authorized administrator's web browser and the ePO web server to protect management session data. The OE.SD_PROTECTION objective provides for the capability to protect system data via mechanisms outside the TSC. The HTTPS implementation provided by the ePO web server and the administrator's web browser is a mechanism outside the TSC.
A.SECUPDTE	Administrators will implement secure mechanisms for receiving and validating updated signature files from McAfee, and for distributing the updates to the central management systems. The OE.SECURE_UPDATES objective ensures Administrators use secure mechanisms to receive and validate the updates from McAfee, then use secure mechanisms to distribute the updates to the central management systems.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.ACCACT	The authorized users of the TOE shall be accountable for their actions within the TOE. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The OE.TIME objective supports this policy by providing a time stamp for insertion into the audit records. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.AUDIT_PROTECTION and OE.SD_PROTECTION objectives counter this threat via IT Environment protections of the audit trail. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification. The OE.AUDIT_PROTECTION and OE.SD_PROTECTION objectives enforce this policy via IT Environment protections of the audit trail. The O.PROTCT objective addresses this policy by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment. The O.EXPORT objective requires the TOE to protect the data from unauthorized disclosure during transit. The OE.SECURE_STORAGE objective requires the IT Environment to provide secure storage and retrieval mechanisms for System data for use by the TOE.
P.MANAGE	The TOE shall only be managed by authorized users. The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.MANSCAN	The authorized users of the workstations shall initiate manual anti-virus scans of removable media (e.g., floppy disks, CDs) introduced into the workstation before accessing any data on the removable media. The O.MALWARE objective requires the TOE to provide the capability to perform manual scans of removable media. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product including allowing workstation users to invoke manual scans.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment. The O.EXPORT objective requires the TOE to protect the data from unauthorized disclosure during transit. The OE.SECURE_STORAGE objective requires the IT Environment to provide secure storage and retrieval mechanisms for System data for use by the TOE.
T.ASPOOF	An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising identification data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network. The O.MEDIAT objective ensures the TOE mediates the flow of all information between client workstations and other users and/or IT entities located on internal and external networks governed by the TOE.
T.BADURL	The TOE may fail to identify an unsafe website or domain requested by the workstation user. The O.MEDIAT objective ensures the TOE mediates the flow of all information between client workstations and other users and/or IT entities located on internal and external networks governed by the TOE.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected. The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.MALWARE	A malicious agent may attempt to introduce malware onto a workstation via network traffic or removable media to compromise data on that workstation, or use that workstation to attack additional systems. The O.MALWARE objective mitigates this threat by providing mechanisms to prevent malware from being introduced onto a workstation.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network. The O.MEDIAT objective ensures the TOE mediates the flow of all information between client workstations and other users and/or IT entities located on internal and external networks governed by the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE manages. The O.MALWARE objective counters this threat by requiring a TOE to detect and take action against known malware introduced to the workstation via network traffic or removable media.

Table 19 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Anti-Malware (FAM) Class of SFRs

All of the components in this section were originally based on the *U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments*, version 1.2, dated 25 July 2007.

This class of requirements was taken from the Anti-Virus PP to specifically address the detection and response capabilities of anti-virus products. The purpose of this class of requirements is to address the unique nature of anti-virus products and provide for requirements about detecting and responding to viruses on protected IT resources.

Functional components were modified to address unique functionality implemented by ENS, including:

- The term “virus” was replaced with “malware” throughout the requirements since the TOE can detect several types of malware, only one of which is a virus. As a consequence the class name was changed from FAV (Anti-Virus) to FAM (Anti-Malware).
- Requirement language in FAM_ACT_(EXT).1 Anti-Malware Actions was changed to reflect functionality that protects user workstations from access point violations, potentially unwanted code and programs, and buffer overflow exploits. These violations and exploits are all considered malware by this Security Target.
- The requirement to monitor SMTP sessions in in FAM_ACT_(EXT).1 Anti-Malware Actions was removed as information flow control policies are more appropriately handled by FDP_IFC.1 and FDP_IFF.1 in this Security Target.
- Requirement language in FAM_ALR_(EXT).1 Anti-Malware Alerts was changed to reflect how events are handled at the Administrator console.

5.1.1 FAM_ACT_(EXT).1 Anti-Malware Actions

Hierarchical to: No other components.

Dependencies: FAM_SCN_(EXT).1 Anti-Malware Scanning

FAM_ACT_(EXT).1.1 Upon detection of memory based malware, the TSF shall prevent the malware from further execution.

FAM_ACT_(EXT).1.2 Upon detection of file-based malware, the TSF shall perform the action(s) specified by the Administrator. Actions are administratively configurable on a per-workstation basis and consist of:

a) Clean the malware from the file,

b) Deny access to the file,

c) Quarantine the file,

d) Delete the file,

e) [selection: [assignment: list of other actions], no other actions].

FAM_ACT_(EXT).1.3 Upon detection of an access point violation, unwanted program, or buffer overflow, the TSF shall perform the action(s) specified by the Administrator. Actions are administratively configurable on a per-workstation basis and consist of:

a) Block the action,

b) Report the action,

c) [selection: [assignment: list of other actions], no other actions].

Application Note: An access point violation is defined as a user and/or process attempting to make unwanted changes to a managed system via its ports, files, shares, and registry and keys.

Management:

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

a) Configuration of the actions to be taken.

Audit:

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

a) Basic: Action taken in response to detection of a malware.

5.1.2 FAM_ALR_(EXT).1 Anti-Malware Alerts

Hierarchical to: No other components.

Dependencies: FAM_SCN_(EXT).1 Anti-Malware Scanning

FAM_ALR_(EXT).1.1 Upon detection of malware, the TSF shall display an alert on the screen of the workstations on which the malware is detected. The alert shall identify the malware that was detected and the action taken by the TOE.

FAM_ALR_(EXT).1.2 The TSF shall continue to display the alerts on the screen of the workstation until they are acknowledged by the user of the workstation, or the user session ends.

FAM_ALR_(EXT).1.3 Upon receipt of an audit event from a workstation indicating detection of malware, the TSF shall display an alert on the screen of the Administrator if a session is active. The alert shall identify the workstation originating the audit event, the malware that was detected, and the action taken by the TOE.

Management:

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

a) Configuration of the alerts to be generated.

Audit:

There are no auditable events foreseen.

5.1.3 FAM_SCN_(EXT).1 Anti-Malware Scanning

Hierarchical to: No other components.

Dependencies: None

FAM_SCN_(EXT).1.1 The TSF shall perform real-time scans for memory based malware based upon known signatures.

FAM_SCN_(EXT).1.2 The TSF shall perform real-time, scheduled, and on-demand scans for file-based malware based upon known signatures.

FAM_SCN_(EXT).1.3 The TSF shall perform scheduled scans at the time and frequency configured by the Administrator.

FAM_SCN_(EXT).1.4 The TSF shall perform manually invoked scans when directed by the Workstation User.

Management:

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

a) Configuration of scheduled scans.

b) Configuration of parameters for all types of scans.

Audit:

There are no auditable events foreseen.

5.2 Extended Component – Audit Data Generation

For this evaluation the FAU_GEN.1 Security Functional Requirement in CC Part 2 has been extended to cover part of the TOE functionality that is not fully supported.

One additional component has been defined. This has been placed in an existing Family GEN: Audit Data Generation within the Class FAU: Security Audit. This choice has been made as the new component is a minor modification to the implementation of security auditing already defined in CC Part 2.

Specifically, the TOE does not generate an audit record of the following auditable event: startup and shutdown of the audit functions. An extended component FAU_GEN_EXT.1 has been added to remove the auditing of TOE startup and shutdown events. All other security requirements from FAU_GEN.1 remain identical.

5.2.1 FAU_GEN_EXT.1 Audit Data Generation (Extended)

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable Time Stamps

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

a) All auditable events for the [selection, choose one of*: minimum, basic, detailed, not specified*] level of audit; and

b) [assignment: *other specifically defined auditable events*].

FAU_GEN_EXT.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, [assignment: *other audit relevant information*].

6 Security Requirements

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

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and the extended components defined in section 5 of this document, all of which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN_(EXT).1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
Anti-Malware	FAM_ACT_(EXT).1	Anti-Malware Actions
	FAM_ALR_(EXT).1	Anti-Malware Alerts
	FAM_SCN_(EXT).1	Anti-Malware Scanning
Cryptographic Support	FCS_CKM.1(1-4)	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
User Data Protection	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of Identification
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_ITT.1	TSF Data Transfer Protection

Table 20 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN_(EXT).1 Audit Data Generation (Extended)

FAU_GEN_(EXT).1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) All auditable events for the not specified level of audit; and

b) *The events identified in the following table*

FAU_GEN_(EXT).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, 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 the following table*.

Application Note: The auditable events for the respective level of auditing are included in the following table:

COMPONENT	EVENT	DETAILS
FAU_SAR.2	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.	None
FDP_IFF.1	All decisions on requests for information flow	The presumed addresses of the source and destination subject.
FAM_ACT_(EXT).1	Action taken in response to detection of a virus	Virus detected, action taken, file or process identifier where virus is detected
FIA_ATD.1	All changes to TSF data (including passwords) result in an audit record being generated.	None
FIA_UAU. 1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	None
FMT_MTD.1	All modifications to the values of TSF data	None
FMT_SMF.1	Use of the management functions.	User identity, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 21 – Audit Events and Details

6.1.1.2 FAU_GEN.2 User Identity Association

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

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *users with the "View audit log" or "View and purge audit log" permission or Administrators* 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.

6.1.2 Anti-Malware (Explicitly Stated)

6.1.2.1 FAM_ACT_(EXT).1 Anti-Malware Actions

FAM_ACT_(EXT).1.1 Upon detection of memory based malware, the TSF shall prevent the malware from further execution.

FAM_ACT_(EXT).1.2 Upon detection of file-based malware, the TSF shall perform the action(s) specified by the Administrator. Actions are administratively configurable on a per-workstation basis and consist of:

a. Clean the malware from the file,

b. Deny access to the file,

c. Quarantine the file,

d. Delete the file,

e. No other actions.

FAM_ACT_(EXT).1.3 Upon detection of an access point violation, unwanted program, or buffer overflow, the TSF shall perform the action(s) specified by the Administrator. Actions are administratively configurable on a per-workstation basis and consist of:

a) Block the action,

b) Report the action,

c) No other actions.

Application Note: An access point violation is defined as a user and/or process attempting to make unwanted changes to a managed system via its ports, files, shares, and registry and keys.

Application Note: The Administrator in this context are users with the Endpoint Security Threat Prevention Policy "View and change settings" permission and/or the Endpoint Security Threat Prevention Tasks "View and change settings" permission.

6.1.2.2 FAM_ALR_(EXT).1 Anti-Malware Alerts

FAM_ALR_(EXT).1.1 Upon detection of malware, the TSF shall display an alert on the screen of the workstations on which the malware is detected. The alert shall identify the malware that was detected and the action taken by the TOE.

FAM_ALR_(EXT).1.2 The TSF shall continue to display the alerts on the screen of the workstation until they are acknowledged by the user of the workstation, or the user session ends.

FAM_ALR_(EXT).1.3 Upon receipt of an audit event from a workstation indicating detection of a malware, the TSF shall display an alert on the screen of the Administrator if a session is active. The alert shall identify the workstation originating the audit event, the malware that was detected, and the action taken by the TOE.

Application Note: Alerts are displayed in the Threat Event Log on the ePO management server.

Application Note: The Administrator in this context are users with the Endpoint Security Threat Prevention Policy "View and change settings" permission and/or the Endpoint Security Threat Prevention Tasks "View and change settings" permission.

6.1.2.3 FAM_SCN_(EXT).1 Anti-Malware Scanning

FAM_SCN_(EXT).1.1 The TSF shall perform real-time scans for memory based malware based upon known signatures.

FAM_SCN_(EXT).1.2 The TSF shall perform real-time, scheduled, and on-demand scans for file-based malware based upon known signatures.

FAM_SCN_(EXT).1.3 The TSF shall perform scheduled scans at the time and frequency configured by the Administrator.

FAM_SCN_(EXT).1.4 The TSF shall perform manually invoked scans when directed by the Workstation User.

Application Note: The Administrator in this context are users with the Endpoint Security Threat Prevention Policy "View and change settings" permission and/or the Endpoint Security Threat Prevention Tasks "View and change settings" permission. A Workstation user refers to a user on a managed client system who are able to execute "on-demand" scans of files on their workstations.

6.1.3 Cryptographic Support (FCS)

6.1.3.1 FCS_CKM.1(1) Cryptographic Key Generation (ePO AES)

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*PRNG for random number generation*] and specified cryptographic key sizes [*256 bits for encryption/decryption*] that meet the following: [*ANSI X9.31 Appendix A.2.4 (CAVP algorithm certificate #1053)*].

6.1.3.2 FCS_CKM.1(2) Cryptographic Key Generation (ePO RSA)

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*PRNG for random number generation*] and specified cryptographic key sizes [*2048 bits for key transport*] that meet the following: [*ANSI X9.31 Appendix A.2.4 (CAVP algorithm certificate #1053)*].

6.1.3.3 FCS_CKM.1(3) Cryptographic Key Generation (MA AES)

FCS_CKM.1.1(3) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*HMAC_DRBG for random number generation*] and specified cryptographic key sizes [*256 bits for encryption/decryption*] that meet the following: [*NIST Special Publication 800-90A (CAVP algorithm certificate #191)*].

6.1.3.4 FCS_CKM.1(4) Cryptographic Key Generation (MA RSA)

FCS_CKM.1.1(4) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*HMAC_DRBG for random number generation*] and specified cryptographic key sizes [*2048 bits for key transport*] that meet the following: [*NIST Special Publication 800-90A (CAVP algorithm certificate #191)*].

6.1.3.5 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 requirements for key zeroization*].

6.1.3.6 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [*the operations described below*] in accordance with a specified cryptographic algorithm [*multiple algorithms as described below*] and cryptographic key sizes [*multiple key sizes described below*] that meet the following: [*multiple standards described below*].

Table 22 – Cryptographic Operations

OPERATION	ALGORITHM	KEY SIZE IN BITS	STANDARDS
Key Transport	RSA encrypt/decrypt	2048	Allowed in FIPS mode
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (operating in CBC mode)	256	FIPS 197(CAVP algorithm certificates #2929 for ePO and #2017 for MA)
Secure Hashing	SHA-256	Not Applicable	FIPS 180-3 (CAVP algorithm certificates #2465 for ePO and #1767 for MA)

6.1.4 Information Flow Control (FDP)

Requirements Overview: This Security Target consists of a single information flow control Security Function Policy (SFP) called the *CLIENT COMMUNICATIONS PROTECTION SFP*. The subjects under control of this policy are human users or IT entities on a TOE Interface sending information through the TOE to external IT entities. The information flowing between subjects in the policy is traffic with attributes, defined in FDP_IFF.1.1, including source and destination addresses. Destination addresses include IP addresses, URLs and domain names. The rules that define the information flow control SFP are found in FDP_IFF.1.2.

6.1.4.1 FDP_IFC.1 – Subset information flow control

Application Note: This policy is called the CLIENT COMMUNICATIONS PROTECTION SFP. The subjects under control of this policy are human users or IT entities on a TOE Interface sending information through the TOE to external IT entities. It is enforced by both the ENS Firewall and Web Control modules.

FDP_IFC.1.1 The TSF shall enforce the *CLIENT COMMUNICATIONS PROTECTION SFP* on:

a) subjects: unauthenticated human users or external IT entities that send and receive information through the TOE to one another;

b) information: traffic sent through the TOE from one subject to another;

c) operation: pass information.

6.1.4.2 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the *CLIENT COMMUNICATIONS PROTECTION SFP* based on **at least** the following types of subject and information security attributes:

a) subject security attributes:

- *presumed address;*
- *no other subject security attributes*

b) information security attributes:

- *presumed address of source subject;*
- *presumed address of destination subject;*
- *network layer protocol;*
- *transport layer protocol;*
- *TOE interface (network connection type) on which traffic arrives and departs;*
- *application information (if applicable);*
- *GTI reputation value (if applicable);*
- *GTI safety rating value (if applicable);*
- *no other information security attributes.*

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

a) When a rule in the rule's group matches the information security attribute values and the action value for the matched rule is "allow". The rules may be composed from all possible combinations of the values of the information security attributes, created by the authorized administrator.

FDP_IFF.1.3 The TSF shall enforce the *none.*

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules:

a) The TOE shall accept requests in which the subject specifies an IP address, URL, or domain name if the McAfee GTI reputation value is "do not block", and any other GTI reputation values allowed by the authorized administrator; and

b) *The TOE shall accept requests in which the subject specifies the URL or domain name if the McAfee GTI safety rating is "green", and any other GTI safety ratings allowed by the authorized administrator.*

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

a) When a rule in the rule's group matches the information security attribute values and the action value for the matched rule is "block". The rules may be composed from all possible combinations of the values of the information security attributes, created by the authorized administrator.

b) The TOE shall reject requests in which the subject specifies an IP address, URL, or domain name if the McAfee GTI reputation value is "High Risk", and any other GTI reputation values disallowed by the authorized administrator; and

c) *The TOE shall reject requests in which the subject specifies the URL or domain name if the McAfee GTI safety rating is "red", and any other GTI safety ratings disallowed by the authorized administrator.*

Application Note: The term "TOE interface" in the context of this TOE refers to the network connection type on the client workstation which may be one or more wired, wireless or virtual connections.

6.1.5 Identification and Authentication (FIA)

6.1.5.1 FIA_ATD.1 User Attribute Definition

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

a) Username;

b) Logon Status (enabled or disabled);

c) Authentication Configuration (must be configured for ePO);

d) Password;

e) Assigned Permissions; and

f) Assigned Role.

Application Note: The TOE maintains security attributes for ePO users. Windows maintains security attributes for Workstation Users and Network Users.

6.1.5.2 FIA_UAU.1 Timing of authentication

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

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

6.1.5.3 FIA_UID.1 Timing of Identification

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

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

6.1.6 Security Management (FMT)

6.1.6.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions *as identified in the following table* to *a user with the permissions identified in the following table, or an Administrator*.

TSF Function(s)	Associated Permission
Client Threat Prevention	Endpoint Security Common: Policy and Tasks "View and change policy and task settings"
	Endpoint Security Threat Prevention: Policy "View and change settings"
	Endpoint Security Threat Prevention: Tasks "View and change settings"
Client Communications Protection	Endpoint Security Common: Policy and Tasks "View and change policy and task settings"
	Endpoint Security Firewall: Firewall "View and change policy and task settings"
Client Web Protection	Endpoint Security Common: Policy and Tasks "View and change policy and task settings"
	Endpoint Security Web Control: Policy "View and change settings"
	Endpoint Security Web Control: Tasks "View and change settings"

Table 23 – Management of TSF Behavior and Associated Permissions

6.1.6.1 FMT_MSA.3 – Static attribute initialization

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

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

Application Note: The default values for the information flow control security attributes appearing in FDP_IFF.1 are intended to be restrictive in the sense that both inbound and outbound information is denied by the TOE until the default values are modified by an authorized administrator.

6.1.6.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, *create and use* the *TSF data identified in the following table* to *a user with the permissions identified in the following tables, or an Administrator*.

TSF Data	Associated Permission	Operations Permitted
Audit Log	View audit log	Query
	View and purge audit log	Query and delete
Dashboards	Use public dashboards	Query and use public dashboards
	Use public dashboards; create and edit private dashboards	Query and use public dashboards; create and modify private dashboards
	Use public dashboards; create and edit private dashboards; make private dashboards public	Query and use public dashboards; create, delete and modify private dashboards
ePO User Accounts	n/a (only allowed by an Administrator)	Query, create, delete and modify
Groups	"Edit System Tree groups and systems"	Query, create, delete and modify
Permission	n/a (only allowed by an Administrator)	Query
Permission Set	n/a (only allowed by an Administrator)	Query, create, delete, modify
Queries and Reports	Use public groups (queries)	Query and use public groups (queries)
	Use public groups; create and edit private queries/reports	Query and use public queries/reports; 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 queries/reports; create, delete and modify (including make public) private queries/reports
Server Settings	Rogue System Detection "View Rogue System Information"	Query
	Rogue System Detection "Create and edit Rogue System Information; manage Rogue Sensors", "Create and edit Rogue System Information; manage Rogue Sensors; Deploy Agents and Add to System Tree"	Query, create, delete and modify
	Software "View packages", "View repositories"	Query
	Software "Add, remove, and change packages; perform pull tasks", "Add, remove, and change repositories; perform replication tasks"	Query, create, delete and modify

TSF Data	Associated Permission	Operations Permitted
	Systems "Edit System Tree groups and systems" with "Deploy agents" selected	Query and modify
System Information	Access to the specific group node in the tree	Query
	"View System Tree tab", access to the specific group node in the tree, and "Edit System Tree groups and systems"	Query, create, delete and modify
System Tree	"View System Tree tab" and access to the specific group node in the tree	Query
	"View System Tree tab", access to the specific group node in the tree, and "Edit System Tree groups and systems"	Query, create, delete and modify
Threat Event Log	View events	Query
	View, delete and purge events	Query and delete
User Interface Policies	ENS Common Policy and Tasks: View policy and task settings	Query
	ENS Common Policy and Tasks: View and change policy and task settings	Query, create, delete and modify

Table 24 - TSF Data Access Permissions for ePO TOE Data

TSF Data	Associated Permission	Operations Permitted
Access Protection Policies	ENS Threat Prevention Policy: View settings	Query
	ENS Threat Prevention Policy: View and change settings	Query, create, delete and modify
AMCore	N/A – content file is a system file	N/A
Application Protection Lists	ENS Threat Prevention Policy: View settings	Query
	ENS Threat Prevention Policy: View and change settings	Query, create, delete and modify
Extra.DAT files	N/A – content file is a system file	N/A
Exclusions	ENS Threat Prevention Policy: View settings	Query
	ENS Threat Prevention Policy: View and change settings	Query, create, delete and modify
Exploit Prevention Content	N/A – content file is a system file	N/A
Exploit Prevention Policies	ENS Threat Prevention Policy: View settings	Query
	ENS Threat Prevention Policy: View and change settings	Query, create, delete and modify

TSF Data	Associated Permission	Operations Permitted
On-Access Scan Policies	ENS Threat Prevention Policy: View settings	Query
	ENS Threat Prevention Policy: View and change settings	Query, create, delete and modify
On-Demand Scan Policies	ENS Threat Prevention Policy: View settings	Query
	ENS Threat Prevention Policy: View and change settings	Query, create, delete and modify
On-Demand Scan Tasks	ENS Threat Prevention Tasks: View settings	Query
	ENS Threat Prevention Tasks: View and change settings	Query, create, delete and modify
Options Policies	ENS Threat Prevention Policy: View settings	Query
	ENS Threat Prevention Policy: View and change settings	Query, create, delete and modify
Quarantine Policies	ENS Threat Prevention Policy: View settings	Query
	ENS Threat Prevention Policy: View and change settings	Query, create, delete and modify
Quarantined Files	N/A – action associated with quarantined files is determined by the Quarantine Policy. Workstation users can access their quarantined files.	N/A
Unwanted Programs	ENS Threat Prevention Policy: View settings	Query
	ENS Threat Prevention Policy: View and change settings	Query, create, delete and modify

Table 25 - TSF Data Access Permissions for Client Threat Prevention

TSF Data	Associated Permission	Operations Permitted
Options Policies	ENS Firewall: View policy and task settings	Query
	ENS Firewall: View and change policy and task settings	Query, create, delete and modify
Rules	ENS Firewall: View policy and task settings	Query
	ENS Firewall: View and change policy and task settings	Query, create, delete and modify
Rule Groups	ENS Firewall: View policy and task settings	Query
	ENS Firewall: View and change policy and task settings	Query, create, delete and modify

Table 26 - TSF Data Access Permissions for Client Communications Protection

TSF Data	Associated Permission	Operations Permitted

TSF Data	Associated Permission	Operations Permitted
Browser Activity	N/A – permissions for Browser Activity as per Queries and Reports permission (ePO)	N/A
Options Policies	ENS Web Control Policy: View settings	Query
	ENS Web Control Policy: View and change settings	Query, create, delete and modify
Safety Ratings	ENS Web Control Policy: View settings	Query
	ENS Web Control Policy: View and change settings	Query, create, delete and modify
Web Control Policies	ENS Web Control Policy: View settings	Query
	ENS Web Control Policy: View and change settings	Query, create, delete and modify

Table 27 - TSF Data Access Permissions for Client Web Protection

6.1.6.3 FMT_SMF.1 Specification of Management Functions

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

a) User Account management,

b) Permission Set management,

c) Audit Log management,

d) Event Log management,

e) System Tree management,

f) Query management,

g) Dashboard management,

h) Endpoint Security Common Module management,

i) Client Threat Prevention Policy management,

j) Client Communications Protection Policy management, and

k) Client Web Protection Policy Management.

6.1.6.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles ePO *Administrator and ePO User assigned to a permission set comprised of any of the following permissions*:

a) View audit log

b) View and purge audit log

c) Edit public queries; create and edit private queries; make private queries public

d) Edit System Tree groups and systems

e) *ENS Common Policy and Tasks: View policy and task settings*

f) *ENS Common Policy and Tasks: View and change policy and task settings*

g) *ENS Threat Prevention Policy/Tasks: View settings*

h) *ENS Threat Prevention Policy/Tasks: View and change settings*

i) *ENS Firewall View policy and task settings*

j) *ENS Firewall View and change policy and task settings*

k) *ENS Web Control Policy: View settings*

l) *ENS Web Control Policy: View and change settings*

m) *System permissions (to specific nodes)*

n) *Use public dashboards*

o) *Use public dashboards; create and edit private dashboards*

p) *Use public dashboards; create and edit private dashboards; make private dashboards public*

q) *Use public queries*

r) *Use public queries; create and edit private queries*

s) *View System Tree tab*

t) View events

u) View, delete and purge events.

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

Application Note: An ePO Administrator is a user account assigned to the built-in Global Administrator permission set. Users are defined ePO user accounts without Administrator permission set but with other specific permission sets.

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

6.1.7 Protection of the TSF (FPT)

6.1.7.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

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

Application Note: FPT_ITT.1 only applies to the transmission of TSF data between the McAfee Agent (installed on the managed client systems) and the ePO server. The protection of TSF data transmitted between the administrator's web browser and the ePO server has been excluded from the evaluation. Additionally, the protection of data transmitted between the ePO server and the external database has also been excluded from the evaluation.

6.2 Security Assurance Requirements

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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
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 28 – Security Assurance Requirements at EAL2

6.3 CC Component Hierarchies and Dependencies

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

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN_(EXT).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 by FAU_GEN_(EXT).1 Satisfied
FAU_SAR.1	No other components	FAU_GEN_(EXT).1	Satisfied by FAU_GEN_EXT.1
FAU_SAR.2	No other components	FAU_SAR.1	Satisfied
FAM_ACT_(EXT).1	No other components	FAM_SCN_(EXT).1	Satisfied
FAM_ALR_(EXT).1	No other components	FAM_SCN_(EXT).1	Satisfied
FAM_SCN_(EXT).1	No other components	None	N/A
FCS_CKM.1(1-4)	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_IDC.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_IDC.2 or FCS_CKM.1 FCS_CKM.4	Satisfied by FCS_CKM.1 and FCS_CKM.4
FDP_IFC.1	No other components	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components	FDP_IFC.1 FMT_MSA.3	Satisfied Satisfied
FIA_ATD.1	No other components	None	N/A
FIA_UAU.1	No other components	FIA_UID.1	Satisfied
FIA_UID.1	No other components	None	N/A
FMT_MOF.1	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_MSA.3	No other components	FMT_MSA.1 FMT_SMR.1	^See note below 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
FPT_ITT.1	No other components	None	N/A

Table 29 – TOE SFR Dependency Rationale

^ The management of security attributes (as required by FMT_MSA.1) for the CLIENT COMMUNICATIONS PROTECTION SFP has been adequately satisfied by FMT_MOF.1 Management of Security Functions Behavior and FMT_MTD.1 Management of TSF Data. Both of these SFRs stipulate the required permissions to alter the TSF functions and data which is needed to manage the security attributes for the CLIENT COMMUNICATIONS PROTECTION SFP.

6.4 Security Requirements Rationale

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

6.4.1 Security Functional Requirements for the TOE

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

OBJECTIVE / SFR	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.MEDIAT	O.EXPORT	O.PROTCT	O.MALWARE
FAU_GEN_(EXT).1		✓						

OBJECTIVE / SFR	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.MEDIAT	O.EXPORT	O.PROTCT	O.MALWARE
FAU_GEN.2		✓						
FAU_SAR 1	✓		✓					
FAU_SAR.2	✓			✓				
FAM_ACT_(EXT).1								✓
FAM_ALR_(EXT).1								✓
FAM_SCN_(EXT).1								✓
FCS_CKM.1(1-4)						✓		
FCS_CKM.4						✓		
FCS_COP.1						✓		
FDP_IFC.1					✓			
FDP_IFF.1					✓			
FIA_ATD.1				✓				
FIA_UAU.1	✓			✓				
FIA_UID.1	✓			✓				
FMT_MOF.1	✓			✓			✓	
FMT_MSA.3			✓		✓			
FMT_MTD.1	✓		✓	✓			✓	
FMT_SMF.1	✓		✓					
FMT_SMR.1	✓		✓	✓				
FPT_ITT.1						✓		

Table 30 – Mapping of TOE SFRs to Security Objectives

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

OBJECTIVE	RATIONALE
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. Users authorized to access the TOE are determined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. The permitted access to TOE data by the roles and permissions is defined [FMT_MTD.1, FMT_SMF.1, FMT_SMR.1]. The audit log records may only be viewed by authorized users [FAU_SAR.1, FAU_SAR.2].
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions. Security-relevant events must be defined and auditable for the TOE [FAU_GEN_(EXT).1]. The user associated with the events must be recorded [FAU_GEN.2].

OBJECTIVE	RATIONALE
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1]. The functions and roles required for effective management are defined [FMT_SMF.1, FMT_SMR.1], and the specific access privileges for the roles and permissions is enforced [FMT_MTD.1]. The TOE must allow the Administrator to specify alternative initial values to override the default values [FMT_MSA.3].
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1].
O.MEDIAT	The TOE must mediate the flow of all information between client workstations and other users and/or IT entities located on internal and external networks governed by the TOE. The TOE will identify the entities involved in the CLIENT COMMUNICATIONS PROTECTION SFP (i.e., users and/or IT entities sending information to other users and/or IT entities and vice versa) [FDP_IFC.1]. The TOE will identify the attributes of the users sending and receiving the information in the CLIENT COMMUNICATIONS PROTECTION SFP, as well as the attributes for the information itself. Policy is defined by stating under what conditions information is permitted to flow [FDP_IFF.1]. The TOE will ensure that there is a default deny policy for the information flow control security rules [FMT_MSA.3].
O.EXPORT	When any TOE component makes its data available to another TOE component, the TOE will ensure the confidentiality of the TOE data. The TOE must protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE [FPT_ITT.1]. The TOE ensures the confidentiality of system data through the implementation of encrypted communications [FCS_CKM.1(1-4), FCS_CKM.4, FCS_COP.1] between TOE components.

OBJECTIVE	RATIONALE
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].
O.MALWARE	The TOE will detect and take action against known malware introduced to the workstation via network traffic or removable media. The TOE is required to scan the user's workstation and all system data for malware [FAM_SCN_(EXT).1]. The TOE will take action against detected malware [FAM_ACT_(EXT).1]. The TOE will alert workstation users and authorized administrators when malware is detected [FAM_ALR_(EXT).1].

Table 31 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Assurance Requirements

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

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: McAfee Endpoint Security 10.1.0 with ePolicy Orchestrator 5.3.1, Version 1.1
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee Endpoint Security 10.1.0 with ePolicy Orchestrator 5.3.1, Version 1.1
ADV_TDS.1: Basic Design	Basic Design: McAfee Endpoint Security 10.1.0 with ePolicy Orchestrator 5.3.1, Version 1.1
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2, Version 1.3
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2, Version 1.3
ALC_CMC.2: Use of a CM System	McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2 Configuration Management Plan, Version 1.4
ALC_CMS.2: Parts of the TOE CM Coverage	McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2 Configuration Management Plan, Version 1.4
ALC_DEL.1: Delivery Procedures	McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2 Software Delivery Process, Version 1.2
ALC_FLR.2: Flaw Reporting Procedures	Flaw Remediation McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2, Version 1.3
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2, Version 1.3

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ATE_FUN.1: Functional Testing	Security Testing: McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2, Version 1.3
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2, Version 1.3

Table 32 – Security Assurance Rationale and Measures

6.4.2.1 Rationale for TOE Assurance Requirements Selection

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

The general level of assurance for the TOE is:

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

6.5 TOE Summary Specification Rationale

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

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

TSF / SFR	Client Threat Prevention	Client Communications Protection	Client Web Protection	Identification & Authentication	Management	Audit	Protected System Data Transfer
FAU_GEN_(EXT).1						✓	
FAU_GEN.2						✓	
FAU_SAR.1						✓	
FAU_SAR.2						✓	
FAM_ACT_(EXT).1	✓	✓					
FAM_ALR_(EXT).1	✓						

SFR \ TSF	Client Threat Prevention	Client Communications Protection	Client Web Protection	Identification & Authentication	Management	Audit	Protected System Data Transfer
FAM_SCN_(EXT).1	✓						
FCS_CKM.1(1-4)							✓
FCS_CKM.4							✓
FCS_COP.1							✓
FDP_IFC.1		✓	✓				
FDP_IFF.1		✓	✓				
FIA_ATD.1					✓		
FIA_UAU.1				✓			
FIA_UID.1				✓			
FMT_MOF.1					✓		
FMT_MSA.3		✓			✓		
FMT_MTD.1					✓		
FMT_SMF.1					✓		
FMT_SMR.1					✓		
FPT_ITT.1							✓

Table 33 – SFR to TOE Security Functions Mapping

SFR	SF AND RATIONALE
FAU_GEN_(EXT).1	**Audit –** User actions are audited according to the events specified in the table with the SFR.
FAU_GEN.2	**Audit –** The audit log records include the associated user name when applicable.
FAU_SAR.1	**Audit –** Audit log records are displayed in a human readable table form from queries generated by authorized users.
FAU_SAR.2	**Audit** – Only authorized users have permission to query audit log records.
FAM_ACT_(EXT).1	**Client Threat Prevention** – The TOE detects memory and file-based malware and prevents them from executing on managed systems. Actions are configured by the Administrator to clean, quarantine or delete file-based malware. **Client Communications Protection** - The TOE will monitor SMTP communications and block traffic from unauthorized processes, while permitting authorized traffic (via the ENS Firewall).
FAM_ALR_(EXT).1	**Client Threat Prevention** – The TOE provides alert notification of detected malware to the workstation user and sends an event to the ePO server managed by the Administrator.

SFR	SF AND RATIONALE
FAM_SCN_(EXT).1	**Client Threat Prevention** – The TOE provides real-time (on-access) and scheduled (on-demand) malware scanning of the workstation memory space and files against known signatures. On-demand scans are scheduled by the Administrator or may be invoked manually by the workstation user.
FCS_CKM.1(1-4)	**Protected System Data Transfer** – The TOE provides secure communications between the ePO server and the McAfee Agent, in part, through the generation of cryptographic keys used to establish encrypted sessions for the safe passage of TSF data.
FCS_CKM.4	**Protected System Data Transfer** – The TOE provides secure communications between the ePO server and the McAfee Agent, in part, through the secure destruction of cryptographic keys used to establish encrypted sessions for the safe passage of TSF data.
FCS_COP.1	**Protected System Data Transfer** – The TOE provides secure communications between the ePO server and the McAfee Agent which allow the safe passage of TSF data between TOE components.
FDP_IFC.1	**Client Communications Protection** - The TSF mediates all communication flows through the ENS Firewall module. It controls traffic flows from users and/or IT entities. **Client Web Protection** - The TSF mediates all requests for URL and domains through the ENS Web Control module. It controls web traffic flows requested by workstation users.
FDP_IFF.1	**Client Communications Protection** - The TSF mediates all communication flows through the ENS Firewall module. It controls traffic flows from users and/or IT entities. **Client Web Protection** - The TSF mediates all requests for URL and domains through the ENS Web Control module. It controls web traffic flows requested by workstation users.
FIA_ATD.1	**Management –** User security attributes are associated with the user account via User Account management.
FIA_UAU.1	**Identification & Authentication -** The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FIA_UID.1	**Identification & Authentication -** The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FMT_MOF.1	**Management** – Authorized system administrators modify the behaviour of the Client Threat Prevention, Client Communications Protection, and Client Web Protection security functions by configuring the policies and tasks for the managed systems.

SFR	SF AND RATIONALE
FMT_MSA.3	**Client Communications Protection** – The TSF implements a default deny policy for the information flow control security rules. **Management** - The TOE must allow the Administrator to specify alternative initial values to override the default values
FMT_MTD.1	**Management** – The permissions assigned to users determine the access privileges of the user to TOE data. Administrators have full access to TOE data.
FMT_SMF.1	**Management** – The TOE provides the management functions specified in FMT_SMF.1.
FMT_SMR.1	**Management** – The TOE provides appropriate permissions for the role of Administrator and users assigned any of the permissions listed in FMT_SMR.1.
FPT_ITT.1	**Protected System Data Transfer** – The TOE encrypts all communication sessions between the McAfee Agent and the ePO server protecting TSF data from unauthorized disclosure and unauthorized modification.

Table 34 – SFR to TSF Rationale

7 TOE Summary Specification

7.1 Client Threat Prevention

The TOE checks for malware (including viruses, trojan horses, adware, spyware, keyloggers, unwanted programs, etc), and other threats by scanning items (such as files, the registry and processes (programs) resident in memory) automatically when users access them or on demand. The TOE detects and reports (alerts) on threats, then takes the actions that have been configured to protect systems. Actions for detected malware include automatic quarantine, cleaning, and deletion from the affected system. This functionality is provided by the Threat Prevention module in the ENS Client.

Scans are configured as either “on-access” or “on-demand”:

- **On-access scan** - the administrator configures on-access scans to run on managed systems. Whenever files, folders, and programs are accessed the on-access scanner intercepts the operation and scans the item, based on criteria defined by the administrator. On-access scans are configured via the On-Access Scan policy settings.
- **On-demand scan** - one of two types of on-demand scans:
    - Manual scans: the administrator configures predefined on-demand scans that users can run on managed systems. The user runs the scan from the ENS Client and selecting a quick scan or full scan. Alternatively, the scan may be executed by right-clicking the file or folder. Specific behavior of all these user scan types can be configured by the administrator.
    - Scheduled scans: The administrator configures and schedules on-demand scans to run on managed systems at a scheduled time, or at system startup. When a scheduled on-demand scan is about to start, the ENS Client displays a scan prompt at the bottom of the screen. On-demand scans are scheduled via the client task settings either as a Custom On-Demand Scan or Policy-Based On-Demand Scan.

Either scan type will deliver notifications to the user and ePO management server when detections occur. Files must meet predefined criteria to indicate a potential threat. Suspected threats are then compared against signatures from the AMCore file for a possible match. The AMCore file is periodically updated by secure mechanisms provided by the IT environment.

The TOE provides malware detection based on the settings that have been configured. The settings can be configured for all processes, or based on whether a process is classified as having a low-risk or high-risk of infection. Scanning occurs when files are either read from, or written to the computer the ENS Client is installed on. The TOE protects user workstations from the following types of malware:

- Viruses (including worms, trojan horses, etc)

- Access point violations
- Potentially unwanted code and programs (e.g. spyware, keyloggers, adware, dialers, etc)
- Buffer overflow exploits

7.1.1 Viruses

When a detection occurs, the TOE takes certain actions depending on what has been configured. There are Primary (First Response) and Secondary actions that the TOE takes when a detection occurs. The primary actions that the TOE takes when a detection occurs:

- Cleaning of files automatically (after quarantining the original)
- Denying access to infected files
- Move infected files to a quarantine folder in email scanning. For stored files, the file is quarantined off-host before being deleted

Secondary actions are actions that the TOE takes if the Primary action fails. Secondary actions that the TOE takes on discovery of a detection include:

- Move infected files to a quarantine folder
- Denying access to infected files (quarantine)
- Delete infected files automatically

When a virus is detected (e.g. an infection occurs) the On-Access Scan Messages box pops up and remains on the screen until the user session ends, or until the alert is acknowledged. Security audit events are also sent to ePO, where they are saved in the Threat Event Log and reviewed via the same mechanism used for audit events (refer to section 7.6). Each audit event includes a timestamp, the type of event, and client identity. Event data is sent via the McAfee Agent which is protected in accordance with Protected System Data Transfer discussed in section 7.7.

7.1.2 Access Point Violations

The TOE prevents unwanted changes to managed systems by restricting access to specified ports, files, shares, and registry and keys. Access Protection uses rules to report or block access to items. The on-access scanner compares a requested action against the list of rules and takes the action specified by the rule. Actions may be initiated by macros, executable files, scripts, Internet Relay Chat (IRC) messages, browser and application help files, and email messages.

Threat Prevention follows this basic process to provide Access Protection when a threat occurs:

1. Access Protection examines the action according to the defined rules, including:

a. Blocking the action

b. Reporting the action

2. If the action breaks a rule, Access Protection manages the action using the information in the configured rules.

3. Access Protection generates and sends an event to ePO management server

7.1.3 Potentially Unwanted Code and Programs

The TOE protects managed systems from potentially unwanted programs that are annoying or can alter the security state or the privacy policy of managed systems. Potentially unwanted programs can be embedded in programs that users download intentionally. Unwanted programs might include spyware, adware, and dialers.

The administrator specifies custom unwanted programs for the on-access and on-demand scanners to detect in the Options policy settings. Unwanted program detection and specific actions to take when detections occur are then enabled in the On-Access Scan policy settings and On-Demand Scan policy settings.

7.1.4 Buffer Overflow Exploits

Exploit Prevention stops exploited buffer overflows from executing arbitrary code. This feature monitors user-mode API calls and recognizes when they are called as a result of a buffer overflow. When a detection occurs, information is displayed on the client system, and sent to the ePO management server. Exploit Prevention protects applications such as Internet Explorer, Microsoft Outlook, Outlook Express, Microsoft Word, and MSN Messenger. Exploit Prevention settings can be enabled or disabled by the administrator on a per policy basis.

7.2 Client Communications Protection

The TOE implements a firewall that scans all incoming and outgoing traffic on managed systems (i.e. clients). As it reviews arriving or departing traffic, the Firewall checks its list of rules, which is a set of criteria with associated actions. If the traffic matches all criteria in a rule, the Firewall acts according to the rule, blocking or allowing traffic through the Firewall. This functionality is provided by the Firewall module in the ENS Client.

The administrator can define rules broadly (e.g., all IP traffic) or narrowly (e.g., identifying a specific application or service) based on the following parameters:

- Rule name
- Status – either enabled or disabled

- Actions – either Allow or block the traffic. Additional options include treating a match as an intrusion and log matching traffic.
- Direction – in, out, or bidirectional
- Network –can be any protocol, IP protocol or a non-IP protocol.
- Connection – can be wired, wireless and/or virtual.
- Transport – can be any transport-layer protocol including ICMP, TCP and UDP.
- Application – any application as identified by its executable filename.

The Firewall uses precedence to apply rules:

1. Firewall applies the rule at the top of the firewall rules list. If the traffic meets this rule's conditions, Firewall allows or blocks the traffic. It doesn't try to apply any other rules in the list.
2. If the traffic doesn't meet the first rule's conditions, Firewall continues to the next rule in the list until it finds a rule that the traffic matches.
3. If no rule matches, the firewall automatically blocks the traffic.

The administrator can group rules according to a work function, service, or application for easier management. The Firewall enables you to make a group of rules location-aware and create connection isolation. This is accomplished by configuring the rule group to be network adapter-aware so that adapter-specific rules can be applied to user workstations with multiple network adapters. Connection isolation prevents undesirable traffic from accessing a designated network.

Firewall Option settings enable the administrator to also block incoming and outgoing traffic from a network connection that McAfee Global Threat Intelligence (GTI)[4] rates as high risk. Values for the incoming and outgoing network reputation threshold can be specified by the administrator under the Options page. Permissible GTI reputation threshold values include "do not block", "high risk", medium risk", and "unverified." The TOE will allow IP addresses, URLs, or domain names if the reputation value is "do not block." Other reputation threshold values may be configured by the authorized administrator. The GTI reputation values are provided to the TOE via secure mechanisms provided by the IT environment.

Security audit events are generated by the Firewall and communicated to ePO, where they are saved in the Threat Event Log and reviewed via the same mechanism used for audit events (refer to section 7.6). Each audit event includes a timestamp, the type of event, and client identity. Event data is sent via the

[4] McAfee GTI is a global Internet reputation intelligence system that determines what is good and bad behavior on the Internet. McAfee GTI uses real-time analysis of worldwide behavioral and sending patterns for email, web activity, malware, and system-to-system behavior. Using data obtained from the analysis, McAfee GTI dynamically calculates reputation scores that represent the level of risk to your network when you visit a webpage. The result is a database of reputation scores for IP addresses, domains, specific messages, URLs, and images.

McAfee Agent which is protected in accordance with Protected System Data Transfer discussed in section 7.7.

7.3 Client Web Protection

The TOE implements a Web Control feature that displays safety ratings and reports for websites during online browsing and searching. Websites are assigned a color-coded safety rating based on analysis and test results from McAfee. The software uses the test results to notify the user about web-based threats they might encounter while visiting the site. The safety rating is also present on search engine results pages. This functionality is provided by the Web Control module in the ENS Client.

The administrator creates policies for Web Control on managed systems to control access to sites, pages, and downloads based on their safety rating or type of content. Safety ratings appear in the following scenarios:

- **On search results pages** — an icon appears next to each site listed. The color of the icon indicates the safety rating for the site. The color of the button corresponds to the site's safety rating:
    - White check mark in green circle - tests revealed no significant problems.
    - Black exclamation mark in yellow circle - tests revealed some issues that users might need to know about. For example, the site tried to change the testers' browser defaults, displayed pop-ups, or sent testers a significant amount of non-spam email.
    - White cross in red circle - tests revealed some serious issues that users must consider carefully before accessing this site. For example, the site sent testers spam email or bundled adware with a download.
    - Gray circle with red diagonal line - a policy setting blocked this site.
    - Gray question mark - this site is unrated.
- **In the browser window** — a McAfee button appears in the upper-right corner. The color of the button indicates the safety rating for the site:
    - Green with McAfee SECURE - this site is tested daily and certified safe by McAfee SECURE.
    - Green - this site is safe.
    - Yellow - this site might have some issues.
    - Red - this site might have some serious issues.

- Gray - no rating is available for this site.
- Orange – a communication error occurred with the McAfee GTI server that contains rating information.
- Blue - no information is available to rate this site. The reason might be that the site is internal or in a private IP address range.
- Black - this site is a phishing site.
- White - a policy setting allows this site.
- Silver - a policy setting disabled Web Control.

Safety ratings are determined by McAfee based on testing criteria for each site and evaluating the results to detect common threats. The safety ratings are provided to the TOE via secure mechanisms provided by the IT environment. The TOE will only allow URL or domain name if the McAfee GTI safety rating is "green", and any other GTI safety ratings allowed by the authorized administrator.

Administrators may create policies to:

- Control access to sites, pages, and downloads, based on their safety rating or type of content. For example, block red sites and warn users trying to access yellow sites.
- Identify sites as blocked or allowed, based on URLs and domains.
- Monitor and regulate browser activity on network computers through the ePO management server, and create detailed reports about websites.

7.4 Identification & Authentication

On the ePO management system, the TOE requires users to identify and authenticate themselves before accessing the TOE software. User accounts must first be created on the ePO server by the Administrator. No action can be initiated before proper identification and authentication (I&A). Each TOE user has security attributes associated with their user account that define the functionality the user is allowed to perform.

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

If the user's password is successfully authenticated, the TOE grants access to the ePO management interface and therefore the TOE functionality. If the authentication is not successful, the login GUI is redisplayed. Upon successful login, the administrator status and the union of all the permissions from the permission sets from the user account configuration are bound to the session. Those attributes

remain fixed for the duration of the session (until the user logs off). If the attributes for a logged in user are changed, those changes will not be bound to a session until the next login by the user.

7.5 Management

The TOE's management security function provides administrator support functionality that enables a user to configure and manage TOE components. Management of the TOE is performed using the ePO management console. Management permissions are defined per-user.

The TOE provides functionality to manage the following:

1. User Account management,
2. Permission Set management,
3. Audit Log management,
4. Event Log management,
5. System Tree management,
6. Query management,
7. Dashboard management,
8. Endpoint Security Common Module management,
9. Client Threat Prevention Policy management,
10. Client Communications Protection Policy management, and
11. Client Web Protection Policy Management.

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

7.5.1 User Account Management

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

1. Username;
2. Logon Status (enabled or disabled);
3. Authentication Configuration (must be configured for ePO);
4. Password;
5. Assigned Permissions; and

6. Assigned Role.

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.

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

1. Change server settings.
2. Create and delete user accounts.
3. Create, delete, and assign permission sets.
4. Limit events that are stored in ePolicy Orchestrator databases.

7.5.2 Permission Set Management

A permission set is a group of permissions that can be granted to any users by assigning it to those users’ accounts. One or more permission sets can be assigned to users.

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 server tasks, but another permission set applied to the same account grants all permissions to server tasks, that account has all permissions to server tasks.

Administrators may create, view, modify and delete permission sets. Each permission set has a unique name so that it can be appropriately associated with users. When a permission set is created or modified, the permissions granted via the permission set may only be specified by the Administrator.

7.5.3 Audit Log Management

The audit log captures all user actions and stores them on the ePO server’s external database (provided by the IT Environment). The administrator may configure the length of time audit entries are to be saved. Entries beyond that time are automatically purged.

An administrator or a user with either the “View audit log” or “View and purge audit log” permission may view events in the audit log.

7.5.4 Event Log Management

The Threat Event Log contains all threat events that McAfee ePO receives from managed systems, including events from the ENS Client, which comprises of the Threat Prevention, Firewall, and Web Protection modules. Events are generate based on the policies configured for each of the 3 modules.

Threat Event Log information can be viewed by an Administrator or users with the “View Events” or “View and purge events log” permission. Administrators may view information originating from any system, while other users are limited to information originating on systems they have been granted permission to view.

The Event Log entries are automatically purged based upon a configured age. An Administrator or users with the "View and purge events" permission may issue a command through the ePO GUI to purge all event records older than a specified time.

7.5.5 System Tree Management

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 systems to be organized within units called groups.

Groups have these characteristics:

1. Groups can be created by Administrators.
2. A group can include both systems and other groups.
3. Groups are modified or deleted by an Administrator.

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 you can provide sorting criteria for the subgroups you create within it.)
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.

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 you add to the System Tree. Inheritance may be disabled for individual groups or systems by an 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.

User permissions in the Systems category that are relevant to this information are:

1. View the "System Tree" tab
2. Edit System Tree groups and systems

Systems may be deleted or moved between groups by an Administrator or users with both the "View the "System Tree" tab" and "Edit System Tree groups and systems" permissions. User access to groups in the System Tree is controlled by individual check boxes in the permission sets for the System Tree.

7.5.6 Query Management

Authorized users may create, view, modify, use and delete queries based upon their permissions. Permissions associated with queries are:

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

7.5.7 Dashboard Management

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 private dashboards
3. Edit public dashboards; create and edit private dashboards; make private dashboards public

7.5.8 Endpoint Security Common Module Management

The Endpoint Security Common module provides settings that apply to all modules and features of ENS. These settings include interface security and language settings for ENS Client, logging, and proxy server settings. The following permission is required to ensure the TOE is configured in accordance with the evaluated configuration: ENS Common Policy and Tasks “View and change policy and task settings”

In the evaluated configuration, the following settings are applied:

- Client Interface Mode – the client interface is locked to prevent workstation users from modifying ENS policies.
- Self-Protection – self-protection mode is enabled to protect ENS system resources from malicious activity.

Please refer to the Operational User Guidance and Preparative Procedures Supplement: McAfee Endpoint Security 10.5.0 with ePolicy Orchestrator 5.3.2 for additional information.

7.5.9 Client Threat Prevention Policy Management

Authorized users may create, view, modify, use and delete Client Threat Prevention policies and task settings based upon the following permissions:

- ENS Threat Prevention Policy “View and change settings”
- ENS Threat Prevention Tasks “View and change settings”

Please refer to section 7.1 for information on how authorized administrators manage Client Threat Prevention.

System data collection, analysis and reaction for Client Threat Prevention	ENS Common Policy and Tasks “View and change policy and task settings”
	ENS Threat Prevention Policy “View and change settings”
	ENS Threat Prevention Tasks “View and change settings”
System data collection, analysis and reaction for Client Communications Protection	ENS Common Policy and Tasks “View and change policy and task settings”
	ENS Firewall “View and change policy and task settings”
System data collection, analysis and reaction for Client Web Protection	ENS Common Policy and Tasks “View and change policy and task settings”
	ENS Web Control Policy “View and change settings”
	ENS Web Control Tasks “View and change settings”

7.5.10 Client Communications Protection Policy Management

Authorized users may create, view, modify, use and delete Client Communication Protection policies and task settings based upon the following permission: ENS Firewall “View and change policy and task settings.”

Please refer to section 7.2 for information on how authorized administrators manage Client Communications Protection.

7.5.11 Client Web Protection Policy Management

Authorized users may create, view, modify, use and delete Client Web Protection policies and task settings based upon the following permissions:

- ENS Web Control Policy “View and change settings”
- ENS Web Control Tasks “View and change settings”

Please refer to section 7.3 for information on how authorized administrators manage Client Web Protection.

7.6 Audit

7.6.1 Audit and Server Task Logs

The TOE's audit security function provides auditing of management actions performed by authorized users. Authorized users may review the audit records via the Audit Log. The TOE utilizes two different types of audit logs to record user and server-related events as they occur on ePO:

1. **Audit Log** which captures all user actions and stores them on the ePO server's external database (provided by the IT environment).
2. **Server Task Log** which lists the currently running or historical server tasks and long-running actions. The Server Task Log is stored on the ePO server's external database (provided by the IT environment).

The auditable events are specified in the Audit Events and Details table in the FAU_GEN_EXT.1 section.

Audit entries may be displayed via reports. The information displayed is configurable, but is always presented in human readable form. The Audit Log displays the following information:

- User name: specifies the McAfee ePO user name of the account that attempted to take the action. The user name is unavailable for some actions, for example, failed logins.
- Priority: specifies the importance of the action determined by McAfee.
- Action: specifies the action the user attempted to take.
- Details: specifies further information about the action, if available.
- Success: specifies whether the action succeeded.
- Start Time: specifies the time (on the ePO server) the action began.
- Completion Time: specifies the time (on the ePO server) the action was completed.

The Server Task Log List displays the following information:

- Name: specifies the name of the server task or action.
- Start Date: specifies the date and time (on the ePO server) when the task started.
- End Date: specifies the date and time (on the ePO server) when the task ended.
- User name: specifies the McAfee ePO user name of the individual who launched or scheduled the task.
- Status: specifies the current status of the task.

- Source: specifies the source of the server task. For example, a source of "Scheduler" indicates that the server task was the result of a server task scheduled to run automatically, whereas a source of "Server Task" indicates that the task was run manually.
- Duration: specifies how long the task ran, or has been running.

Audit Log entries can be queried against by an Administrator or users with the "View Audit Log" or "View and purge audit log" permission. The Audit Log entries are automatically purged based upon a configured age. An Administrator or users with the "View and purge audit log" permission may issue a command through the ePO GUI to purge all audit records older than a specified time. The audit log entries are stored in the external database. Protection of the Audit Log and Server Task Log is provided by the IT environment.

7.6.2 Threat Event Log

The Threat Event Log contains all threat events that McAfee ePO receives from managed systems, including events from the ENS Client, which comprises of the Threat Prevention, Firewall, and Web Protection modules. Events are generate based on the policies configured for each of the 3 modules.

The Threat Event Log entries may be displayed via dashboards and reports. The information displayed is configurable, but is always presented in human readable form. The Threat Event Log is stored on the ePO server's external database (provided by the IT environment).

Threat Event Log information can be viewed by an Administrator or users with the "View Events" or "View and purge events log" permission. Administrators may view information originating from any system, while other users are limited to information originating on systems they have been granted permission to view.

The Event Log entries are automatically purged based upon a configured age. An Administrator or users with the "View and purge events" permission may issue a command through the ePO GUI to purge all event records older than a specified time. Protection of the Threat Event Log is provided by the IT environment.

7.7 Protected System Data Transfer

The TOE consists of distributed components. Communications between McAfee Agents and ePO take the form of XML messages. Communications can include policies to implement, properties collected from managed systems, event data gathered by the ENS application, or tasks to be run on the 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 DHE_RSA_AES256_SHA).

In FIPS mode, ePO uses OpenSSL v1.0.2j with FIPS module v2.0.8 (FIPS 140-2 certificate #1747) for TLS 1.2. McAfee Agent uses RSA BSAFE Crypto-C Micro Edition v4.0.1 (FIPS 140-2 certificate #2097) to provide cryptographic services for this link. 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.

OPERATION	ALGORITHM	KEY SIZE IN BITS	STANDARDS	CAVP Cert #
Key Transport	RSA encrypt/decrypt	2048	Allowed in FIPS mode	OpenSSL #1535 BSAFE #1046
Symmetric encryption and decryption	Advanced Encryption Standard (AES) (operating in CBC mode)	256	FIPS 197	OpenSSL #2929 BSAFE #2017
Secure Hashing	SHA-256	Not Applicable	FIPS 180-3	OpenSSL #2465 BSAFE #1767