Security Target

McAfee Endpoint Security 10.7.x with

ePolicy Orchestrator 5.10.x

Document Version 1.0

July 22, 2022

Trellix

Musarubra, LLC

6220 America Center Drive

San Jose, CA 95002

www.trellix.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), McAfee Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.x. 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 that meet the set of requirements.

Table of Contents

List of Tables

List of Figures

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 10.7.x with ePolicy Orchestrator 5.10.x
ST Revision	1.0
ST Publication Date	July 22, 2022
Author	Primasec Ltd.

1.2 TOE Reference

TOE Reference	McAfee Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.x
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	States evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable.
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Defines the security objectives for the TOE/operational environment, and provides a rationale to demonstrate that the security objectives satisfy the threats.
5	Extended Components Definition	Defines the extended components used in the evaluation .
6	Security Requirements	States the functional and assurance requirements for this TOE.
7	Security Requirements Rationale	Provides the rationale relating the security objectives, security functional requirements and the TOE summary specification.

SECTION	TITLE	DESCRIPTION
8	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 types of operation to be performed on security 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.

Other than in 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
Administrator	A person issued with access credentials for ePO, allowing access to management functions of the TOE.
ASSC	Agent-server secure communication (ASSC)
ATP	Adaptive Threat Protection
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
ENS	McAfee Endpoint Security
ePO	ePolicy Orchestrator
ePO Administrator	A person assigned the Administrator permission set in ePO

TERM	DEFINITION
ePO User	A person assigned permissions to carry out tasks in ePO, but not assigned the Administrator permission
Exception	Defines a set of attributes that instructs the Agent to not enforce a rule or policy, resulting in an Event not being generated.
GTI	Global Threat Intelligence
I&A	Identification and Authentication
IPS	Intrusion Prevention System
IT	Information Technology
JRE	Java Runtime Environment
MA	McAfee Agent
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
User	A person having access to TOE functions on a client device.

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

McAfee® Endpoint Security (ENS) is a security management solution that protects servers, computer systems, laptops, and tablets against known and unknown threats. These threats include malware, suspicious communications, unsafe websites, and downloaded files. Endpoint Security enables multiple defense technologies to communicate in real time to analyze and protect against threats.

While multiple management options are available, the TOE must be managed using McAfee ePolicy Orchestrator (ePO). In the TOE configuration only Windows-based clients are managed.

Security functionality is enforced on client computers through the following integrated modules working collectively to protect systems from a wide range of threats from software, communications, and websites:

- **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.
- **Firewall** - Monitors communication between the computer and resources on the network and the Internet. Intercepts suspicious communications.

- **Web Control** – Monitors web searching and browsing activity on client systems, and blocks downloads and access to websites based on safety rating and content.
- **Adaptive Threat Protection**[1] – Analyzes content from the enterprise, and decides how to respond, based on file reputation, rules and reputation thresholds.

Together, these modules are referred to as the McAfee Endpoint Security Client. In addition, the Common module provides settings for common features, such as interface security and logging. This module is installed automatically if any other module is installed. All modules integrate into a single Endpoint Security interface on the client system.

In addition to the integrated client modules, the TOE requires the installation of the McAfee Agent on each computer to be protected.

ENS client software is operating system specific, and 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) computers. The architecture allows the ENS software to be centrally managed, and yet decrease the 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 computer to be protected, and contains five integrated ENS modules, together with the McAfee Agent. ePO Management software is installed on a dedicated server.

1.7.1 McAfee Endpoint Security (ENS) Client

The McAfee ENS Client is comprised of the Threat Prevention, Firewall, Web Control, Adaptive Threat Protection and Common 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. 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.

[1] Adaptive Threat Protection is an optional module that is included within the scope of the TOE.

  - 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. Connecting to the ePO server or directly to a McAfee 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.
    - Latest threat information from McAfee GTI for unknown objects.
    - Upgrades to software components (via ePO only).
    - 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. 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 installed on each managed system that provides secure communication between the ENS Client and the ePO server. McAfee Agent is a vehicle of information and enforcement between the ePO server and each managed (client) computer. It performs the following functions:

- Gathers information and events from managed computers and sends them to the ePO server.
- Installs the ENS Client on the managed computers.
- Provides the monitoring policies to the ENS client installed on the managed computers.
- 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 that 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 computers.
- ENS-specific functions for administering policy management for the Threat Prevention, Firewall, Web Control and Adaptive Threat Protection 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), audit data, and all other relevant data that the server needs to keep managed systems up to date. ePO provides cryptographic support for authentication to the internal SQL database, and for encryption of some of the data stored within it, using RSA BSAFE Crypto-C Micro Edition 4.1.2 (CMVP certificate #2294). Note that this is not used for protection of the network traffic to an SQL server, but is rather an additional layer of internal data protection that is outside the scope of this evaluation. In the evaluated configuration this database is installed on the same physical platform as ePO.

ePO can be managed using a browser interface. Communication with the browser is protected using TLS. ePO provides support for this connection using Bouncy Castle FIPS Java API 1.0.2.1.

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.

Note that ePO can be used to manage a wide range of McAfee products, but all managed products other than ENS are excluded from the scope of the evaluation.

1.7.4 Physical Boundary

The TOE is software-only and includes:

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

The physical components of the TOE are 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 client computers (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 conform to the evaluated configuration, the following hardware and software components must be used. Note that the product extensions listed in the table manage policies and tasks on the ePO server, and the installation packages install Endpoint Security on the client endpoints.

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software (available for download from McAfee.com when in possession of a valid grant number)	• McAfee Endpoint Security 10.7.0 February 2022 Update, with the following extensions and installation packages: ○ Platform 10.7.0.3255 ○ Platform Extension 10.7.0.1076 ○ Threat Prevention 10.7.0.3299 ○ Threat Prevention Extension 10.7.0.1248 ○ Firewall 10.7.0.2157 ○ Firewall Extension 10.7.0.1116 ○ Web Control 10.7.0.2581 ○ Web Control Extension 10.7.0.1162 ○ Adaptive Threat Protection 10.7.0.3437 ○ Adaptive Threat Protection Extension 10.7.0.1128 ○ Threat Detection Reporting Extension 1.0.0.720[2] • ePO Server 5.10.0 Refresh 6 (download package EPO_510_2428_68_LR6.zip), Update 13 (download package ePO_5.10.0_Update_13.zip) • McAfee Agent Version 5.7.5.504 McAfee Agent Extension 5.7.5.54
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 (available from docs.McAfee.com)	The guidance for the TOE is described in the following documentation: • Security Target: McAfee Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.x (this document) • McAfee Endpoint Security 10.7.x Product Guide - Windows • McAfee Endpoint Security 10.7.x Installation Guide • McAfee ePolicy Orchestrator 5.10.0 Product Guide • McAfee ePolicy Orchestrator 5.10.0 Installation Guide • McAfee Agent 5.7.x Product Guide • McAfee Agent 5.7.x Installation Guide • McAfee Endpoint Security 10.7.x with ePolicy Orchestrator 5.10.- Common Criteria Evaluated Configuration Guide

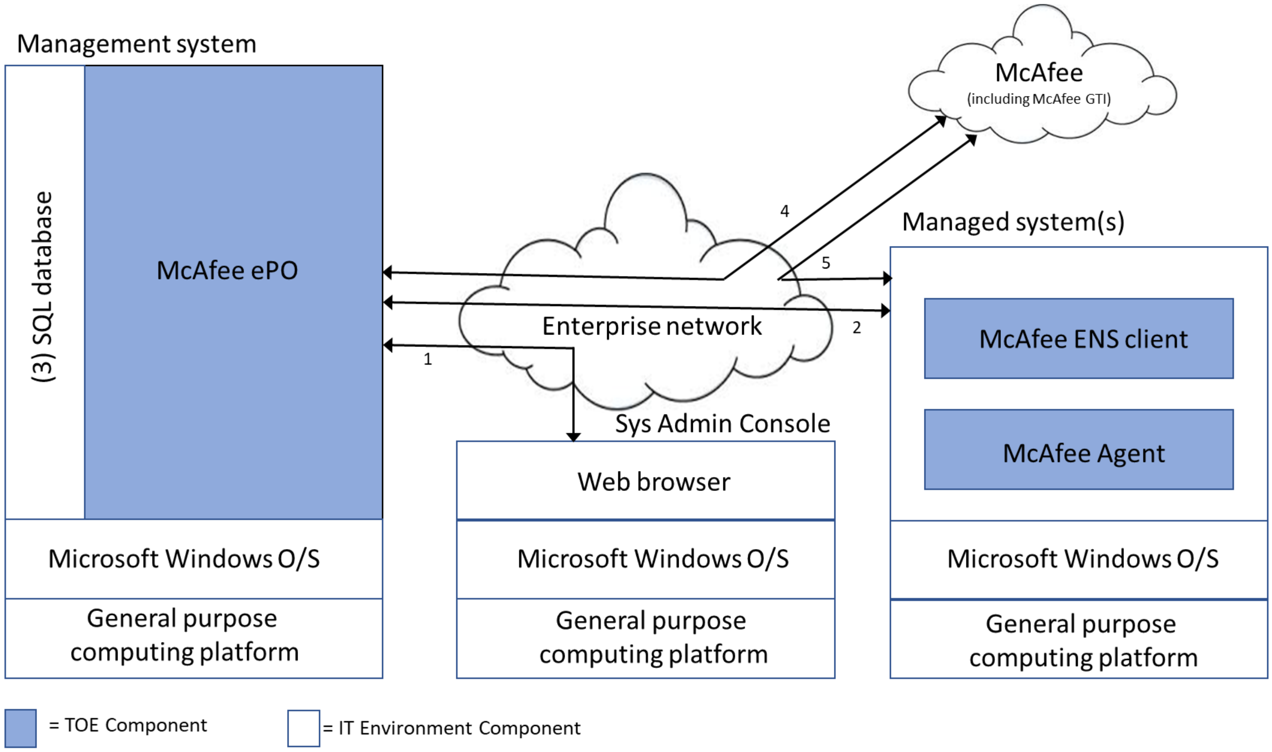
Table 3 – Evaluated Configuration for the TOE

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

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

[2] Provides ePO reporting functionality as part of the Adaptive Threat Protection module.

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.



1 ePO can be managed locally or remotely over the enterprise network, using a web browser.

2 ePO and McAfee Agent communicate via the enterprise network for client installation, configuration and reporting.

3 ePO uses an external database to store configuration data, reports and audit records. In the evaluated configuration this database is installed on the same physical platform as ePO.

4 ePO receives TOE updates and AMCore content[3] from McAfee. The ENS Client receives updates and content from ePO using MA.

5 During monitoring of processes and scanned items the ENS Client sends queries and receives responses from external McAfee GTI, Advanced Threat Protection and Real Protect servers.

Figure 1 – TOE Boundary

1.7.5 Specific Options for the Evaluated Configuration

The following specific configuration options apply to the evaluated configuration:

[3] When ENS searches files for threats, the scan engines analyze files and processes using threat information stored in the AMCore content files. AMCore content files contain information (signatures and rules) for cleaning and counteracting damage that the threat can cause. McAfee finds and adds known threat information to the content files, then releases these updated content files regularly.

1. Adaptive Threat Protection[4] is included in the evaluated configuration.
2. Self-managed systems (i.e. when a User installs the client software, customizes the features, and manages detections) are excluded from the evaluation.
3. All cloud based ePO deployments have been excluded from the evaluated configuration.
4. The IT Environment provides an external database for event storage, and other system data, used by the ePO server. The database can reside on the same platform as ePO, or can be configured on a different platform. In the evaluated configuration the same platform is used, and a TLS connection is not required.
5. The ENS Client interface must be locked, with self-protection enabled.
6. The option to consult a TIE Server for reputation information is not configured, and the TOE uses GTI only.
7. Certificate, Windows and LDAP Administrator authentication methods to the ePO server have been excluded from the evaluated configuration.
8. The utilization of syslog servers, Windows event logs, email or Twitter accounts to send events and/or system messages has been excluded from the evaluated configuration.
9. The use of ePO web API commands, with the command-line, to automate ePO configuration using scripts has been excluded from the evaluation.
10. Running the ePO server in cluster mode is not permitted in the evaluated configuration.
11. Expert Rules that can be configured for Access Protection policies have been excluded from the evaluation.
12. Network IPS protection for Threat Prevention has been excluded from the evaluation.

1.7.6 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 compatible (4 cores minimum recommended)
Memory	8GB physical RAM recommended minimum
Free Disk Space	20 GB — Recommended minimum
Network Interface Card	100MB or higher

[4] Adaptive Threat Protection (formerly named Threat Intelligence) is an optional ENS module that analyzes content the enterprise, and decides what to do based on file reputation, rules, and reputation thresholds.

Component	Minimum Requirements
Operating System (64-bit)	Microsoft Windows Server 2019
DBMS	Microsoft SQL Server 2017
Required Software (installed automatically)	Microsoft Visual C++ 2010 Redistributable Package (x64 and x86) Microsoft Visual C++ 2015 Redistributable Package (x64 and x86) MSXML 3.0 and 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 computers. The supported platforms for these components are both client and server Windows-based operating systems:

OS TYPE	SUPPORTED AGENT OS
Client	Windows 10 21H2
Server	Windows 2019 Server

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 Edge (on Windows version 1703 and later) Microsoft Edge Chromium Google Chrome

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

ENS makes use of McAfee GTI and Real Protect services provided by McAfee, that are present in the TOE environment. These provide cloud-based reputation services for files, processes, websites, network connections and certificates.

The ENS Client uses Windows to provide cryptographic services in support of TLS 1.2 connections direct to the McAfee GTI service. These cryptographic services are FIPS-140 validated (CMVP certificate: Windows 10 & Windows Server 2019 #3197).

The ENS Client uses McAfee OpenSSL FIPS Object Module v1.0.2c to provide cryptographic services in support of TLS 1.2 connections direct to the McAfee Real Protect service.

1.7.7 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 this section.

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 are pre-defined by the Administrator to run 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 computers 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 computers is prevented by monitoring user-mode API calls to recognize when they occur. When a detection occurs, information is recorded in the activity log, alerted on the client computer, and sent to the management server.
Client Communications Protection	The TOE implements a firewall that scans all incoming and outgoing traffic on managed computers (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 an Administrator to also block incoming and outgoing

TSF	DESCRIPTION
	traffic from a network connection that McAfee Global Threat Intelligence (GTI)[5] 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 computer.
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. Administrators create policies for Web Control on managed computers 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. An Administrator can monitor and regulate browser activity on network computers, and create detailed reports about websites. Administrators can also control User access to Web Control features and configuration settings.
Client Adaptive Threat Protection	The TOE provides Adaptive Threat Protection (ATP), which examines content on a managed computer, and decides what action to take based on file reputation, rules, and reputation thresholds. It is designed to protect against files with unknown reputations, detect malicious patterns, and correct false positives. ATP uses McAfee GTI to support this analysis. Dynamic Application Containment allows files whose reputation is unknown to run in a container, limiting the actions they can take.
Identification and Authentication	The TOE requires Administrators 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 Administrator has security attributes (permissions) associated with their account that define the functionality the Administrator is allowed to perform.
Management	The TOE's Management Security Function provides Administrator functionality that enables an Administrator to configure and manage TOE

[5] McAfee GTI is a global Internet reputation intelligence system that characterizes 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 a network when a webpage or file is accessed. The result is a database of reputation scores for IP addresses, domains, specific messages, URLs, and images.

TSF	DESCRIPTION
	components. Configuration functionality includes enabling an authorized Administrator to modify TSF Data. Management functionality includes invocation of TOE functions that affect 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 Administrator.
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 undetected modification.

Table 7 – Logical Boundary Descriptions

1.7.8 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 Administrators.

1.7.8.1 ePO TOE Data

TSF Data	Description	AD	UA	GE
Audit Log	History list of Administrator actions on the ePO server.			✓
Dashboards	Collections of chart-based queries that are refreshed at an Administrator-configured interval.			✓
ePO Administrator Accounts	Administrator name, role, authentication type, logon status, and permission set for each Administrator 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 Administrators by assigning it to those Administrators' 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 computer (e.g. internet address) in the System Tree.			✓
System Tree	A hierarchical collection of all of the systems managed by ePolicy Orchestrator.			✓

TSF Data	Description	AD	UA	GE
Threat Event Log	Lists all threat events generated by the managed computers.			✓
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)

1.7.8.2 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 computer.			✓
AMCore	A content file which contains the latest rules and signatures used by Threat Prevention and Adaptive Threat Protection on the client computers.			✓
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 computers.			✓
On-Access Scan Policies	Policies that enable and define when on-access scans are performed and the actions taken upon detection on the client computers. 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 computers, 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 computers.			✓
Options Policies	Policies that specify the quarantine settings, exclusions, and unwanted program detections on the client computers.			✓
Quarantine Policies	Policies that specify where quarantined files are stored on the client computers, and how long they are kept.			✓
Quarantined Files	Collection of files on a client computer that have been quarantined by Threat Prevention.			✓
Unwanted Programs	A list of undesirable programs to be detected on the client computers.			✓

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

1.7.8.3 Client Communications Protection TOE Data

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)

1.7.8.4 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)

Information)

1.7.8.5 Client Adaptive Threat Protection TOE Data

TSF Data	Description	AD	UA	GE
Adaptive Threat Protection policies	Dynamic Application Containment policies and default policies specify rules for application containment (blocking and monitoring).			✓
ATP rules	Determine what processes can and can't do within a specific context, and can change reputation based on context and behavior. McAfee delivers updates to rules in AMCore content every month.			✓
Custom file exclusions	List of explicitly trusted files within an organization.			✓
Local reputation cache	Stored on each client computer, as first port of call to lookup file reputations (hashes).			✓

TSF Data	Description	AD	UA	GE
Process monitoring logs	Logs of all files that unknown processes create, modify or delete, allowing rollback.			✓
Quarantine Policies	Policies that specify where quarantined files are stored on the client computers, and how long they are kept.			✓
Quarantined Files	Collection of files on a client computer that have been quarantined by Adaptive Threat Protection.			✓
Sensitivity level	Configures the sensitivity level to use with client-based scanning when determining whether the file matches known malware (low, medium, high)			✓
Rule assignment	Specifies the set of rules that Adaptive Threat Protection uses to calculate a reputation.(productivity, balanced, security)			✓

Table 12 – Client Adaptive Threat Protection TOE Data (Legend: AD=Authentication data; UA=User attribute; GE=Generic Information)

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 5 (April 2017) Part 2 extended and Part 3 conformant at Evaluation Assurance Level 2 augmented by ALC_FLR.2– Flaw Reporting Procedures (EAL2+).

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:

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

This chapter identifies assumptions as A.A*ssumption*, threats as T.*Threat* and policies as P.*Policy*.

3.1 Threats

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

- Attackers who are not TOE Users or Administrators: They may have public knowledge of how the TOE operates, but are assumed to possess a low skill level, limited resources, and no physical access to the TOE.
- TOE Users and Administrators: They may have extensive knowledge of how the TOE operates, may possess a high skill level, moderate resources to alter TOE configuration settings or parameters, and may have physical access to the TOE. TOE Users and Administrators may act in an unsafe manner, but are assumed not to be wilfully hostile to the TOE, or to the assets that it protects.

Both threat agents are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE, and the hosts on the protected network.

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE is responsible for addressing threats to the environment in which it resides, and there are also threats related to the TOE itself.

The TOE addresses the following threats.

THREAT	DESCRIPTION
T.MALWARE	An attacker may attempt to introduce malware onto computers via network traffic or removable media, with the aim of gaining unauthorized access to User data, or disruption of operations on that computer, or using that computer to attack additional systems.
T.COMMS	An attacker may attempt to compromise communications between Users and resources on a network and the internet, with the aim of gaining unauthorized access to data or disrupting operations.

THREAT	DESCRIPTION
T.BADWEB	Users may access unsafe websites, or download unsafe files, that may lead to unauthorized disclosure of User data or disruption of operations.

Table 13 – Threats in the TOE Environment

THREAT	DESCRIPTION
T.BADACCESS	An unauthorized person may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.COMDIS	An attacker may attempt to disclose, modify or delete the data collected and produced by the TOE by bypassing a security mechanism.
T.FACCNT	Attempts by an unauthorized person to access TOE data or security functions may go undetected, allowing the correct functioning of the TOE to be compromised.
T.IMPCON	An unauthorized person may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.ASPOOF	An attacker 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.

Table 14 – Threats against the TOE

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following organizational security policy applies to the TOE environment.

POLICY	DESCRIPTION
P.CRYPTO	When carrying out cryptographic functions to protect the integrity of data in transit the TOE shall use cryptographic modules that have been validated to FIPS 140.

Table 15 – 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.TIME	The IT Environment will provide reliable timestamps for the TOE to use.
A.DYNAMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT systems the TOE monitors.
A.GTI	McAfee GTI is present in the IT environment, and can be accessed by the TOE.
A.GTIDOWN	Managed computers will securely download reputation values for URLs and domains and safety ratings for websites in real-time through McAfee GTI.
A.MANAGE	There will be one or more competent individuals assigned to administer the TOE and the security of the information it contains.
A.NOEVIL	The Administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTECT	The TOE, and hardware and software critical to security policy enforcement, will be protected from unauthorized physical modification.
A.SECMGMT	Management sessions will utilize HTTPS communication between the Administrator's web browser and the ePO web server to protect management session data.
A.SECUPDATE	Administrators will implement secure mechanisms for receiving and validating updated threat information and TOE updates from McAfee, and for distributing the updates via the central management system.

Table 16 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.KMALWARE	The TOE must detect and take action against known malware introduced to a client device via network traffic or removable media.
O.UMALWARE	The TOE must monitor User activity to detect, monitor, and take action against unknown files accessed, and processes run on a client device, based on file reputation.
O.FIREWALL	The TOE must monitor and control communication between client devices and resources on the internal network and internet to intercept suspicious communications.
O.WEB	The TOE must monitor web searching and browsing activity on client devices, and block websites and downloads based on reputation and content.
O.ACCESS	The TOE must allow authorized persons to access only appropriate TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of 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 administrators prior to allowing access to TOE functions and data.
O.EXPORT	When any TOE component makes its data available to another TOE component, the TOE must ensure the confidentiality of the TOE data.
O.PROTECT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.CRYPTO	The TOE must provide cryptographic functionality and protocols required for the TOE to securely transfer information between distributed portions of the TOE, and between the TOE and the browser used to support management sessions; and must use only cryptographic modules that have been validated to FIPS 140.

Table 17 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.MANSCAN	Authorized users of client devices must initiate manual anti-virus scans of removable media (e.g., USB tokens, CDs) introduced into the client device before accessing any data on the removable media.
OE.AUDIT_PROTECTION	The IT Environment must 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.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 must be interoperable with the IT System it monitors.
OE.PERSON	Personnel working as authorized administrators must be carefully selected and trained for proper operation of the System.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE, and its supporting hardware and software, that are critical to security policy are protected from any physical attack.
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 must ensure that threat information and TOE 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 must securely store TOE data in the external database and securely retrieve it when directed by the TOE.
OE.GTI	McAfee GTI must be accessible by the TOE in the IT Environment.
OE.GTIDAT	Administrators must ensure that managed computers receive reputation values for URLs and domains, and safety ratings for websites from McAfee GTI in real-time via secure mechanisms.
OE.TIME	The IT Environment must provide reliable timestamps to the TOE.

Table 18 – 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. The following table provides a high-level mapping of coverage for each threat, assumption, and policy:

OBJECTIVE THREAT / ASSUMPTION	O.KMALWARE	O.UMALWARE	O.FIREWALL	O.WEB	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.EXPORT	O.PROTECT	O.CRYPTO	OE.MANSCAN	OE.AUDIT PROTECTION	OE.CREDEN	OE.INSTAL	OE.INTROP	OE.PERSON	OE.PHYSICAL	OE.PROTECT	OE.SD PROTECTION	OE.SECURE UPDATES	OE.SECURE STORAGE	OE.GTI	OE.GTIDAT	OE.TIME
T.MALWARE	✓	✓										✓									✓		✓	✓	
T.COMMS			✓																						
T.BADWEB				✓																	✓		✓	✓	
T.BADACCESS					✓		✓	✓		✓				✓				✓							
T.COMDIS					✓			✓	✓	✓	✓			✓				✓				✓			
T.FACCNT					✓	✓		✓					✓												✓
T.IMPCON					✓	✓		✓		✓				✓				✓			✓				
T.ASPOOF			✓																						
A.ACCESS																✓									
A.TIME																									✓
A.DYNAMIC																✓	✓								
A.GTI																			✓				✓		
A.GTIDOWN																								✓	
A.MANAGE															✓		✓								
A.NOEVIL														✓	✓		✓								
A.PROTECT																		✓							
A.SECMGMT																			✓	✓					
A.SECUPDATE																					✓				
P.CRYPTO											✓														

Table 19 – 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
T.MALWARE	*An attacker may attempt to introduce malware onto computers via network traffic or removable media, with the aim of gaining unauthorized access to User data or disruption of operations on that computer, or using that computer to attack additional systems.* The O.KMALWARE and O.UMALWARE objectives mitigate this threat by providing mechanisms to detect and manage malware that may be introduced onto a client device. OE.MANSCAN supports this by requiring Users to instigate manual scans of removable devices. OE.SECURE_UPDATES, OE.GTI and OE.GTIDAT deal with the provision of up to date threat information, and the availability of GTI in the environment to provide the latest threat information.
T.COMMS	*An attacker may attempt to compromise communications between Users and resources on a network and the internet, with the aim of gaining unauthorized access to data or disrupting operations.* O.FIREWALL mitigates this threat by requiring the TOE to monitor and control communications between client devices and the internet.
T.BADWEB	*Users may access unsafe websites, or download unsafe files, that may lead to unauthorized disclosure of data or disruption of operations.* O.WEB mitigates this threat by requiring the TOE monitor web searching and browsing activity on client devices, and block websites and downloads based on reputation and content. OE.SECURE_UPDATES, OE.GTI and OE.GTIDAT support this objective by helping to ensure that up to date threat information (AMCore content) is available and deployed to client devices, and that GTI is available in the TOE environment.
T.BADACCESS	*An unauthorized person may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.* O.EADMIN calls for the presence of effective management functions on the TOE. O.IDAUTH mitigates the threat of misuse by requiring that Administrators are authenticated before access is granted to TOE management functions and data. OE.CREDEN requires that administrators protect their access credentials. O.ACCESS requires that access by authenticated Administrators to TOE functions and data is restricted to that needed to perform their duties. O.PROTECT requires that The TOE prevents interference with its operation by Users or unauthorized persons. OE.PHYSICAL addresses the need to protect against interference via physical attacks.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.COMDIS	*An attacker may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.* The O.IDAUTH objective requires authentication of Administrators prior to any TOE data access. OE.CREDEN requires that administrators protect their access credentials. The O.EXPORT objective requires 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.PROTECT objective addresses this threat by providing TOE self-protection. The OE.PHYSICAL and OE.PROTECT objectives require that the TOE is protected against physical interference O.CRYPTO requires that communications are protected by encryption against disclosure or undetected modification. OE.SECURE_STORAGE requires that TOE data be protected in the external database.
T.FACCNT	*Attempts by an unauthorized person to access TOE data or security functions may go undetected, allowing the correct functioning of the TOE to be compromised.* The O.AUDITS objective counters this threat by requiring the TOE to audit attempted data access and use of TOE functions. OE.TIME supports this objective by requiring an accurate time source from the IT environment. OE.AUDIT_PROTECTION supports this by requiring protection for audit data when exported from the TOE. The O.IDAUTH objective requires authentication prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized persons to access TOE functions and data.
T.IMPCON	*An unauthorized person may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.* The O.IDAUTH objective requires authentication of Administrators prior to any TOE function accesses. . OE.CREDEN requires that administrators protect their access credentials. The O.ACCESS objective builds upon the O.IDAUTH objective by requiring that authorized persons can only access TOE functions requires for their roles. O.AUDITS supports this objective by requiring records of access to functions and data. O.PROTECT requires that the TOE provide protections against unauthorized modifications. OE.PHYSICAL requires that the TOE is protected against configuration changes through physical interference. OE.SECURE_UPDATES requires that potential updates to threat information (AMCore content) and the TOE are validated before being applied.
T.ASPOOF	*An attacker 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.FIREWALL objective ensures the TOE mediates the flow of all information between client devices and other users and/or IT entities located on internal and external networks governed by the TOE.

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 requires that the TOE has the necessary access.
A.TIME	*The IT Environment will provide reliable timestamps for the TOE to use.* OE.TIME requires reliable timestamps to be provided by the IT environment.
A.DYNAMIC	*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 requires that the TOE has the necessary access to the IT System. The OE.PERSON objective requires that the TOE will be managed appropriately by trained staff.
A.GTI	*McAfee GTI is present in the IT environment, and can be accessed by the TOE.* OE.GTI requires that McAfee GTI is present in the IT environment, and is accessible by the TOE. OE.PROTECT requires that updates are protected by the environment from tampering.
A.GTIDOWN	*Managed computers will securely download reputation values for URLs and domains and safety ratings for websites in real-time through McAfee GTI.* The OE.GTIDAT objective requires that managed systems receive reputation values for URLs and domains and safety ratings for websites from McAfee GTI in real-time via secure mechanisms.
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 requires all Administrators to be qualified and trained to manage the TOE. OE.INSTALL requires that the TOE is managed in a manner consistent with IT security.
A.NOEVIL	*The Administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.* The OE.PERSON objective requires all Administrators to be qualified and trained to manage the TOE The OE.INSTAL objective requires that the TOE is properly installed and operated. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data
A.PROTECT	*The TOE, and hardware and software critical to security policy enforcement, will be protected from unauthorized physical modification.* The OE.PHYSICAL objective provides for the physical protection of the TOE, and for its supporting hardware and software.
A.SECMGMT	*Management sessions will utilize HTTPS communication between the Administrator's web browser and the ePO web server to protect management session data.* The OE.SD_PROTECTION and OE.PROTECT objectives require 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.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.SECUPDATE	*Administrators will implement secure mechanisms for receiving and validating updated threat information and TOE updates from McAfee, and for distributing the updates via the central management system.* The OE.SECURE_UPDATES objective requires Administrators to use secure mechanisms to receive and validate the updates from McAfee, then use secure mechanisms to distribute the updates to the central management systems.
P.CRYPTO	*When carrying out cryptographic functions to protect the integrity of data in transit the TOE shall use cryptographic modules that have been validated to FIPS 140.* O.CRYPTO requires that communication between the management server and client devices be encrypted using a FIPS 140 validated module. It also requires that the TOE supports management sessions via a remote browser using a FIPS 140 validated cryptographic module.

Table 20 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Anti-Malware (FAM) Class of SFRs

The components in this section are 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 addresses the detection and response capabilities of anti-malware products 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 client devices 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-client device 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-client device 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 client device 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 client device until they are acknowledged by the user of the client device, or the user session ends.

FAM_ALR_(EXT).1.3 Upon receipt of an audit event from a client device 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 client device 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 and reputation.

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

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

FAM_SCN_(EXT).1.4 The TSF shall perform manually invoked scans when directed by a 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 listed 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(1-2)	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.2	User authentication before any action
	FIA_UID.2	User Identification before any action
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
Trusted Path	FTP_TRP.1	Trusted Path

Table 21 – 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 table below*].

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 table below*].

COMPONENT	AUDIT 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 malware	Malware detected, action taken, file or process identifier where malware is detected
FIA_ATD.1	All changes to TSF data (including passwords) result in an audit record being generated.	None
FIA_UAU. 2	All use of the authentication mechanism	User identity, location
FIA_UID.2	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 22 – 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 [*ePO Users with the "View audit log" or "View and purge audit log" permission or ePO 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-client device 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-client device 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 client device 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 client device until they are acknowledged by the user of the client device, or the user session ends.

FAM_ALR_(EXT).1.3 Upon receipt of an audit event from a client device 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 client device 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 requires 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 and reputation.

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

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

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

Application Note: Administrators require the Endpoint Security Threat Prevention Policy "View and change settings" permission and/or the Endpoint Security Threat Prevention Tasks "View and change settings" permission.

6.1.3 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 [*CTR_DRBG for random number generation*] and specified cryptographic key sizes *[128 bits and 256 bits for AES encryption/decryption, 2048 bits for RSA key transport*] that meet the following: [*NIST Special Publication 800-133Rev2*].

6.1.3.2 FCS_CKM.1(2) Cryptographic Key Generation (MA)

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*CTR_DRBG for random number generation*] and specified cryptographic key sizes [*256 bits for AES encryption/decryption, 2048 bits for RSA key transport*] that meet the following: [*NIST Special Publication 800-133Rev2*].

6.1.3.3 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: [*No standard*].

6.1.3.4 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 23 – Cryptographic Operations

OPERATION	ALGORITHM	KEY SIZE IN BITS	STANDARDS
Key Exchange	RSAECDHE		See NIST SP800-52 rev2
Authentication/Digital Signature	RSA DSA ECDSA		FIPS 186-4
Symmetric encryption and decryption	AES (operating in CBC mode) AES (operating in GCM, CBC modes)	256 128, 256	FIPS 197, NIST SP800-38A for McAfee OpenSSL FIPS Object Module FIPS 197, NIST SP800-38A (CBC), NIST SP800-38D (GCM) for Bouncy Castle
Secure Hashing	SHA-256 SHA, SHA-256, SHA-384		FIPS 180-4 (for McAfee OpenSSL FIPS Object Module FIPS 180-4 for Bouncy Castle
DRBG			NIST SP800-90A

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 device, 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 Administrators. Windows maintains security attributes for client device Users.

6.1.5.2 FIA_UAU.2 User authentication before any action

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

6.1.5.3 FIA_UID.2 User identification before any action

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

6.1.6 Security Management (FMT)

6.1.6.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [modify the behavior] of the functions [*as identified in the following table* to *an ePO User with the permissions identified in the following table, or an ePO 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”

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

Table 24 – 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 [restrictive] 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 ePO Administrator*].

TSF Data	Associated Permission	Operations Permitted
Audit Log	View audit log	View
	View and purge audit log	View and delete
Dashboards	Use public dashboards	Use public dashboards
	Use public dashboards; create and edit private dashboards	Use public dashboards; create and modify private dashboards
	Use public dashboards; create and edit private dashboards; make private dashboards public	Use public dashboards; create and modify private dashboards; make private dashboards public
ePO User Accounts	n/a (only allowed by an ePO 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 ePO Administrator)	Query

TSF Data	Associated Permission	Operations Permitted
Permission Set	n/a (only allowed by an ePO Administrator)	Query, create, delete, duplicate, edit and assign (to a user)
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
	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 25 - 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
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

TSF Data	Associated Permission	Operations Permitted
Quarantined Files	N/A – action associated with quarantined files is determined by the Quarantine Policy. 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 26 - 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 27 - TSF Data Access Permissions for Client Communications Protection

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 28 - TSF Data Access Permissions for Client Web Control

TSF Data	Associated Permission	Operations Permitted
Adaptive Threat Protection policies	ENS Adaptive Threat Protection: Policy: View settings	Query
	ENS Adaptive Threat Protection: Policy: View and change settings	Query, create, delete and modify

TSF Data	Associated Permission	Operations Permitted
ATP rules	ENS Adaptive Threat Protection: Policy: View settings	Query
	ENS Adaptive Threat Protection: Policy: View and change settings	Query and modify
Custom file exclusions	ATP file exclusion works when added to the Threat Prevention exclusion list	N/A
Local reputation cache	N/A – data held on client computer	N/A
Process monitoring logs	N/A – data held on client computer	N/A
Quarantine Policies	Quarantine policy is handled by the Threat Prevention module	N/A
Quarantined Files	N/A – action associated with quarantined files is determined by the Quarantine Policy. Users can access their quarantined files.	N/A
Sensitivity level	ENS Adaptive Threat Protection: Policy: View settings	Query
	ENS Adaptive Threat Protection: Policy: View and change settings	Query, modify
Rule assignment	ENS Adaptive Threat Protection: Policy: View settings	Query
	ENS Adaptive Threat Protection: Policy: View and change settings	Query, modify

Table 29 - TSF Data Access Permissions for Adaptive Threat 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: [*Management of TSF data*].

6.1.6.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [*ePO Administrator and ePO User with assigned permissions*].

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

Application Note: An ePO Administrator here is an ePO user account assigned to the built-in Administrator permission set. ePO Users refer to ePO user accounts without the Administrator permission set, but with other specific permission sets. In ePO a role is called a permission set. Elsewhere in this ST the terms Administrator (ePO Administrator or ePO User) and User (person using a client device) are used.

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.

6.1.8 Trusted Path (FTP)

6.1.8.1 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall provide a trusted communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*undetected modification*].

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
ASE: Security Target	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	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 30 – 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.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(1-2)	No other components	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Satisfied by FCS_COP.1 and FCS_CKM.4
FCS_CKM.4	No other components	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Satisfied by FCS_CKM.1
FCS_COP.1	No other components	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	Satisfied by FCS_CKM.1 and FCS_CKM.4
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.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UID.2	FIA_UID.1	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

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FMT_MTD.1	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components	None	N/A
FMT_SMR.1	No other components	FIA_UID.1	Satisfied by FIA_UID.2
FPT_ITT.1	No other components	None	N/A
FTP_TRP.1	No other components	None	N/A

Table 31 – 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.

7 Security Requirements Rationale

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

7.1 Security Functional Requirements for the TOE

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

OBJECTIVE SFR	O.KMALWARE	O.UMALWARE	O.FIREWALL	O.WEB	O.ACCESS	O.AUDITS	O.EADMIN	O.IDAUTH	O.EXPORT	O.PROTECT	O.CRYPTO
FAU_GEN_(EXT).1						✓					
FAU_GEN.2						✓					
FAU_SAR 1					✓		✓				
FAU_SAR.2					✓			✓			
FAM_ACT_(EXT).1	✓	✓									
FAM_ALR_(EXT).1	✓	✓									
FAM_SCN_(EXT).1	✓	✓									
FCS_CKM.1(1-2)									✓	✓	✓
FCS_CKM.4									✓	✓	✓
FCS_COP.1									✓	✓	✓
FDP_IFC.1			✓	✓							
FDP_IFF.1			✓	✓							
FIA_ATD.1								✓			
FIA_UAU.2					✓			✓			
FIA_UID.2					✓			✓			
FMT_MOF.1					✓			✓		✓	
FMT_MSA.3			✓				✓				
FMT_MTD.1					✓		✓	✓		✓	
FMT_SMF.1					✓		✓				
FMT_SMR.1					✓		✓	✓			
FPT_ITT.1									✓		
FTP_TRP.1										✓	✓

Table 32 – Mapping of TOE SFRs to Security Objectives

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

OBJECTIVE	RATIONALE
O.KMALWARE	*The TOE must detect and take action against known malware introduced to a client device via network traffic or removable media.* The TOE is required to scan the client device for malware [FAM_SCN_(EXT).1]. The TOE will take action against detected malware [FAM_ACT_(EXT).1]. The TOE will alert Users and authorized Administrators when malware is detected [FAM_ALR_(EXT).1].
O.UMALWARE	*The TOE must monitor User activity to detect, monitor, and take action against unknown files accessed, and processes run on a client device, based on file reputation.* The TOE is required to scan the client computer for malware [FAM_SCN_(EXT).1]. The TOE will take action against detected malware [FAM_ACT_(EXT).1]. The TOE will alert Users and authorized Administrators when malware is detected [FAM_ALR_(EXT).1].
O.FIREWALL	*The TOE must monitor and control communication between client devices and resources on the internal network and internet to intercept suspicious communications.* 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.WEB	*The TOE must monitor web searching and browsing activity on client devices, and block websites and downloads based on reputation and content.* The TOE will examine attempts by Users to access web pages and download files, and will allow or deny that access based on the CLIENT COMMUNICATIONS PROTECTION SFP [FDP_IFC.1, FDP_IFF.1], displaying alerts to Users as determined by the policy.
O.ACCESS	*The TOE must allow authorized persons to access only appropriate TOE functions and data.* Administrators authorized to access the TOE are determined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized Administrators 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 Administrators [FAU_SAR.1, FAU_SAR.2].

OBJECTIVE	RATIONALE
O.AUDITS	*The TOE must record audit records for data accesses and use of 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].
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 administrators 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.2, FIA_UAU.2]. 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.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(1-2), FCS_CKM.4, FCS_COP.1] between TOE components.
O.PROTECT	*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]. The TOE supports protection of remote management sessions using FIPS validated cryptography (FCS_CKM.1(1), FCS_CKM.4, FCS_COP.1, FTP_TRP.1).

OBJECTIVE	RATIONALE
O.CRYPTO	*The TOE must provide cryptographic functionality and protocols required for the TOE to securely transfer information between distributed portions of the TOE, and must use only cryptographic modules that have been validated to FIPS 140.* The cryptographic SFRs [FCS_CKM.1(1-2), FCS_CKM.4 and FCS_COP.1] describe key generation and cryptographic operation for encryption between end points of the distributed TOE, and between the TOE and the browser used to support remote management sessions. FTP_TRP.1 requires the use of a trusted path for remote management sessions.

Table 33 – Rationale for Mapping of TOE SFRs to Objectives

7.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor, assuming the vendor follows reasonable software engineering practices, and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the TOE environment. While the System may monitor a hostile environment, the servers on which it is located are assumed to provide protection by employing measures appropriate to that environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the protected environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8 TOE Summary Specification

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

The security functions are provided by the TOE to meet the security functional requirements. Each function is described in this section, and the related security functional requirements are given. This serves both to describe the security functions, and to provide a rationale that the security functions satisfy the necessary requirements.

TOE Security Function	SFR ID	Description
Client Threat Prevention	FAM_ACT_(EXT).1	Anti-Malware Actions
	FAM_ALR_(EXT).1	Anti-Malware Alerts
	FAM_SCN_(EXT).1	Anti-Malware Scanning
Client Communication Protection	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
	FMT_MSA.3	Static Attribute Initialization
Client Web Protection	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Client Adaptive Threat Protection	FAM_ACT_(EXT).1	Anti-Malware Actions
	FAM_ALR_(EXT).1	Anti-Malware Alerts
	FAM_SCN_(EXT).1	Anti-Malware Scanning
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.1	User Identification before any action
Security Management	FIA_ATD.1	User Attribute Definition
	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.3	Static Attribute Initialization

TOE Security Function	SFR ID	Description
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
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
Protected System Data Transfer	FCS_CKM.1(1-2)	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
	FPT_ITT.1	TSF Data Transfer Protection

Table 34 – Security Function to SFR mapping

8.1 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, and then takes the actions to protect systems that have been configured. 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: An Administrator configures predefined on-demand scans that Users can run on client devices. The User runs the scan from the ENS Client by 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 an Administrator.

- Scheduled scans: An Administrator configures and schedules on-demand scans to run on client devices 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 the 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 client devices 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

8.1.1 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 are:

- Clean files automatically (after quarantining the original);
- Deny 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;
- Deny 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 8.7). 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 8.8.

8.1.2 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.

8.1.3 Potentially Unwanted Code and Programs

The TOE protects client devices 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.

An 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.

8.1.4 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 device, and sent to the ePO management server. Exploit Prevention protects applications such as Google Chrome, Microsoft Outlook, Outlook Express, Microsoft Word, and MSN Messenger. Exploit Prevention settings can be enabled or disabled by an Administrator on a per policy basis.

8.2 Client Communications Protection

The TOE implements a firewall that scans all incoming and outgoing traffic on managed systems (i.e. client devices). 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.

An 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 – IP;
- Connection –wired, wireless and/or virtual;
- Transport – ICMPv4/v6, TCP or UDP;
- Application – any application as identified by its executable filename.

The firewall uses precedence to apply rules:

1. The firewall applies the rule at the top of the firewall rules list. If the traffic meets this rule's conditions, the firewall allows or blocks the traffic. It does not try to apply any other rules in the list.
2. If the traffic doesn't meet the first rule's conditions, the 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.

An Administrator can group rules according to a work function, service, or application for easier management. The firewall enables a group of rules to be made 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 client devices with multiple network adapters. Connection isolation prevents undesirable traffic from accessing a designated network.

Firewall option settings enable an Administrator to block incoming and outgoing traffic from a network connection that McAfee Global Threat Intelligence (GTI)[6] rates as high risk. Values for the incoming and

[6] 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

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 8.7). Each audit event includes a timestamp, the type of event, and client identity. Event data is sent via McAfee Agent which is protected in accordance with Protected System Data Transfer discussed in section 8.8.

8.3 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 a 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.

An 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.

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 a network when a webpage or file is accessed. The result is a database of reputation scores for IP addresses, domains, specific messages, URLs, and images. The TOE submits fingerprints, or hashes, to the central database server, hosted by McAfee , to identify malware. By submitting these hashes detection may be available sooner than when McAfee publishes the next content file update. McAfee GTI is outside the scope of the TOE, but the interface to it is in scope.

  - 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 is 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 GTI 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 access to the URL or domain name if the McAfee GTI safety rating is “green”, and any other GTI safety ratings allowed by an 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.

8.4 Adaptive Threat Protection

The TOE provides Adaptive Threat Protection (ATP), which examines content and decides what to do based on file reputation, rules, and reputation thresholds. It is designed to **protect** against files with unknown reputations, **detect** malicious patterns, and **correct** false positives.

8.4.1 Protect

The TOE can block or contain files and processes with unknown reputations using the following:

- Reputation**-based file handling** — ATP alerts when an unknown file enters the environment. Instead of sending the file information to McAfee GTI for analysis, ATP can block the file immediately.
- **Dynamic Application Containment** — Allows unknown files to run in a container, limiting the actions they can take. When an organization first uses a file, whose reputation is not known, ATP can run it in a container, monitoring with the ATP and Real Protect scanners. Containment rules define which actions the contained application can't perform. Dynamic Application Containment also contains processes when they load PE files (Portable Executables) and DLLs (Dynamic Link Libraries) that downgrade the process reputation.

File reputation indicates the reputation of a file. Process reputation indicates the reputation of a running process, and can change over time. Pre-execution scanning and reputation sources, such as McAfee GTI, determine the reputation of a file. Multiple factors, including the reputation of the primary executable of the process and its parent, and post-execution scanning, determine the reputation of a process. Post-execution scanning includes Real Protect behavioral scanning, ATP rules and Dynamic Application Containment.

Real Protect can operate both locally on the client and in the McAfee cloud. Client-based Real Protect uses machine learning on the client system to determine whether the file matches known malware. Cloud-based Real Protect collects and sends file attributes and behavioral information to the machine-learning system at McAfee for malware analysis.

8.4.2 Detect

The TOE can detect malicious patterns and malware in memory using these ATP features:

- **Real Protect scanning** — Performs automated behavior analysis. Real Protect inspects suspicious files and activities on a client system, and detects malicious patterns using machine-learning techniques. Real Protect client-based and cloud-based scans include DLL scanning to keep trusted processes from loading untrusted PE and DLL files.
- **Credential Theft Protection** — Protects against credential theft. The credential theft protection technology is designed to stop attacks specifically targeting the Local Security Authority Subsystem Service (LSASS).
- **Enhanced script scanning** — Integration with AMSI (Antimalware Scan Interface) provides enhanced scanning for threats in non-browser-based scripts, such as PowerShell, JavaScript, and VBScript.
- **ATP rules** — Determines what processes can and can't do within a specific context, and can change reputation based on the context and behavior.

8.4.3 Correct

Clean files and eliminate false positives using these ATP features:

- **File cleaning** — ATP can clean files when the file reputation reaches a specified threshold.

  - **Enhanced remediation** — If a process is unknown, enhanced remediation monitors its behavior; and logs all files that the process creates, and, optionally, all files that the process changes or deletes. If a monitored process exhibits malicious behavior, enhanced remediation stops the process, its children, and ancestors, and rolls back the changes that it made, restoring the system as close as possible to its original state before the process ran.

  - **Custom file exclusions** — If a custom file is trusted, but has a default reputation of malicious, it is blocked. It can be excluded from scanning, or the file's reputation can be changed to trusted, allowing it to run in the organization without requesting an updated DAT file from McAfee.

  - **False positive mitigation**: If ATP gets a file reputation above a certain threshold from McAfee GTI, it can automatically override a false positive detection by Adaptive Threat Protection or Threat prevention.
  - **Adaptive Threat Protection rules** — McAfee delivers updates to rules in AMCore content every month.

  - **ePO Dashboards and reports** — Show activity and detections, which can be used to tune Adaptive Threat Protection settings. (Managed systems)

8.4.4 ATP Operation

Adaptive Threat Protection uses the local reputation cache, McAfee GTI and McAfee Real Protect for reputation information to determine how to handle files and processes on the client system. ATP uses rules to target live-off-the-land and fileless attacks, and enhanced remediation to roll back changes if attacks occur.

1. An Administrator configures ATP settings in ePO, and enforces them to the client system.

2. A User executes a file on the client system. Adaptive Threat Protection checks the local reputation cache for the file.

3. If the file is not in the local reputation cache, ATP queries McAfee GTI for the reputation.

4. Depending on the file's reputation and ATP settings:
   - The file is allowed to run;
   - The file is cleaned;
   - The file is blocked;
   - The file is allowed to run in a container;
   - The User is prompted for the action to take.

For a process with a known trusted reputation, ATP rules determine the appropriate actions for the process. ATP monitors the process, its children, and ancestors for suspicious behavior, which can indicate a fileless attack, and blocks the process if needed. If the process reputation is unknown (50 or lower), enhanced remediation backs up changes, and rolls back if the process exhibits malicious behavior. If the file is not in the local reputation cache, ATP queries McAfee GTI for the reputation, or for a process can send attributes and behavioral information to McAfee Real Protect for analysis.

5. ATP logs the details then generates and sends an event to ePO.

AMCore content files include updates to scanners, engines, and rules that Adaptive Threat Protection uses to dynamically compute the reputation and acceptable behavior of files and processes on client systems. McAfee adds rules to the content files. With the rules, content files include information about preventing malware behaviors. New threats appear, and McAfee releases updated content files, regularly.

8.5 Identification & Authentication

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

Administrators must log in to the TOE with a valid user name and password, supplied via the management console, before any access is granted to TOE functions or data. When the credentials are presented by the Administrator, the TOE determines if the role is defined and their status is active.

If the Administrator's password is successfully authenticated, the TOE grants access to the ePO management interface, and therefore to the TOE functionality. If the authentication is not successful, the login screen 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 Administrator logs off). If the attributes for a logged in Administrator are changed, those changes will not be bound to a session until their next login.

8.6 Management

The TOE's management security function provides administrator support functionality that enables an Administrator 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. **Administrator accounts[7] -** Each Administrator authorized for login to the TOE must be defined on the ePO management console. ePO maintains two types of roles: "Administrator" and users with selected permissions. 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 any users who are not Administrators (Users assigned to the "administrator" permission set). Administrators are granted all permissions. Only Administrators may perform ePO user account management functions (create, view, modify, and delete.
2. **Permission Sets** - 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.
3. **Audit Log** - 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.
4. **Event Log** - The Threat Event Log contains all threat events that ePO receives from managed systems, based on the policies configured for each of the 4 modules. Threat Event Log information can be viewed by an authorized Administrator. The Event Log entries are automatically purged based upon a configured age. An authorized may issue a command through the ePO management console to purge all event records older than a specified time.
5. **System Tree access** - 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.
6. **Queries and Reports** - Authorized users may create, view, modify, use and delete queries based upon their permissions.
7. **Dashboards** - User-specific dashboards may be configured to display data of interest to each user.
8. **Endpoint Security Common Module** - 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.
9. **Client Threat Prevention Policy** - Authorized users may create, view, modify, use and delete Client Threat Prevention policies and task settings.
10. **Client Communications Protection Policy** - Authorized users may create, view, modify, use and delete Client Communication Protection policies.
11. **Client Web Protection Policy** - Authorized Administrators may create, view, modify, use and delete Client Web Protection policies and task settings.

[7] Within ePO documentation the term "Administrator" is used to mean an ePO user with the Administrator permission set. This ST generally uses the term Administrator to refer to all ePO users, to distinguish those managing the TOE from users on client devices. This ST uses "Authorised Administrator" to refer to an ePO Administrator, or an ePO user granted the appropriate permission set.

12. **Adaptive Threat Protection Policy** - Authorized Administrators may create, view, modify, use and Adaptive Threat Protection policies and task settings.

8.7 Audit

8.7.1 Audit and Server Task Logs

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

1. **Audit Log** - Captures all Administrator actions and stores them on the ePO server's external database (provided by the IT environment).
2. **Server Task Log** - 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 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 as 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 ePO user name of the person 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 authorized Administrator. The Audit Log entries are automatically purged based upon a configured age. An authorized Administrator may issue a command through the ePO management console 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.

8.7.2 Threat Event Log

The Threat Event Log contains all threat events that ePO receives from managed systems, including events from the ENS Client, which comprises of the Threat Prevention, Firewall, Web Protection, and Adaptive Threat Protection modules. Events are generate based on the policies configured for each of the 4 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 authorized Administrator.

The Event Log entries are automatically purged based upon a configured age. An authorized Administrator may issue a command through the ePO management console to purge all event records older than a specified time. Protection of the Threat Event Log is provided by the IT environment.

8.8 Protected System Data Transfer

This section covers only external protected data transfer using externally visible encryption services provided by the TOE.

8.8.1 ePO to MA

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 1.2. In the evaluated configuration the available ciphers for this communication are limited by configuration to ECDHE_RSA _AES256_GCM_SHA384 and ECDHE_RSA _AES128_GCM_SHA256.

In FIPS mode, ePO uses OpenSSL 1.0.2za with McAfee OpenSSL FIPS Object Module v1.0.2c (FIPS 140-2 certificate #2969) for TLS 1.2. This is implemented using the Apache Server. McAfee Agent uses OpenSSL

1.0.2za with McAfee OpenSSL FIPS Object Module v1.0.2c (FIPS 140-2 certificate #2969, CAVP certificate number A848) to provide cryptographic services for this link.

8.8.2 ePO to remote management workstation

The TOE supports secure communications between ePO and remote management workstations. Messages are transferred via HTTPS. The TOE protects these transmissions between the ePO and the remote management workstations from disclosure and modification by encrypting the transmissions under TLS 1.2. The connection will be instigated from a remote management workstation (outside the scope of the TOE) and the TOE provides support for the use of the following ciphers.

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,
TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

ePO uses Bouncy Castle FIPS Java API 1.0.2.1 (FIPS 140-2 certificate #3514, CAVP certificate number C2204) for TLS 1.2.

8.8.3 ENS client to Real Protect service

The ENS Client sends data concerning processes to the McAfee Real Protect service for analysis to determine whether the process exhibits malicious behavior. This communication uses OpenSSL 1.0.2za with McAfee OpenSSL FIPS Object Module v1.0.2c (FIPS 140-2 certificate #2969, CAVP certificate number A848) for TLS 1.2.

8.8.4 ENS client verification of AMCore content

Updates to AMCore content are downloaded from McAfee by ePO. These are distributed to ENS Clients using MA. The integrity of the file content is verified by MA through verification of the RSA 2048-bit signature, using OpenSSL 1.0.2za with McAfee OpenSSL FIPS Object Module v1.0.2c (FIPS 140-2 certificate #2969, CAVP certificate number A848).

8.8.5 Vendor affirmation

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. ePO and MA are tested by McAfee on all supported platforms.

8.9 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	Client Adaptive Threat Protection	Identification & Authentication	Security 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	✓			✓				
FAM_SCN_(EXT).1	✓			✓				
FCS_CKM.1(1-2)								✓
FCS_CKM.4								✓
FCS_COP.1								✓
FDP_IFC.1		✓	✓					
FDP_IFF.1		✓	✓					
FIA_ATD.1						✓		
FIA_UAU.2					✓			
FIA_UID.2					✓			
FMT_MOF.1						✓		
FMT_MSA.3		✓				✓		
FMT_MTD.1						✓		
FMT_SMF.1						✓		
FMT_SMR.1						✓		
FPT_ITT.1								✓

Table 35 – 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.

SFR	SF AND RATIONALE
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, based on known signatures, and prevents them from executing on managed systems. Actions are configured by the Administrator to clean, quarantine or delete file-based malware. **Client Adaptive Threat Protection** - The TOE detects memory and file-based malware, based on file reputation, and prevents them from executing on managed systems. Actions are configured by the Administrator to clean, quarantine or delete file-based malware.
FAM_ALR_(EXT).1	**Client Threat Prevention** – The TOE provides alert notification of detected malware to the User and sends an event to the ePO server managed by the Administrator. **Client Adaptive Threat Protection** – – The TOE provides alert notification of detected malware to the User and sends an event to the ePO server managed by the Administrator.
FAM_SCN_(EXT).1	**Client Threat Prevention** – The TOE provides real-time (on-access) and scheduled (on-demand) malware scanning of the client device memory space and files against known signatures. On-demand scans are scheduled by the Administrator, or may be invoked manually by the User. **Client Adaptive Threat Protection** - The TOE provides real-time (on-access) and scheduled (on-demand) malware scanning of the client device memory space and files using reputation and dynamic access containment. On-demand scans are scheduled by the Administrator, or may be invoked manually by the User.
FCS_CKM.1(1-2)	**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.

SFR	SF AND RATIONALE
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 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 Users.
FIA_ATD.1	**Management –** User security attributes are associated with the user account via User Account management.
FIA_UAU.2	**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.2	**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 behavior of the Client Threat Prevention, Client Communications Protection, and Client Web Protection security functions by configuring the policies and tasks for the managed systems.
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.

SFR	SF AND RATIONALE
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 36 – SFR to TSF Rationale