Security Target

Symantec™ Endpoint Protection Version 12.1.2

Document Version 0.8

February 13, 2013

Prepared For:

Symantec Corporation

350 Ellis Street

Mountain View, CA 94043

www.symantec.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Revision History

Version	Date	Description	Author
0.4	12/22/11	Update in response to ORs of 12/16/11 which included a request for a revision history.	Sue Toorans (Apex)
0.5	1/13/12	Respond to ORs filed on behalf of the certifier on 1/6/12	Sue Toorans (Apex)
0.6	3/26/12	Respond to ORs	Sue Toorans (Apex)
0.7	6/20/12	Update due to AGD CR responses	Sue Toorans (Apex)
0.8	2/13/13	Updated SEP version to 12.1.2	Wes Higaki (Apex)

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Endpoint Protection Version 12.1.2. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

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: Symantec™ Endpoint Protection Version 12.1.2
ST Revision	0.6
ST Publication Date	March 26, 2012
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	Symantec™ Endpoint Protection Version 12.1.2

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

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

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets and a change in text color, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized* 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.

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[1] describes the terms and acronyms used in this document:

TERM	DEFINITION
AVPP	U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments, version 1.2, dated 25 July 2007
CC	Common Criteria version 3.1 (ISO/IEC 15408)
EAL	Evaluation Assurance Level
FTP	File Transfer Protocol
OSP	Organizational Security Policy
SFR	Security Functional Requirement
SFP	Security Function Policy
SOF	Strength Of Function
ST	Security Target
TCP	Transmission Control Protocol

[1] Derived from the IDSPP

TERM	DEFINITION
TOE	Target Of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

The Symantec Endpoint Protection Version 12.1.2 delivers a comprehensive antivirus/endpoint security solution with a single agent and a single, centralized management console. It has a rules-based firewall engine, browser protection and Generic Exploit Blocking (GE) shields systems from drive-by downloads and from network based attacks. It protects against viruses, worms, Trojans, spyware, bots, zero-day threats and root kits.

Endpoint Protection Version 12.1.2 may hereafter also be referred to as the TOE in this document.

1.7 TOE Description

Symantec Endpoint Protection Version 12.1.2 combines Symantec AntiVirus with advanced threat prevention to deliver a defense against malware for laptops, desktops, and servers. It provides protection against even the most sophisticated attacks that evade traditional security measures, such as rootkits, zero-day attacks, and mutating spyware.

The product type of the Target of Evaluation (TOE) described in this Security Target (ST) is an antivirus application running on workstations (e.g., desktops and laptops), along with a management component running on a central server to control and monitor execution of the antivirus application.

The evaluated features of Symantec Endpoint Protection Version 12.1.2 include the following components:

- Symantec Endpoint Protection Client – protects servers, desktops, and laptops systems
- Symantec Endpoint Protection Manager (and management console) – executes management operations

1.7.1 Physical Boundary

The TOE is a software TOE and is defined as the Endpoint Protection Version 12.1.2 and includes the RSAENH cryptographic module from the Microsoft Windows operating systems. In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	Endpoint Protection Version 12.1.2
IT Environment	See Section 1.7.2 – Hardware and Software Supplied by the IT Environment

Table 3 – Evaluated Configuration for the TOE

The TOE boundary is shown below:

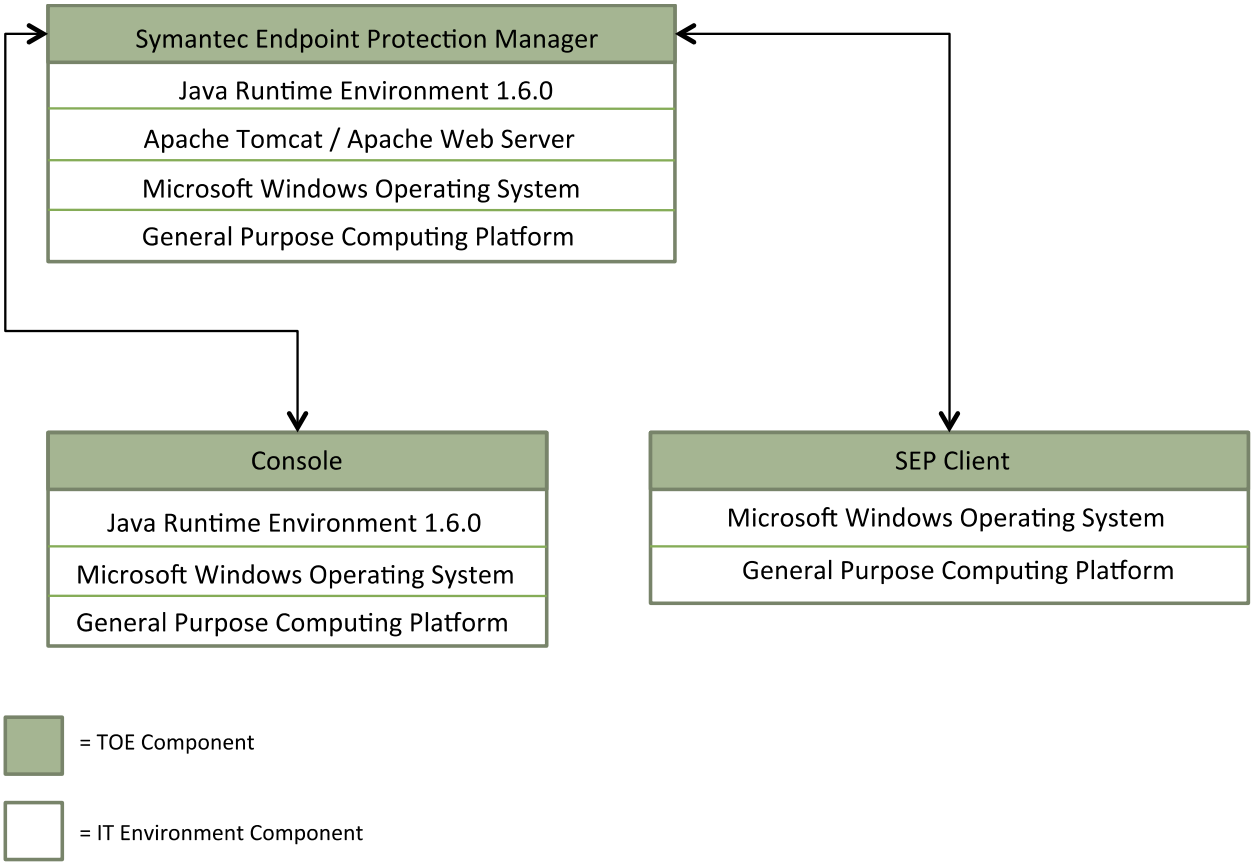

Figure 1 – TOE Boundary

At a high level, the TOE interfaces include the following:

1. Software interfaces for connection to internal TOE components and external IT products.
2. Software interfaces to receive and process traffic from internal TOE components and external IT products.
3. Management interface to handle administrative actions.

The TOE's evaluated configuration requires one or more instances of a SEP Client, one instance of a SEP Manager, and one or more instances of a workstation for management via Console. Communications between the components are protected via SSL tunnel, provided by the Operational Environment.

1.7.2 Hardware and Software Supplied by the IT Environment

The Symantec Endpoint Protection Manager (and management console) system requirements are as follows:

- 32-bit processor: 1-GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended)
- 64-bit processor: 2-GHz Pentium 4 with x86-64 support or equivalent minimum Intel Itanium IA-64 is not supported.
- Operating systems: Windows XP (32-bit, SP-3 or higher, 64-bit, all SPs), Windows Server 2003 (32-bit, 64-bit, R2, SP1 or later), Windows Server 2008 (32-bit, 64-bit).
- Windows Vista (32-bit, 64-bit) is not officially supported.
- RAM memory: 1 GB of RAM minimum (2 GB of RAM recommended)
- Hard disk: 4 GB or more free space
- Java Runtime Environment 1.6.0.u24
- Apache Tomcat 6.0.32
- Apache HTTP Server 2.2.16

The client system requirements are as follows:

- 32-bit processor: for Windows operating systems, 1-GHz Intel Pentium III or equivalent minimum (Intel Pentium 4 or equivalent recommended); for Mac operating systems, Intel Core Solo, Intel Core Duo
- 64-bit processor: for Windows operating systems, 2-GHz Pentium 4 with x86-64 support or equivalent minimum; for Mac operating systems, Intel Core 2 Duo, Intel Quad-Core Xeon
- Intel Itanium IA-64 is not supported.
- PowerPC is not supported (32-bit or 64-bit).
- Operating systems: Windows XP (32-bit, SP-3 or later, 64-bit, all SPs), Windows XP Embedded (SP-3 or later), Windows Vista (32-bit, 64-bit), Windows 7 (32-bit, 64-bit), Windows 7 Embedded, Windows Server 2003 (32-bit, 64-bit, R2, SP-2 or later), Windows Server 2008 (32-bit, 64-bit), Windows Small Business Server 2011 (64-bit), or Windows Essential Business Server 2008 (64-bit), Mac OS X 10.5 or 10.6 (32-bit, 64-bit only), Mac OS X Server 10.5 or 10.6 (32-bit, 64-bit)
- RAM memory: 512 MB of RAM minimum (1 GB of RAM recommended)
- Hard disk: 900 MB or more free space
- Browser: Internet Explorer 7, 8 or 9. Required to install the client by using Remote Push (Windows clients only). Mozilla Firefox 3.6 or 4.0.

The Symantec Endpoint Protection Manager includes an embedded database. Alternatively, the following version of Microsoft SQL Server can be used:

- SQL Server 2008, SP-2 or later

1.7.3 Logical Boundary

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

TSF	DESCRIPTION
Antivirus	The TOE is designed to help prevent memory-based and file-based viruses. The TOE can be configured to perform various actions if a virus is detected.
Audit	The audit services include details on actions taken when a virus is detected as well as administrative actions performed while accessing the TOE. The TOE generates audits when security-relevant events occur, stores the audit information on the local system, transmits the audit information to a central management system, generates alarms for designated events, and provides a means for audit review. Protection of audit data in the audit trail involves the TOE and the Operating System (OS). The TOE controls the insertion of audit events into the audit log and the deletion of audit events from the audit log. The OS provides basic file protection services for the audit log.
Cryptographic Operations	The TOE implements FIPS-approved cryptographic functionality to verify the integrity of the signature files download from Symantec Security Response / Live Update.
Management	The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to Antivirus and Audit.

Table 4 – Logical Boundary Descriptions

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 extended and Part 3 conformant at Evaluation Assurance Level 2 augmented with ALC_FLR.2.

2.2 Protection Profile Conformance Claim

The TOE claims demonstrable conformance to the U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness Environments, version 1.2, dated 25 July 2007.

3 Security Problem Definition

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

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

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

3.1 Threats

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

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.ACCIDENTAL_ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.AUDIT_ COMPROMISE	A user or process may gain unauthorized access to the audit trail and cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a security relevant event.
T.AUDFUL	An unauthorized user may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being discovered thereby causing potential security vulnerabilities.

THREAT	DESCRIPTION
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to scan files or process administrator requests.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted)
T.UNATTENDED_SESSION	A user may gain unauthorized access to an unattended session.
T.UNIDENTIFIED_ACTIONS	Failure of the authorized administrator to identify and act upon unauthorized actions may occur.
T.VIRUS	A malicious agent may attempt to introduce a virus onto a workstation via network traffic or removable media to compromise data on that workstation, or use that workstation to attack additional systems.

Table 5 – Threats Addressed by the TOE

3.2 Organizational Security Policies

The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION
P.ACCESS_BANNER	The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e. encryption, decryption, signature, hashing, key exchange, and random number generation services)
P.MANUAL_SCAN	The authorized users of the workstations shall initiate manual anti-virus scans of removable media (e.g., floppy disks, CDs) introduced into the workstation before accessing any data on the removable media.
P.ROLES	The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

Table 6 – 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.AUDIT_ALARM	The TOE receives alarms from the IT Environment to signal when audit logs are nearing capacity.
A.AUDIT_BACKUP	Administrators will back up audit files and monitor disk usage to ensure audit information is not lost.
A.DOMAIN_SEPARATION	The IT environment will provide a separate domain for the TOE's operation.
A.NO_BYPASS	The IT environment will ensure the TSF cannot be bypassed.
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrative guidance.
A.PHYSICAL	It is assumed that the appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
A.SECURE_COMMS	It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
A.SECURE_UPDATES	Administrators will implement secure mechanisms for receiving and validating updated signature files from the Anti-Virus vendors, and for distributing the updates to the central management systems.

Table 7 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ADMIN_GUIDANCE	The TOE will provide administrators with the necessary information for secure management.
O.ADMIN_ROLE	The TOE will provide an authorized administrator role to isolate administrative actions.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security-relevant events.
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information.
O.AUDIT_REVIEW	The TOE will provide the capability to selectively view audit information.
O.CONFIGURATION_IDENTIFICATION	The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified.
O.CORRECT_TSF_OPERATION	The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.
O.CRYPTOGRAPHY	The TOE shall use NIST FIPS 140-2 cryptographic services.
O.DOCUMENTED_DESIGN	The design of the TOE is adequately and accurately documented.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE.
O.PARTIAL_FUNCTIONAL_TEST	The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.
O.PARTIAL_SELF_PROTECTION	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.
O.VIRUS	The TOE will detect and take action against known viruses introduced to the workstation via network traffic or removable media.
O.VULNERABILITY_ANALYSIS	The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.

Table 8 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION

OBJECTIVE	DESCRIPTION
OE.AUDIT_ALARM	The IT Environment will provide alarms to authorized administrators to signal when audit logs are nearing capacity.
OE.AUDIT_BACKUP	Audit log files are backed up and can be restored, and audit log files will not run out of disk space.
OE.AUDIT_STORAGE	The IT Environment will provide a means for secure storage of the TOE audit log files.
OE.DISPLAY_BANNER	The IT environment will display an advisory warning regarding the use of the system.
OE.DOMAIN_SEPARATION	The IT environment will provide an isolated domain for the execution of the TOE.
OE.NO_BYPASS	The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.
OE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.PHYSICAL	Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
OE.RESIDUAL_INFORMATION	The IT environment will ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated.
OE.SECURE_COMMS	The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
OE.SECURE_UPDATES	Enterprises using the TOE shall ensure that signature file updates are received from the vendor 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.TIME_STAMPS	The IT Environment will provide reliable time stamps.
OE.TOE_ACCESS	The IT environment will provide mechanisms that control a user's logical access to the TOE.

Table 9 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

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

	A.AUDIT_BACKUP	A.DOMAIN_SEPARATION	A.NO_BYPASS	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	A.SECURE_UPDATES	T.ACCIDENTAL_ADMIN_ERROR	T.AUDIT_ COMPROMISE	T.AUDITFUL	T.MASQUERADE	T.POOR_DESIGN	T.POOR_IMPLEMENTATION	T.POOR_TEST	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNATTENDED_SESSION	T.UNIDENTIFIED_ACTIONS	T.VIRUS	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.CRYPTOGRAPHY	P.MANUAL_SCAN	P.ROLES
O.ADMIN_GUIDANCE								✓																
O.ADMIN_ROLE																								✓
O.AUDIT_GENERATION																		✓			✓			
O.AUDIT_PROTECT									✓															
O.AUDIT_REVIEW																		✓						
O.CONFIGURATION_IDENTIFICATION												✓	✓											
O.CORRECT_TSF_OPERATION														✓		✓								
O.CRYPTOGRAPHY																						✓		
O.DOCUMENTED_DESIGN												✓		✓										
O.MANAGE																✓							✓	
O.PARTIAL_FUNCTIONAL_TEST													✓	✓										
O.PARTIAL_SELF_PROTECTION									✓							✓								
O.VIRUS																			✓				✓	
O.VULNERABILITY_ANALYSIS												✓	✓	✓										
OE.AUDIT_ALARM										✓														
OE.AUDIT_BACKUP	✓																							
OE.AUDIT_STORAGE									✓															
OE.DISPLAY_BANNER																				✓				
OE.DOMAIN_SEPARATION		✓							✓							✓								
OE.NO_BYPASS			✓						✓							✓								
OE.NO_EVIL				✓																				
OE.PHYSICAL					✓																			
OE.RESIDUAL_INFORMATION									✓						✓	✓								

	A.AUDIT_BACKUP	A.DOMAIN_SEPARATION	A.NO_BYPASS	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	A.SECURE_UPDATES	T.ACCIDENTAL_ADMIN_ERROR	T.AUDIT_ COMPROMISE	T.AUDITFUL	T.MASQUERADE	T.POOR_DESIGN	T.POOR_IMPLEMENTATION	T.POOR_TEST	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNATTENDED_SESSION	T.UNIDENTIFIED_ACTIONS	T.VIRUS	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.CRYPTOGRAPHY	P.MANUAL_SCAN	P.ROLES
OE.SECURE_COMMS						✓																		
OE.SECURE_UPDATES							✓																	
OE.TIME_STAMPS																		✓			✓			
OE.TOE_ACCESS											✓						✓				✓			

Table 10 – 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	ADDRESSED BY	RATIONALE
T.ACCIDENTAL_ADMIN_ ERROR: An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	O.ADMIN_GUIDANCE: The TOE will provide administrators with the necessary information for secure management.	O.ADMIN_GUIDANCE helps to mitigate this threat by ensuring the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner. Having this guidance helps to reduce the mistakes that an administrator might make that could cause the TOE to be configured in a way that is insecure.
T.AUDIT_ COMPROMISE: A user or process may cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	O.AUDIT_PROTECT: The TOE will provide the capability to protect audit information. OE.AUDIT_STORAGE: The IT environment will contain mechanisms to provide secure storage and management of the audit log. OE.RESIDUAL_ INFORMATION: The TOE will ensure that any	O.AUDIT_PROTECT contributes to mitigating this threat by controlling access to the individual audit log records. No one is allowed to modify audit records, the System Administrator is the only one allowed to delete audit records, and the TOE has the capability to prevent auditable actions from occurring if the audit trail is full. OE.AUDIT_STORAGE contributes to

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
	information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. O.PARTIAL_SELF_PROTECTION: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces. OE.DOMAIN_SEPARATION: The IT environment will provide an isolated domain for the execution of the TOE. OE.NO_BYPASS: The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	mitigating this threat by restricting the ability of users in the IT Environment to access the audit log file. OE.RESIDUAL_INFORMATION prevents a user not authorized to read the audit trail from access to audit information that might otherwise be persistent in a resource used by the TOE (e.g., memory). By preventing residual information in a resource, audit information will not become available to any user or process except those explicitly authorized for that data. O.PARTIAL_SELF_PROTECTION contributes to countering this threat by ensuring that the TSF can protect itself from users via its own interfaces. This limits access to the audit information to the functions defined for the specified roles. OE.DOMAIN_SEPARATION contributes to countering this threat by ensuring that the TSF is protected from users through mechanisms other than its own interfaces. If the OS could not maintain and control a domain of execution for the TSF separate from other processes, the TSF could not be trusted to control access to the resources under its control, which includes the audit trail which are always invoked is also critical to the migration of this threat. OE.NO_BYPASS ensures audit compromise can not occur simply by bypassing the TSF.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE

T.AUDITFUL:
An unauthorized user may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
	OE.AUDIT_ALARM:
	The IT Environment will provide alarms to authorized administrators to signal when audit logs are nearing capacity.
		OE.AUDIT_ALARM mitigates this threat in that the Operating System provides for the following alarms to meet this requirement:
		1. When free disk space reaches 200 megabytes (MB), the user will receive the following message for 10 seconds, once per session:
		`You are running out of disk space on [drive]. To free space on this drive by deleting old or unnecessary files, click here.`
		2. When free disk space reaches 80 MB, the user will receive the following message for 30 seconds, every four hours, twice per session:
		`You are running very low on disk space on [drive]. To free space on this drive by deleting old or unnecessary files, click here.`
		3. When free disk reaches 50 MB, the user will receive the following message for 30 seconds, every five minutes, until free space is above 50 MB:
		`You are running very low on disk`

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
		space on [drive]. To free space on this drive by deleting old or unnecessary files, click here
T.MASQUERADE: A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	OE.TOE_ACCESS: The IT Environment will provide mechanisms that control a user's logical access to the TOE.	OE.TOE_ACCESS mitigates this threat by requiring authorized administrators and workstation users to be identified and authenticated, a necessary step in controlling the logical access to the TOE and its resources by constraining how and when users can access the TOE. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.
T.POOR_DESIGN: Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.	O.CONFIGURATION_IDENTIFICATION: The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified. O.DOCUMENTED_DESIGN: The design of the TOE is adequately and accurately documented. O.VULNERABILITY_ANALYSIS: The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design. O.DOCUMENTED_DESIGN ensures that the design of the TOE is documented, permitting detailed review by evaluators. O.VULNERABILITY_ANALYSIS_TEST ensures that the design of the TOE is analyzed for design flaws.
T.POOR_IMPLEMENTATION: Unintentional errors in	O.CONFIGURATION_IDENTIFICATION: The configuration of the TOE is fully	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.	identified in a manner that will allow implementation errors to be identified. O.PARTIAL_FUNCTIONAL_TESTING: The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements. O.VULNERABILITY_ANALYSIS: The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	to provide control of the changes made to the TOE's implementation. O.PARTIAL_FUNCTIONAL_TESTING increases the likelihood that any errors that do exist in the implementation will be discovered through testing. O.VULNERABILITY_ANALYSIS_TEST helps reduce errors in the implementation that may not be discovered during functional testing. Ambiguous design documentation and the fact that exhaustive testing of the external interfaces is not required may leave bugs in the implementation undiscovered in functional testing.
T.POOR_TEST: Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.	O.DOCUMENTED_DESIGN The design of the TOE will be adequately and accurately documented. O.PARTIAL_FUNCTIONAL_TESTING: The TOE will undergo some security functional testing that demonstrates the TSF satisfies the security functional requirements. O.CORRECT_TSF_OPERATION: The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site. O.VULNERABILITY_ANALYSIS: The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.DOCUMENTED_DESIGN helps to ensure that the TOE's documented design satisfies the security functional requirements. In order to ensure the TOE's design is correctly realized in its implementation, the appropriate level of functional testing of the TOE's security mechanisms must be performed during the evaluation of the TOE. O.PARTIAL_FUNCTIONAL_TESTING increases the likelihood that any errors that do exist in the implementation will be discovered through testing. O.CORRECT_TSF_OPERATION provides assurance that the TSF continues to operate as expected in the field. O.VULNERABILITY_ANALYSIS_TEST addresses this concern by requiring a vulnerability analysis be

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
		performed in conjunction with testing that goes beyond functional testing. This objective provides a measure of confidence that the TOE does not contain security flaws that may not be identified through functional testing.
T.RESIDUAL_DATA: A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to scan files or process administrator requests.	OE.RESIDUAL_INFORMATION: The IT Environment will ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated.	OE.RESIDUAL_INFORMATION counters this threat by ensuring that memory contents are not persistent when resources are released by the TOE and allocated to another user/process.
T.TSF_COMPROMISE: A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).	OE.RESIDUAL_INFORMATION: The IT Environment will ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated. O.PARTIAL_SELF_PROTECTION: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces. OE.DOMAIN_SEPARATION: The IT environment will provide an isolated domain for the execution of the TOE. O.MANAGE: The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE. O.CORRECT_TSF_OPERATION: The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	OE.RESIDUAL_INFORMATION is necessary to mitigate this threat, because even if the security mechanisms do not allow a user to explicitly view TSF data, if TSF data were to inappropriately reside in a resource that was made available to a user, that user would be able to inappropriately view the TSF data. O.PARTIAL_SELF_PROTECTION is necessary so that the TSF protects itself and its resources from inappropriate access through its own interfaces. OE.DOMAIN_SEPARATION is necessary so that the TSF is protected from other processes executing on the workstation. O.MANAGE is necessary because an access control policy is not specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions. O.CORRECT_TSF_OPERATION

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
	OE.NO_BYPASS: The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	provides assurance that the TSF continues to operate as expected in the field. OE.NO_BYPASS ensures TSF compromise can not occur simply by bypassing the TSF.
T.UNATTENDED_ SESSION: A user may gain unauthorized access to an unattended session.	OE.TOE_ACCESS: The IT environment will provide mechanisms that control a user's logical access to the TOE.	OE.TOE_ACCESS helps to mitigate this threat by including mechanisms that place controls on user's sessions. Locking a session reduces the opportunity of someone gaining unauthorized access to the session when the console is unattended.
T.UNIDENTIFIED_ACTIONS: The administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.	O.AUDIT_REVIEW: The TOE will provide the capability to selectively view audit information. O.AUDIT_GENERATION: The TOE will provide the capability to detect and create records of security relevant events associated with users. OE.TIME_STAMPS: The IT environment shall provide reliable time stamps for accountability and protocol purposes.	O.AUDIT_REVIEW helps to mitigate this threat by providing the Security Administrator with a required minimum set of configurable audit events that could indicate a potential security violation. By configuring these auditable events, the TOE monitors the occurrences of these events (e.g. set number of authentication failures, set number of information policy flow failures, self-test failures, etc.). O.AUDIT_GENERATION helps to mitigate this threat by recording actions for later review. OE.TIME_STAMPS helps to mitigate this threat by ensuring that audit records have correct timestamps.
T.VIRUS: A malicious agent may attempt to introduce a virus onto a workstation via network traffic or removable media to compromise data on that workstation, or use that workstation to attack	O.VIRUS: The TOE will detect and take action against known viruses introduced to the workstation via network traffic or removable media.	O.VIRUS mitigates this threat by providing mechanisms to prevent a virus from being introduced onto a workstation.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
additional systems.		
P.ACCESS_BANNER: The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	OE.DISPLAY_BANNER: The IT Environment will display an advisory warning regarding use of the system.	OE.DISPLAY_BANNER satisfies this policy by ensuring that the system displays a banner that provides all authorized users with a warning about the unauthorized use of the system.
P.ACCOUNTABILITY: The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.AUDIT_GENERATION: The TOE will provide the capability to detect and create records of security-relevant events associated with users. OE.TIME_STAMPS: The IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps. OE.TOE_ACCESS: The TOE will provide mechanisms that control a user's logical access to the TOE.	O.AUDIT_GENERATION addresses this policy by recording security-relevant events. The administrator's ID is recorded when any security relevant change is made to the TOE. OE.TIME_STAMPS plays a role in supporting this policy by requiring the IT environment to provide a reliable time stamp. The audit mechanism is required to include the current date and time in each audit record. OE. TOE_ACCESS supports this policy by requiring the IT environment to identify and authenticate all authorized administrators and workstation users prior to allowing any TOE access. While the user ID of these users can be assured, since they are authenticated, this PP allows unauthenticated users to access the TOE and the identity is then a presumed network identifier (e.g., IP address).
P.CRYPTOGRAPHY: Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction,	O.CRYPTOGRAPHY: The TOE shall use NIST FIPS 140-2 validated cryptographic services.	O.CRYPTOGRAPHY requires that cryptographic services conform to the policy by mandating FIPS 140-2 validation.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).		
P.MANUAL_SCAN: The authorized users of the workstations shall initiate manual anti-virus scans of removable media (e.g., floppy disks, CDs) introduced into the workstation before accessing any data on that removable media.	O.VIRUS: The TOE will detect and take action against known viruses introduced to the workstation via network traffic or removable media. O.MANAGE: The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE.	O.VIRUS requires the TOE to provide the capability to perform manual scans of removable media. O.MANAGE provides the workstation user with the ability to invoke the manual scan capability.
P.ROLES: The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.	O.ADMIN_ROLE: The TOE will provide an authorized administrator role to isolate administrative actions.	O.ADMIN_ROLE addresses this policy by requiring the TOE to support an administrator role, and restrict specific actions to that role.
A.AUDIT_BACKUP: Administrators will back up the audit files and monitor disk usage to ensure audit information is not lost.	OE.AUDIT_BACKUP: Audit log files are backed up and can be restored, and audit log files will not run out of disk space.	OE.AUDIT_BACKUP addresses the assumption by requiring the audit log files to be backed up, and by requiring monitoring of disk space usage to ensure space is available.
A.DOMAIN_SEPARATION: The IT environment will provide a separate domain for the TOE's operation.	OE.DOMAIN_SEPARATION: The IT environment will provide an isolated domain for the execution of the TOE.	OE.DOMAIN_SEPARATION restates the assumption. The workstation OS and hardware provide domain separation between processes.
A.NO_BYPASS: The IT environment will ensure the TSF cannot be bypassed.	OE.NO_BYPASS: The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	OE.NO_BYPASS restates the assumption. The workstation OS ensures the TSF is invoked.
A.NO_EVIL: Administrators are non-hostile, appropriately	OE.NO_EVIL: Sites using the TOE shall ensure that authorized administrators are non-	OE.NO_EVIL restates the assumption.

THREATS, POLICIES, AND ASSUMPTIONS	ADDRESSED BY	RATIONALE
trained, and follow all administrator guidance.	hostile, appropriately trained and follow all administrator guidance.	
A.PHYSICAL: It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.	OE.PHYSICAL: Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.	OE.PHYSICAL restates the assumption.
A.SECURE_COMMS: It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.	OE.SECURE_COMMS: The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.	OE.SECURE_COMMS restates the assumption. The workstation OS will provide a secure line of communication for the TOE.
A.SECURE_UPDATES: Administrators will implement secure mechanisms for receiving and validating updated signature files from the Anti-Virus vendors, and for distributing the updates to the central management systems.	OE.SECURE_UPDATES: Enterprises using the TOE shall ensure that signature file updates are received from the vendor via secure mechanisms, the updates are validated before being used, and the updates are distributed to central management systems within the Enterprise via secure mechanisms.	OE.SECURE_UPDATES restates the assumption. Administrators use secure mechanisms to receive and validate the updates from the vendor, then use secure mechanisms to distribute the updates to the central management systems.

Table 11 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

5.1 Anti-Virus (FAV) Class of SFRs

All of the components in this section are taken from 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 is taken from the Anti-Virus PP to specifically address the detection and response capabilities of anti-virus products. The purpose of this class of requirements is to address the unique nature of anti-virus products and provide for requirements about detecting and responding to viruses on protected IT resources. These SFRs are explicitly defined as there are no suitable components, families, or classes in Part 2 of the Common Criteria that meet the TSF.

5.1.1 FAV_ACT_(EXT).1 Anti-Virus Actions

Hierarchical to: No other components.

Dependencies: FAV_SCN_(EXT).1 Anti-Virus Scanning

FAV_ACT_(EXT).1.1 Upon detection of a memory based virus, the TSF shall prevent the virus from further execution.

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

a) Clean the virus from the file

b) Quarantine the file,

c) Delete the file,

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

FAV_ACT_(EXT).1.3 The TSF shall actively monitor processes attempting to access a remote system using TCP or UDP remote port 25 (SMTP) and block traffic from unauthorized processes defined by [assignment: ST author to complete] and simultaneously permit traffic from authorized process defined by [assignment: ST author to complete].

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 virus.

5.1.2 FAV_ALR_(EXT).1 Anti-Virus Alerts

Hierarchical to: No other components.

Dependencies: FAV_SCN_(EXT).1 Anti-Virus Scanning

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

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

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

FAV_ALR_(EXT).1.4 The TSF shall continue to display the alerts on the screen of the Central Administrator until they are acknowledged by the Central Administrator, or the Central Administrator session ends.

Application Note: The deletion of such audit alerts is necessary in some scenarios (e.g. a rampant outbreak of virus infection) to prevent failure due to the enormous number of generated alerts exhausting system or administrator resources. FAV_ALR_(EXT).1.4 requires the administrator acknowledge the alerts generated. A large number of alerts requiring acknowledgement, particularly during a short period of time, may prevent the administrator from adequately responding to the overall incident. If deletion of alerts is deemed necessary, the vendor must analyze the different scenarios that could occur in order to derive a comprehensive justification for deleting alerts. The solution must take into account such factors as the type of alerts, whether to delete the oldest or the newest alerts generated, and any other relevant factors based on the scenarios that might occur.

Application Note: The analysis used to determine which alerts are deleted should be publicly documented in the Security Target and noted in the associated Validation Report.

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 FAV_SCN_(EXT).1 Anti-Virus Scanning

Hierarchical to: No other components.

Dependencies: None

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

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

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

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

Management:

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

a) Configuration of scheduled scans.

b) Configuration of parameters for all types of scans.

Audit:

There are no auditable events foreseen.

5.2 Extended Security Assurance Components

None

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 those that were explicitly stated, and the AVPP all of which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1NIAP-0347	Audit Data Generation
	FAU_GEN.2NIAP-0410	User Identity Association
	FAU_SAR.1	Audit Review
	FAU_STG.1(1)-NIAP-0429	Protected Audit Trail Storage
	FAU_STG.NIAP-0414-NIAP-0429	Site-Configurable Prevention of Audit Loss
Antivirus	FAV_ACT_(EXT).1	Antivirus Actions
	FAV_ALR_(EXT).1	Antivirus Alerts
	FAV_SCN_(EXT).1	Antivirus Scanning
Cryptographic Support	FCS_COP.1	Cryptographic Operation
Security Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 12 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1-NIAP-0347 Audit Data Generation

FAU_GEN.1.1-NIAP-0347 The TSF shall be able to generate an audit record of the following auditable events:

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

b) All auditable events for the *minimum* level of audit; and

c) *The events identified in Table 13 – FAU_GEN.1 Events and Additional Information.*

FAU_GEN.1.2-NIAP-0347 The TSF shall record within each audit record at least the following

information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the additional information identified in Table 13 – FAU_GEN.1 Events and Additional Information.*

SFR	AUDITABLE EVENTS	ADDITIONAL INFORMATION
FAU_GEN.1-NIAP-0347	None	Not Applicable
FAU_GEN.2-NIAP-0410	None	Not Applicable
FAU_SAR.1	None	Not Applicable
FAU_STG.1-NIAP-0429	None	Not Applicable
FAU_STG.NIAP-0414-NIAP-0429	Selection of an action	Action selected
FAV_ACT_(EXT).1	Action taken in response to detection of a virus	• Virus detected • Action taken • File or Process where the virus was detected
FAV_ALR_(EXT).1	None	Not Applicable
FAV_SCN_(EXT).1	None	Not Applicable
FCS_COP.1	None	Not Applicable
FMT_MOF.1	None	Not Applicable
FMT_MTD.1	None	Not Applicable
FMT_SMF.1	None	Not Applicable
FMT_SMR.1	None	Not Applicable

Table 13 – FAU_GEN.1 Events and Additional Information

6.1.1.2 FAU_GEN.2-NIAP-0410 User Identity Association

FAU_GEN.2.1-NIAP-410 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(1) The TSF shall provide [the Central Administrator] with the capability to read [all audit information] from the audit records **on the central management system**.

FAU_SAR.1.2(1) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.1.1(2) The TSF shall provide [the Central Administrator and Workstation Users] with the capability to read [all audit information] from the audit records **on the workstation**

being used.

FAU_SAR.1.2(2) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: The Workstation User is permitted to review all audit records saved on the workstation being used by that user. The Central Administrator is permitted to review all logs on a specific workstation (which will only apply to that workstation) or on the central management system (which will apply to all workstations within that domain).

6.1.1.4 FAU_STG.1(1)-NIAP-0429 Protected Audit Trail Storage

FAU_STG.1(1).1-NIAP-0429 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion **via the TSFI**.

FAU_STG.1(1).2-NIAP-0429 The TSF shall be able to *prevent* unauthorized modifications to the audit records in the audit trail **via the TSFI**.

Application Note: FAU_STG.1 -NIAP-0429 applies to both the central management system and the individual workstations.

Application Note: This instance of FAU_STG.1 -NIAP-0429 applies to protection of the audit records via the TSFI. The IT Environment (OS) is responsible for preventing deletion of the audit file via OS interfaces.

6.1.1.5 FAU_STG.NIAP-0414-NIAP-0429 Site-Configurable Prevention of Audit Loss

FAU_STG.NIAP-0414-1-NIAP-0429 The TSF shall provide the administrator the capability to select one or more of the following actions *overwrite the oldest stored audit records* and [no other actions] to be taken if the audit trail is full.

FAU_STG. NIAP-0414-2-NIAP-0429 The TSF shall *overwrite the oldest stored audit records* if the audit trail is full and no other action has been selected.

FAU_STG.NIAP-0414-3-NIAP-0429 The TSF shall alert the administrator [when free disk space reaches 200 MB, 80 MB and 50 MB] before audit storage reaches capacity.

Application Note: The TOE should alert the administrator prior to audit storage becoming exhausted. The objective of this alert is to allow the administrator sufficient time to resolve the audit storage shortage before records must be deleted (for example, by archiving). When audit storage is exhausted and deletion of records is to occur, an administrative alert containing details of the deletion should be recorded in an alternate audit storage location.

Application Note: The ST and VR should characterize the specific behavior of the TOE when audit storage is exhausted. In general, the TOE should delete the minimum number of audit records required, taking into account TOE performance issues. It may be appropriate to delete the newest audit records rather than the oldest. The TOE may also employ a mechanism to delete audit records that are essentially identical. The ST should contain a rationale for the audit storage deletion policy and deletion quantity.

Application Note: The intent of the assignment in this SFR is to indicate the point at which an alert is required. Example completions are along the lines of:

…shall alert the administrator [10 minutes] before audit storage reaches capacity.

…shall alert the administrator [10 records] before audit storage reaches capacity.

…shall alert the administrator [when 3% of the storage space remains] before audit storage reaches capacity.

6.1.2 Antivirus (FAV) – Extended Requirements

6.1.2.1 FAV_ACT_(EXT).1 Anti-Virus Actions

FAV_ACT_(EXT).1.1 Upon detection of a memory-based virus, the TSF shall prevent the virus from further execution.

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

a) Clean the virus from the file,

b) Quarantine the file,

c) Delete the file,

d) [Perform no action].

FAV_ACT_(EXT).1.3 The TSF shall actively monitor processes attempting to access a remote system using TCP or UDP remote port 25 (SMTP) and block traffic from unauthorized processes defined by [comparing a request for network port access to the antivirus rules] and simultaneously permit traffic from authorized processes defined by [taking no additional actions].

6.1.2.2 FAV_ALR_(EXT).1 Antivirus Alerts

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

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

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

FAV_ALR_(EXT).1.4 The TSF shall continue to display the alerts on the screen of the Central Administrator until they are acknowledged by the Central Administrator, or the Central Administrator session ends.

6.1.2.3 FAV_SCN_(EXT).1 Antivirus Scanning

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

FAV_SCN_(EXT).1.2 The TSF shall perform real-time, scheduled, and on-demand scans for file-based

viruses based upon known signatures.

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

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

6.1.3 Cryptographic Support (FCS)

6.1.3.1 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [a message digest calculation to verify the integrity of the signature files] in accordance with a specified cryptographic algorithm [SHA-1] and cryptographic key sizes (*not applicable*) that meet the following: [FIPS 180-2, Certificate Numbers 783 (Windows XP), 176, 613, 816 (Windows Server 2003), 753 (Windows Server 2008), and 1081 (Windows Server 2008 SP1)].

Application Note: Conforming STs should specify the Cryptographic Module Validation Program (CMVP) validated algorithm certificate number.

Application Note: Message digests use hash functions, which do not have keys. Therefore, the assignment related to the cryptographic key size has been set to "not applicable".

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1(1) The TSF shall restrict the ability to *determine the behavior of, disable, enable* the functions [

a) Auditing,

b) Real-time virus scanning, and

c) Scheduled virus scanning]

to [the Central Administrator].

FMT_MOF.1.1(2) The TSF shall restrict the ability to *modify the behavior of* the functions [manually invoked virus scanning] to [Workstation Users].

6.1.4.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1(1) The TSF shall restrict the ability to *query, modify, delete* the [

a) Actions to be taken on workstations when a virus is detected,

b) Files to be scanned automatically on workstations,

c) Minimum depth of file scans on workstations,

d) Scheduled scan frequency on workstations,

e) Processes authorized to transmit data to a remote system using TCP or UDP remote port 25 (SMTP).

f) Virus scan signatures, and

g) Audit logs on the central management system]

to [the Central Administrator].

FMT_MTD.1.1(2) The TSF shall restrict the ability to modify the [

a) Depth of file scans on manually invoked scans on workstations, and

b) Files to be scanned manually on workstations]

to [the Central Administrator and Workstation Users].

FMT_MTD.1.1(3) The TSF shall restrict the ability to *query, delete* the [audit logs on the workstation being used] to [the Central Administrator and Workstation Users].

6.1.4.3 FMT_SMF.1 Specification of Management Functions

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

a) Enable and disable operation of the TOE on workstations,

b) Configure operation of the TOE on workstations,

c) Update virus scan signatures,

d) Acknowledge alert notifications from the central management system,

e) Review audit logs on the central management system,

f) Increase the depth of file scans on manually invoked scans,

g) Acknowledge alert notifications on the workstation being used, and

h) Review audit logs on the workstation being used

].

6.1.4.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Central Administrator, Workstation User, Network User].

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

Application Note: The Workstation User is defined by the Central Administrator installing a SEP Client on a Workstation and specifying a Group for that workstation within the SEPM Console.

6.2 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.1-NIAP-0347	None	FPT_STM.1	Satisfied by the Operational Environment (OE.TIME_STAMPS)
FAU_GEN.2-NIAP-410	None	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied by the Operational Environment (OE.TOE_ACCESS)
FAU_SAR.1	None	FAU_GEN.1	Satisfied
FAU_STG.1(1)-NAIP-0429	None	FAU_GEN.1	Satisfied
FAU_STG.NIAP-0414-NIAP-0429	none	FAU_GEN.1 FAU_STG.1,	Satisfied Satisfied by the Operational Environment (OE.AUDIT_ALARM)
FAV_ACT_(EXT).1	None	FAV_SCN_(EXT).1	Satisfied
FAV_ALR_(EXT).1	None	FAV_SCN_(EXT).1	Satisfied
FAV_SCN_(EXT).1	None	None	None
FCS_COP.1	None	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	Not satisfied. The only cryptographic function is a message digest that does not use keys.
FMT_MOF.1	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1(1)	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1(2)	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1(3)	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	None	None	None
FMT_SMR.1	None	FIA_UID.1	Satisfied by the Operational Environment

Table 14 - TOE SFR Dependency Rationale

6.3 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). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
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 15 – Security Assurance Requirements at EAL2

6.3.1 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 2. EAL2 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL2 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface.

6.4 Security Requirements Rationale

6.4.1 Security Functional Requirements for the TOE

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

	O.ADMIN_GUIDANCE	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECT	O.AUDIT_REVIEW	O.CONFIGURATION_IDENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.DOCUMENTED_DESIGN	O.MANAGE	O.PARTIAL_FUNCTIONAL_TEST	O.PARTIAL_SELF_PROTECTION	O.VIRUS	O.VULNERABILITY_ANALYSIS
ADV_ARC.1												✓		
ADV_FSP.2									✓					
ADV_TDS.1									✓					
AGD_OPE.1	✓													
AGD_PRE.1	✓													
ALC_CMC.2						✓								
ALC_DEL.1	✓													
ALC_FLR.2						✓								
ATE_COV.1											✓			
ATE_FUN.1											✓			
ATE_IND.2											✓			
AVA_VAN.2														✓
FAU_GEN.1NIAP-0347			✓				✓							
FAU_GEN.2NIAP-0410			✓				✓							
FAU_SAR.1					✓		✓							
FAU_STG.1-NIAP-0429				✓										
FAU_STG.NIAP-0414-NIAP-0429				✓										
FAV_ACT_(EXT).1							✓						✓	
FAV_ALR_(EXT).1							✓						✓	
FAV_SCN_(EXT).1							✓						✓	
FCS_COP.1								✓						
FMT_MOF.1(1)		✓								✓				
FMT_MOF.1(2)		✓								✓				
FMT_MOF.1(3)		✓								✓				
FMT_MTD.1		✓								✓				
FMT_SMF.1		✓								✓				
FMT_SMR.1		✓								✓				

Table 16 – Mapping of TOE SFRs to Security Objectives

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

OBJECTIVE	ADDRESSED BY	SFR AND RATIONALE
O.ADMIN_GUIDANCE The TOE will provide the administrators with the necessary information for secure management.	ALC_DEL.1 AGD_PRE.1 AGD_OPE.1	ALC_DEL.1 ensures that the administrator is provided documentation that instructs them how to ensure the delivery of the TOE, in whole or in parts, without tampering or corruption during delivery. This requirement ensures the administrator has the ability to begin their TOE installation with a clean (e.g. malicious code has not been inserted once it has left the developer's control) version of the TOE, which is necessary for secure management of the TOE. AGD_PRE.1 ensures the administrator has the information necessary to install the TOE in the evaluated configuration. Often times a vendor's product contains software that is not part of the TOE and has not been evaluated. The documentation ensures that once the administrator has followed the installation and configuration guidance the result is a TOE in a secure configuration. AGD_OPE.1 mandates the developer provide the administrator with guidance on how to operate the TOE in a secure manner. This includes describing the interfaces the administrator uses in managing the TOE, security parameters that are configurable by the administrator, how to configure the TOE's rule set and the implications of any dependencies of individual rules. The documentation also provides a description of how to setup and review the auditing features of the TOE.

OBJECTIVE	ADDRESSED BY	SFR AND RATIONALE
O.ADMIN_ROLE The TOE will provide an authorized administrator role to isolated administrative actions.	FMT_MOF.1(1) FMT_MOF.1(2) FMT_MOF.1(3) FMT_MTD.1 FMT_SMR.1	FMT_SMR.1 requires that the TOE establish a Central Administrator role. FMT_MOF.1(1), FMT_MOF.1(2), FMT_MOF.1(3), and FMT_MTD.1 specify the privileges that only the Central Administrator may perform.
O.AUDIT_GEN The TOE will provide the capability to detect and create records of security relevant events.	FAU_GEN.1NIAP-0347 FAU_GEN.2NIAP-0410	FAU_GEN.1NIAP-0347 defines the set of events that the TOE must be capable of recording. This requirement ensures that the Administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements. FAU_GEN.2NIAP-0410 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the userid. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated.
O.AUDIT_PROTECT The TOE will provide the capability to protect audit information.	FAU_SAR.1 FAU_STG.1(1)-NIAP-0429 FAU_STG.NIAP-0414-1-NIAP-0429	FAU_SAR.1 restricts the ability to read the audit trail to the Audit Administrator, thus preventing the disclosure of the audit data to any other user. However, the TOE is not expected to prevent the disclosure of audit data if it has been archived or saved in another form (e.g. moved or copied to an

OBJECTIVE	ADDRESSED BY	SFR AND RATIONALE
		ordinary file). The FAU_STG family dictates how the audit trail is protected. FAU_STG.1(1)-NIAP-0429 restricts the ability to delete audit records to the Security Administrator. FAU_STG.NIAP-0414-1-NIAP-0429 defines when alarms will be issued as the audit logs near capacity. This helps to ensure that audit records are not lost. This ensures the integrity of the audit trail is maintained.
O.AUDIT_REVIEW The TOE will provide the capability to selectively view audit information.	FAU_SAR.1	FAU_SAR.1 provides the ability to review the audits in a user-friendly manner.
O.CONFIGURATION_IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified.	ALC_CMC.2 ALC_FLR.2	ALC_CMC.2 addresses this objective by requiring that there be a unique reference for the TOE, and that the TOE is labeled with that reference. It also requires that there be a CM system in place, and that the configuration items that comprise the TOE be uniquely identified. This provides a clear identification of the composition of the TOE. ALC_FLR.2 addresses this objective by requiring that there be a mechanism in place for identifying flaws subsequent to fielding, and for distributing those flaws to entities operating the system.
O.CORRECT_TSF_OPERATION The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.	FAU_GEN.1NIAP-0347 FAU_GEN.2NIAP-0410 FAU_SAR.1 FAV_SCN_(EXT).1 FAV_ALR_(EXT).1 FAV_ACT_(EXT).1	Correct TSF operation can be determined by injecting a known virus into the TOE and ensuring that the proper events occur. The FAV class will detect and act upon the virus. The FAU_GEN family will generate an audit event when the virus is detected. FAU_SAR.1 enables the administrator to review the audit events.

OBJECTIVE	ADDRESSED BY	SFR AND RATIONALE
O.CRYPTOGRAPHY The TOE shall use NIST FIPS 140-2 validated cryptographic services.	FCS_COP.1	FCS_COP.1 requires that the message digest used to verify integrity of the signature file utilizes a FIPS 140-2 Approved cryptographic algorithm.
O.DOCUMENTED_DESIGN The design of the TOE is adequately and accurately documented.	ADV_FSP.2 ADV_TDS.1	ADV_FSP.2 requires that the interfaces to the TOE be documented and specified. ADV_TDS.1 requires that the TOE design be documented and specified and that said design be shown to correspond to the interfaces.
O.MANAGE The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE.	FMT_MOF.1(1) FMT_MOF.1(2) FMT_MOF.1(3) FMT_MTD.1 FMT_SMF.1 FMT_SMR.1	Restricted privileges are defined for the Central Administrator and Workstation Users. FMT_MOF.1(1), FMT_MOF.1(2), and FMT_MOF.1(3) define particular TOE capabilities that may only be used by the users. FMT_MTD.1 defines particular TOE data that may only be altered by these users. FMT_SMF.1 and FMT_SMR.1 define the administrative functions and roles provided by the TOE.
O.PARTIAL_FUNCTIONAL_TEST The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.	ATE_COV.1 ATE_FUN.1 ATE_IND.2	ATE_FUN.1 requires that developer provide test documentation for the TOE, including test plans, test procedure descriptions, expected test results, and actual test results. These needs to identify the functions tested, the tests performed, and test scenarios. They require that the developer run those tests, and show that the expected results were achieved. ATE_COV.1 requires that there be a correspondence between the tests in the test documentation and the TSF as described in the functional specification.

OBJECTIVE	ADDRESSED BY	SFR AND RATIONALE
		ATE_IND.2 requires that the evaluators test a subset of the TSF to confirm correct operation, on an equivalent set of resources to those used by the developer for testing. These sets should include a subset of the developer run tests.
O.PARTIAL_SELF_PROTECTION The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.	ADV_ARC.1	ADV_ARC.1 provides the security architecture description of the security domains maintained by the TSF that are consistent with the SFRs. Since self-protection is a property of the TSF that is achieved through the design of the TOE and TSF, and enforced by the correct implementation of that design, self-protection will be achieved by that design and implementation.
O.VIRUS The TOE will detect and take action against known viruses introduced to the workstation via network traffic or removable media.	FAV_ACT_(EXT).1 FAV_ALR_(EXT).1 FAV_SCN_(EXT).1	FAV_SCN_(EXT).1 requires that the TOE scan for viruses. FAV_ACT_(EXT).1 requires that the TOE take action against viruses once they are detected. FAV_ALR_(EXT).1 defines alerting requirements to ensure the users aware that a virus was detected.
O.VULNERABILITY_ANALYSIS The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	AVA_VAN.2	The AVA_VAN.2 component provides the necessary level of confidence that vulnerabilities do not exist in the TOE that could cause the security policies to be violated. AVA_VAN.2 requires the evaluator to perform a search for potential vulnerabilities in all the TOE deliverables. For those vulnerabilities that are not eliminated by the developer, a rationale must be provided that describes why these vulnerabilities cannot be exploited by a threat agent with a basic attack potential, which is in keeping with the desired assurance level of this TOE.

OBJECTIVE	ADDRESSED BY	SFR AND RATIONALE
		This component provides the confidence that security flaws do not exist in the TOE that could be exploited by a threat agent of basic attack potential to violate the TOE's security policies.

Table 17 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Assurance Requirements

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

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: Symantec Endpoint Protection Version 12.1.2
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: Symantec Endpoint Protection Version 12.1.2
ADV_TDS.1: Basic Design	Basic Design: Symantec Endpoint Protection Version 12.1.2
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Symantec Endpoint Protection Version 12.1.2
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Symantec Endpoint Protection Version 12.1.2
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: Symantec Endpoint Protection Version 12.1.2
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: Symantec Endpoint Protection Version 12.1.2
ALC_DEL.1: Delivery Procedures	Delivery Procedures: Symantec Endpoint Protection Version 12.1.2
ALC_FLR.2: Flaw Reporting Procedures	Flaw Reporting Procedures: Symantec Endpoint Protection Version 12.1.2
ATE_COV.1: Evidence of Coverage	Security Testing: Symantec Endpoint Protection Version 12.1.2
ATE_FUN.1: Functional Testing	Security Testing: Symantec Endpoint Protection Version 12.1.2
ATE_IND.2: Independent Testing – Sample	Security Testing: Symantec Endpoint Protection Version 12.1.2

Table 18 – Security Assurance Rationale and Measures

7 TOE Summary Specification

7.1 TOE Security Functions

The security functions described in the following subsections fulfill the security requirements that are defined in Section 6 – Security Requirements. The security functions performed by the TOE are as follows:

- Antivirus
- Audit
- Cryptographic Operations
- Management

7.1.1 Antivirus

The TOE is designed to help prevent memory-based and file-based viruses. If a memory-based virus is detected on a host machine, the TOE will prevent the virus from further executions. The TOE also provides for administrator-defined actions upon detection of a virus-infected file; the administrator can configure the TOE to clean the file, quarantine the file, delete the file, or take no action on the file. Configuration of these options is performed by the Central Administrator via the SEPM console. The TOE monitors the host machine's files and processes over TCP or UPD remote port 25 (SMTP) to ensure unauthorized processes are not executed.

The Antivirus function is designed to satisfy the following security functional requirements:

- FAV_ACT_(EXT).1
- FAV_ALR_(EXT).1
- FAV_SCN_(EXT).1

7.1.2 Audit

The TOE provides robust reporting capabilities to provide the Central Administrator with insight on the Server and Workstation antivirus-related activities. Additionally, the TOE supports the provision of log data from each system component.

The reporting functions give you the up-to-date information that you need to monitor and make informed decisions about the security of your network. The management console Home page displays the automatically generated charts that contain information about the important events that have happened recently in your network. You can use the filters on the Reports page to generate predefined or custom reports. You can use the Reports page to view graphical representations and statistics about

the events that happen in your network. You can use the filters on the Monitors page to view more detailed, real-time information about your network from the logs.

Reporting runs as a Web application within the management console, and TOE reporting features include the following:

- Customizable Home page with your most important reports, overall security status, and links to Symantec Security Response
- Summary views of reports on antivirus status, firewall/IDS status, compliance status, and site status
- Predefined quick reports and customizable graphical reports with multiple filter options that you can configure
- The ability to schedule reports to be emailed to recipients at regular intervals
- Support for Microsoft SQL or an embedded database for storing event logs
- The ability to run client scans, to turn client firewall and Auto-Protect on, and to restart computers directly from the logs
- The ability to add application exclusions directly from the logs
- Configurable notifications that are based on security events

The TOE generates audit data for various events, and this audit data is aggregated into a series of pre-defined reports. An authorized administrator can view and filter the following reports:

REPORT TYPE	DESCRIPTION
Application Control and Device Control	Displays information about events where some type of behavior was blocked. These reports include information about application security alerts, blocked targets, and blocked devices. Blocked targets can be registry keys, dlls, files, and processes.
Audit	Displays information about the policies that clients and locations use currently.
Compliance	Displays information about the compliance status of your network. These reports include information about Enforcer servers, Enforcer clients, Enforcer traffic, and host compliance.
Computer Status	Displays information about the operational status of the computers in your network, such as which computers are infected. These reports include information about versions, clients that have not checked in to the server, client inventory, and online status.
Firewall	Displays information about attacks on the firewall and about firewall traffic and packets.
Risk	Displays information about risk events on your management servers and their clients. It includes information about Proactive Threat Protection.
Scan	Displays information about antivirus and antispyware scan activity.

REPORT TYPE	DESCRIPTION
System	Displays information about event times, event types, sites, domains, servers, and severity levels.

Table 19 – Available Reports

From the SEPM console, the Central Administrator can also view Virus Detection reports, which include the following parameters:

- Infected client
- Infected file and/or process
- Action taken upon discovery.

The report will include the following details for actions taken upon discovery:

- Clean the virus from the file,
- Quarantine the file,
- Delete the file,
- No action taken on the file.

Reports are available only to operators that have explicit access to reports, and this privilege is defined by the system administrator (i.e., Central Administrator role). Operators with access to reports can search audit records and can sort records by date/time of event, the type of event recorded, and the affected host identity.

All system reports and audit logs are stored in an embedded database on the SEPM. If the database reaches storage capacity, the TOE will overwrite the oldest records.

The Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1- NIAP-0347
- FAU_GEN.2 NIAP-0410
- FAU_SAR.1
- FAU_STG.1-NIAP-0429
- FAU_STG.NIAP-0414-NIAP-0429

7.1.3 Cryptographic Operations

The TOE supports the import of user data without security attributes. Imported user data includes virus definitions that are imported from Symantec Security Response, a team of dedicated intrusion experts,

security engineers, virus hunters, threat analysts, and global technical support teams that work in tandem to provide extensive coverage for enterprise businesses and consumers. User data is imported from Symantec Security Response to the Live Update Client component of the TOE. Virus definitions are verified via SHA-1 by the Live Update Client subcomponent of the TOE.

The SHA-1 implementation is provided by a FIPS 140-validated module provided by Windows. The following table details the validations:

OPERATING SYSTEM	CMVP Cert #
Windows XP (32-bit, SP-3 or higher, 64-bit, all SPs)	(FIPS 140-2 cert. #989)
Windows Server 2003 (32-bit, 64-bit, R2, SP1 or later)	(FIPS 140-2 cert. #382, 868, 1012)
Windows Server 2008 (32-bit, 64-bit)	(FIPS 140-2 cert. #1010)

Table 20 - Cryptographic Module Validations

The Cryptographic Operations functions are designed to satisfy the following security functional requirements:

- FCS_COP.1

7.1.4 Management

The functionality in the TOE requires management to ensure proper configuration control. These pieces of Management functionality are described in the following subsections:

7.1.4.1 Security Roles

The TOE maintains three roles: system administrator, administrator, and limited administrator. The AVPP specifies a Central Administrator, Network User, and Workstation User. The table below maps the role groups and provides a brief description of each:

SEP ROLE	AVPP ROLE	DESCRIPTION
System Administrator	Central Administrator Network User	Domain management Administrator management Server management

SEP ROLE	AVPP ROLE	DESCRIPTION
Administrator and Limited Administrator	Central Administrator Network User	Create administrators in their domain Delete and modify the administrators that were created in their domain Change attributes for the administrators that are created in their domain. These attributes include notification, security, and permission settings.
SEP Client	Workstation User	Perform the work that is assigned to them by the system administrator or administrator Configure their own attributes including security settings and notification settings

Table 21 – Description of Roles Supported in the TOE

The System Administrator role in the TOE is responsible for all management functions of the TOE, including management of TOE security functions and review of TOE audit data. The System Administrator can configure the TOE to support the actions defined in 7.1.1 – Antivirus.

7.1.4.2 Security Audit

A TOE Administrator can view system reports and specific component logs. The Administrator can further define lifespans for the storage of reports/logs and can view, print, save, schedule, and delete them as part of the Security Audit capabilities.

7.1.4.3 Access Control

The Administrator manages the creation and enforcement of different levels of access within the TOE, and each level of access has set of services available (as defined in Table 21 – Description of Roles Supported in the TOE). The Administrator can define services available to various privilege levels/roles without granting full System Administrator privileges.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1(1)
- FMT_MOF.1(2)
- FMT_MOF.1(3)
- FMT_MTD.1
- FMT_SMF.1

- FMT_SMR.1