Security Target: Symantec™ Endpoint Protection Version 11.0

ST Version 1.6

June 2, 2008

Prepared For:

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
www.symantec.com

Prepared By:

Apex Assurance Group, LLC
5448 Apex Peakway Drive, Ste. 101
Apex, NC 27502
www.apexassurance.com

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Symantec™ Endpoint Protection Version 11.0. 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.

Document Revision History

REVISION	DATE	DESCRIPTION
1.0	September 23, 2007	Initial release
1.1	November 8, 2007	Address initial verdicts from EWA-Canada
1.2	January 14, 2008	Minor updates
1.3	February 21, 2008	Update with details to address PD-0129
1.4	March 11, 2008	Clarify roles and descriptive mapping to PP roles
1.5	May 13, 2008	Remove proprietary marking and other final edits
1.6	June 2, 2008	Clarify final validator comment; release for publishing

Table of Contents

1 INTRODUCTION 7
1.1 IDENTIFICATION 7
1.2 OVERVIEW 7
1.3 CC CONFORMANCE CLAIM 7
1.4 ORGANIZATION 8
1.5 DOCUMENT CONVENTIONS 8
1.6 DOCUMENT TERMINOLOGY 9
2 TOE DESCRIPTION 10
2.1 PRODUCT TYPE 10
2.2 PRODUCT DESCRIPTION 10
2.2.1 Symantec Endpoint Protection Client 10
2.2.1.1 Operating System Support 10
2.2.2 Symantec Endpoint Protection Manager 11
2.2.2.1 Operating System Support 11
2.2.3 Operator Roles in the TOE 11
2.2.3.1 Central Administrator 11
2.2.3.2 Workstation User 12
2.2.3.3 Network User 12
2.3 TOE BOUNDARIES 12
2.3.1 Physical Boundary Configuration 12
2.3.2 Logical Boundaries 13
2.3.2.1 Antivirus 13
2.3.2.2 Audit 13
2.3.2.3 Cryptographic Operations 14
2.3.2.4 Management 14
2.3.2.5 Protection of the TOE 14
3 TOE SECURITY ENVIRONMENT 15
3.1 SECURE USE ASSUMPTIONS 15
3.2 THREATS TO SECURITY 15
3.2.1 Threats Addressed by the TOE 16
3.2.2 Threats Addressed by Operating Environment 17
3.3 ORGANIZATIONAL SECURITY POLICIES 17
4 SECURITY OBJECTIVES 18
4.1 SECURITY OBJECTIVES FOR THE TOE 18
4.2 SECURITY OBJECTIVES FOR THE IT ENVIRONMENT 19
4.3 SECURITY OBJECTIVES FOR THE NON-IT ENVIRONMENT 20
5 IT SECURITY REQUIREMENTS 21
5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 21
5.1.1 Security Audit (FAU) 21
5.1.1.1 FAU_GEN.1 Audit Data Generation 21
5.1.1.2 FAU_GEN.2 User Identity Association 23
5.1.1.3 FAU_SAR.1 Audit Review 23
5.1.1.4 FAU_SAR.2 Restricted Audit Review 23
5.1.1.5 FAU_SAR.3 Selectable Audit Review 23
5.1.1.6 FAU_STG.1 Protected Audit Trail Storage 24
5.1.1.7 FAU_STG.4 Site-Configurable Prevention of Audit Loss 24
5.1.2 Antivirus (FAV) – Explicitly Stated 24
5.1.2.1 FAV_ACT_EXP.1 Anti-Virus Actions 24
5.1.2.2 FAV_ALR_EXP.1 Antivirus Alerts 25

5.1.2.3 FAV_SCN_EXP.1 Antivirus Scanning ... 25
5.1.3 Cryptographic Support (FCS)... 25
5.1.3.1 FCS_COP.1 Cryptographic Operation... 25
5.1.4 Security Management (FMT) ... 26
5.1.4.1 FMT_MOF.1 Management of Security Functions Behavior ... 26
5.1.4.2 FMT_MTD.1 Management of TSF Data ... 26
5.1.4.3 FMT_SMF.1 Specification of Management Functions ... 26
5.1.4.4 FMT_SMR.1 Security Roles ... 27
5.1.5 Protection of the TSF (FPT)... 27
5.1.5.1 FPT_SEP_EXP.1 Partial TSF Domain Separation... 27
5.2 SECURITY FUNCTIONAL REQUIREMENTS FOR THE IT ENVIRONMENT ... 27
5.2.1 Security Audit (FAU)... 27
5.2.1.1 FAU_STG.1 Protected Audit Trail Storage ... 27
5.2.2 User Data Protection (FDP) ... 28
5.2.2.1 FDP_RIP.1 Subset Residual Information Protection ... 28
5.2.3 Identification and Authentication (FIA)... 28
5.2.3.1 FIA_AFL.1 Authentication Failure Handling... 28
5.2.3.2 FIA_SOS.1 Verification of Secrets ... 28
5.2.3.3 FIA_UAU.2 User Authentication Before any Action... 28
5.2.3.4 FIA_UAU.6 Re-Authenticating ... 28
5.2.3.5 FIA_UID.2 User Identification Before any Action... 28
5.2.3.6 FIA_PLA_EXP.1 Performance and Log Alerts (EXP) ... 29
5.2.4 Protection of the TSF (FPT)... 29
5.2.4.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection ... 29
5.2.4.2 FPT_RVM.1 Non-Bypassability of the TSP... 29
5.2.4.3 FPT_SEP.1 TSF Domain Separation ... 29
5.2.4.4 FPT_STM.1 Reliable Time Stamps... 29
5.2.5 TOE Access (FTA) ... 29
5.2.5.1 FTA_SSL.1 TSF-Initiated Session Locking... 29
5.2.5.2 FTA_TAB.1 Default TOE Access Banners... 30
5.3 SECURITY REQUIREMENTS FOR THE NON-IT ENVIRONMENT ... 30
5.4 TOE SECURITY ASSURANCE REQUIREMENTS ... 30

6 TOE SUMMARY SPECIFICATION ... 32

6.1 TOE SECURITY FUNCTIONS... 32
6.1.1 Antivirus ... 32
6.1.2 Audit... 32
6.1.3 Cryptographic Operations... 35
6.1.4 Management ... 35
6.1.4.1 Security Roles... 35
6.1.4.2 Security Audit... 36
6.1.4.3 Access Control... 36
6.1.5 TSF Protection ... 36
6.2 SECURITY ASSURANCE MEASURES... 36

7 PROTECTION PROFILE CLAIMS ... 40

8 RATIONALE... 41

8.1 RATIONALE FOR SECURITY OBJECTIVES OF THE TOE, IT ENVIRONMENT, AND NON-IT ENVIRONMENT ... 41
8.1.1 Summary Mapping of Security Objectives... 41
8.1.2 Rationale for Security Objectives of the TOE ... 42
8.2 SECURITY REQUIREMENTS RATIONALE ... 51
8.2.1 Summary of TOE Security Requirements... 51
8.2.2 Sufficiency of Security Requirements... 53
8.2.3 Summary of IT Environment Security Requirements ... 59
8.2.4 Sufficiency of Security Requirements for the IT Environment ... 60
8.3 TOE SUMMARY SPECIFICATION RATIONALE... 62

8.3.1 Sufficiency of IT Security Functions 63
8.4 RATIONALE FOR IT SECURITY REQUIREMENT DEPENDENCIES 64
8.4.1 Rationale for Unsupported SFR Dependencies 66
8.5 RATIONALE FOR EXPLICITLY STATED REQUIREMENTS 67
8.6 RATIONALE FOR SECURITY ASSURANCE REQUIREMENTS 67
8.7 RATIONALE FOR STRENGTH OF FUNCTION CLAIM 67
8.8 RATIONALE FOR PROTECTION PROFILE CLAIMS 68

List of Tables

Table 1 – ST Organization and Description 8

Table 2 – Acronyms Used in Security Target 9

Table 3 – Symantec Endpoint Protection Client: Supported Operating Systems 10

Table 4 – Symantec Endpoint Protection Manager: Supported Operating Systems 11

Table 5 – Evaluated Configuration for the TOE 12

Table 6 – TOE Security Functional Requirements 21

Table 7 – FAU_GEN.1 Events and Additional Information 23

Table 8 – Security Assurance Requirements 30

Table 9 – Available Reports 34

Table 10 – Description of Roles Supported in the TOE 35

Table 11 – Assurance Measures 39

Table 12 – Modifications from Protection Profile 40

Table 13 – Mapping of Assumptions, Threats, and OSPs to Security Objectives 42

Table 14 – Mapping of Threats, Policies, and Assumptions to Objective 51

Table 15 – Mapping of TOE Security Functional Requirements and Objectives 53

Table 16 – Rationale for TOE Objectives 59

Table 17 – Mapping of IT Environment Security Functional Requirements and Objectives 60

Table 18 – Rationale for IT Environment Objectives 62

Table 19 – Mapping of Security Functional Requirements to IT Security Functions 63

Table 20 – Sufficiency of IT Security Functions 64

Table 21 – TOE SFR Dependency Rationale 66

Table 22 – Unsupported SFR Dependency Rationale 66

Table 23 – Rationale for Explicitly Stated Requirements 67

List of Figures

Figure 1 – TOE Boundary..13

1 Introduction

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

1.1 Identification

This section provides information necessary to identify and control this ST and its Target of Evaluation.

ST Title:	Security Target: Symantec™ Endpoint Protection Version 11.0
ST Revision:	1.6
ST Publication Date:	June 2, 2008
TOE Identification:	Symantec™ Endpoint Protection Version 11.0
Vendor:	Symantec Corporation
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.3 and applicable international and NIAP interpretations as of November 23, 2004.
Author:	Apex Assurance Group
PP Compliance:	U.S. Government Protection Profile for Anti-Virus Applications for Workstations in Basic Robustness Environments, Version 1.1, April 4, 2006
Keywords:	Symantec™, antivirus, endpoint protection

1.2 Overview

The TOE is Symantec™ Endpoint Protection Version 11.0, which delivers a comprehensive antivirus/endpoint security solution with a single agent and a single, centralized management console. Symantec™ Endpoint Protection Version 11.0 may hereafter also be referred to as the TOE in this document.

1.3 CC Conformance Claim

The TOE meets the following claims:

- Common Criteria Part 2 Extended
- Common Criteria Part 3 EAL2 conformant with augmentation to include ALC_FLR.2 and AVA_MSU.1.
- Conformance to *U.S. Government Protection Profile for Anti-Virus Applications for Workstations in Basic Robustness Environments, Version 1.1, April 4, 2006.*

1.4 Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the Security Target
2	TOE Description	Defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
3	TOE Security Environment	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE and the TOE environment
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE
6	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.
7	PP Claims	Specifies Protection Profile conformance claims of the TOE
8	Rationale	Provides a rationale to demonstrate that the security objectives satisfy the threats; provides justifications of dependency analysis and strength of function issues

Table 1 – ST Organization and Description

1.5 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 2.3 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 paragraph 2.1.4 of 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, 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, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

- Application notes provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized* text within the functional requirements and are preceded with the text "*Application Note*"

Italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.6 Document Terminology

The following table provides a list of acronyms used within this document:

TERM	DEFINITION
AVPP	U.S. Government Protection Profile for Anti-Virus Applications for Workstations in Basic Robustness Environments, Version 1.1, April 4, 2006
CC	Common Criteria
CMVP	Cryptographic Module Validation Program
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OSP	Organizational Security Policy
PP	Protection Profile
SEP	Symantec™ Endpoint Protection
SFR	Security Functional Requirement
SHA	Security Hash Algorithm
SOF	Strength Of Function
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy

Table 2 – Acronyms Used in Security Target

2 TOE Description

This section describes the Target of Evaluation (TOE), the provided security functionality (logical boundaries), and the physical TOE boundaries.

2.1 Product Type

Symantec™ Endpoint Protection 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.

2.2 Product Description

The evaluated features of Symantec™ Endpoint Protection are comprised of the following components:

- Symantec Endpoint Protection Client
- Symantec Endpoint Protection Manager (and management console)

The following sections describe each component in more detail.

2.2.1 Symantec Endpoint Protection Client

The Symantec Endpoint Protection Client is software that protects servers, desktops, and laptops systems on an internal network.

2.2.1.1 Operating System Support

OPERATING SYSTEM	32-BIT	64-BIT
Microsoft Windows Vista	✓	✓
Microsoft Windows 2003	✓	✓
Microsoft Windows XP (SP2[1])	✓	✓
Microsoft Windows 2000 (SP3 and higher)	✓	

Table 3 – Symantec Endpoint Protection Client: Supported Operating Systems

[1] Tested on Service Pack 2 but compatible with previous versions of Windows XP

2.2.2 Symantec Endpoint Protection Manager

The management functions of the Central Administrator may execute on a separate system from the portion of the TOE performing virus scanning on workstations; this portion of the TOE is called Symantec Endpoint Protection Manager (SEPM). The SEPM communicates with individual workstations via an agent over HTTPS that is installed with the Symantec Endpoint Protection Client software. The SEPM is managed via Console application running on a host computer, which communicates with the SEPM via HTTPS.

2.2.2.1 Operating System Support

OPERATING SYSTEM	32-BIT	64-BIT
Microsoft Windows 2003	✓	✓
Microsoft Windows XP (SP2[2])	✓	
Microsoft Windows 2000 (SP3 and higher)	✓	

Table 4 – Symantec Endpoint Protection Manager: Supported Operating Systems

2.2.3 Operator Roles in the TOE

The TOE supports the roles defined in the following sections.

2.2.3.1 Central Administrator

The Central Administrator controls the operation of all instances of the TOE under their authority. This role has the authority to:

- Remotely manage operation of the TOE on workstations
- Schedule scans of existing files
- Manually invoke scans
- Control the minimum depth of scans
- Update virus signature files
- Receive alert notifications from the centralized management system
- Acknowledge alert notifications from the centralized management system
- Review the TOE audit information in the centralized management system

Application Note: When the workstation is stand-alone (i.e., not network-attached), the local

[2] Tested on Service Pack 2 but compatible with previous versions of Windows XP

administrator for the workstation assumes the privileges of the Central Administrator for that workstation. The Central Administrator privileges associated with the centralized management system do not apply to this scenario, and operation of the TOE is administered locally.

2.2.3.2 Workstation User

This role is defined as the user utilizing the workstation on which the SEP Client is installed. This role has the authority to:

- Manually invoke scans
- Increase the depth of scans on manually invoked scans
- Receive alert notifications for events on the workstation being used
- Acknowledge alert notifications for events on the workstation being used
- Review the TOE audit information on the workstation being used

2.2.3.3 Network User

This role is defined as a remote user or process sending information to the workstation via a network protocol. This role has the authority to:

- Send information to the workstation

2.3 TOE Boundaries

2.3.1 Physical Boundary Configuration

The TOE is defined as Symantec™ Endpoint Protection Version 11.0. In order to comply with the evaluated configuration, the following components should be used:

COMPONENT	VERSION NUMBER
SEPM Software	Version 11.0.776.942
Client Software	Version: 11.0.780.1109
Operating System	Please see Table 3 – Symantec Endpoint Protection Client: Supported Operating Systems and Table 4 – Symantec Endpoint Protection Manager: Supported Operating Systems for a list of operating systems supported in the evaluated configuration

Table 5 – Evaluated Configuration for the TOE

Figure 1 – TOE Boundary illustrates the physical scope and the physical boundary of the Symantec Endpoint Protection solution and harnesses the TOE components and the elements of the TOE Environment.

The essential physical components for the proper operation of the TOE in the evaluated configuration are as follows:

- Symantec Endpoint Protection Client
- Symantec Endpoint Protection Manager
- Console

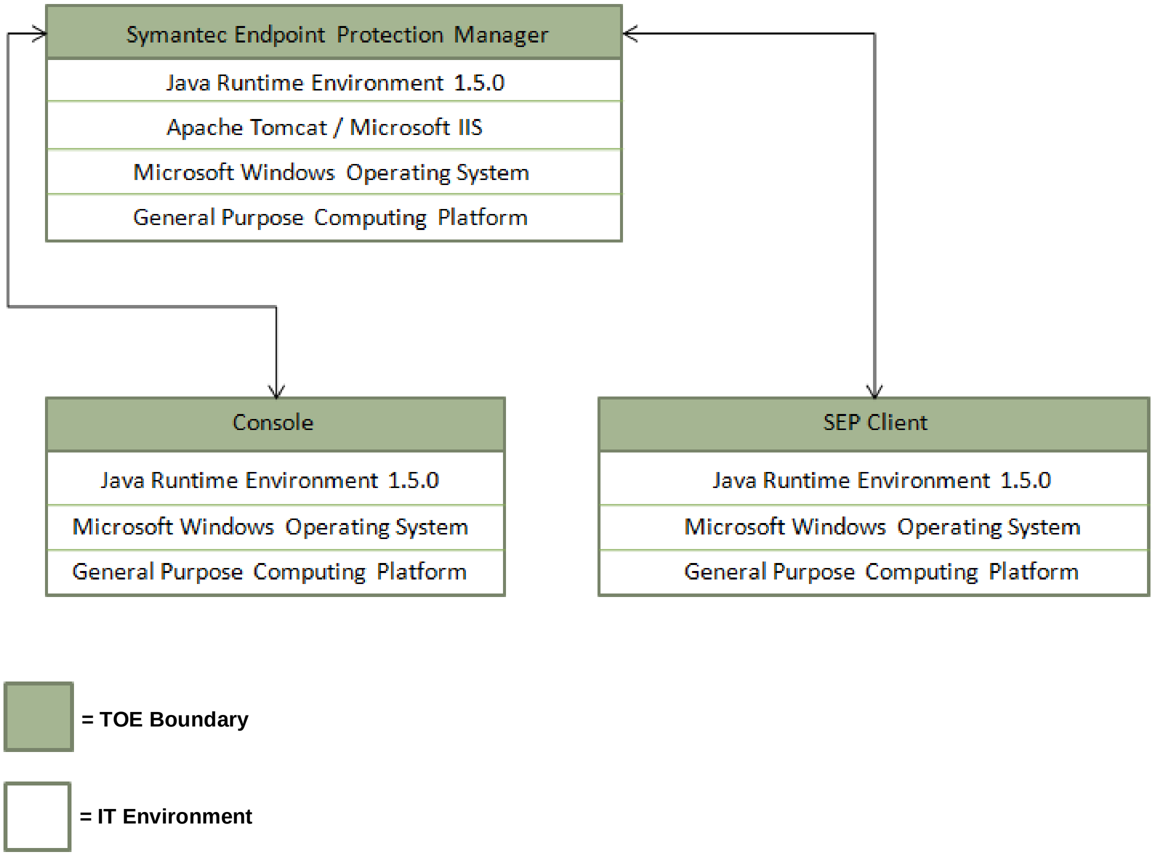
Symantec Endpoint Protection Manager
Java Runtime Environment 1.5.0
Apache Tomcat / Microsoft IIS
Microsoft Windows Operating System
General Purpose Computing Platform
Console
Java Runtime Environment 1.5.0
Microsoft Windows Operating System
General Purpose Computing Platform
SEP Client
Java Runtime Environment 1.5.0
Microsoft Windows Operating System
General Purpose Computing Platform
= TOE Boundary
= IT Environment

Figure 1 – TOE Boundary

2.3.2 Logical Boundaries

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.

2.3.2.1 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.

2.3.2.2 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.

2.3.2.3 Cryptographic Operations

The TOE implements FIPS-approved cryptographic functionality to verify the integrity of the signature files download from Symantec Security Response / Live Update.

2.3.2.4 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.

2.3.2.5 Protection of the TOE

Protection of the TOE is required to ensure the TOE security services are not bypassed or tampered with. The TOE and the OS cooperatively provide this service. Between separate portions of the TOE, secure communication is provided by the IT Environment.

3 TOE Security Environment

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

- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used
- 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

3.1 Secure Use Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The secure use assumptions include assumptions for personnel, physical environment, and operational concerns.

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 operational environment must be managed in accordance with assurance requirements documentation for delivery, operation, and user/administrator guidance. The following specific conditions are assumed to exist in an environment where the TOE is employed.

A.AUDIT_BACKUP Administrators will back up the audit files and monitor disk usage to ensure audit information is not lost.

A.NO_EVIL Administrators are non-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.

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.

3.2 Threats to Security

The TOE or IT environment addresses the threats identified in the following sections.

3.2.1 Threats Addressed by the TOE

The TOE addresses the following threats:

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.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..

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.

3.2.2 Threats Addressed by Operating Environment

The TOE Operating Environment is not required to explicitly address any threats, although the TOE Operating Environment is constrained by the assumptions made above in the Secure Use Assumptions section.

3.3 Organizational Security Policies

The organizational security policies relevant to the operation of the TOE are as follows:

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 that 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.

4 Security Objectives

This section describes the security objectives for the TOE and the TOE's operating environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

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_PROTECTION 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 validated 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.

4.2 Security Objectives for the IT Environment

The IT security objectives for the IT environment are addressed below:

OE.AUDIT_ALARM The IT Environment will provide the capability to produce an audit alarm before the audit log is full.

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 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 within 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.

4.3 Security Objectives for the Non-IT Environment

There are no security objectives for the non-IT environment.

5 IT Security Requirements

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

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table. These security requirements are defined in Sections 5.1 - 5.4.

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_SAR.3	Selectable Audit Review
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.4	Site-Configurable Prevention of Audit Loss
Antivirus	FAV_ACT_EXP.1	Antivirus Actions
	FAV_ALR_EXP.1	Antivirus Alerts
	FAV_SCN_EXP.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
Protection of the TSF	FPT_SEP_EXP.1	Partial TSF Domain Separation

Table 6 – TOE Security Functional Requirements

5.1 TOE Security Functional Requirements

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

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

c) [The events identified in Table 7 – FAU_GEN.1 Events and Additional Information.

]

FAU_GEN.1.2 The TSF shall record within each audit record at last 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 7 – FAU_GEN.1 Events and Additional Information].

SFR	AUDITABLE EVENTS	ADDITIONAL INFORMATION
FAU_GEN.1	None	Not Applicable
FAU_GEN.2	None	Not Applicable
FAU_SAR.1	None	Not Applicable
FAU_SAR.2	None	Not Applicable
FAU_SAR.3	None	Not Applicable
FAU_STG.1	None	Not Applicable
FAU_STG.4	Selection of an action	Action selected
FAV_ACT_EXP.1	Action taken in response to detection of a virus	• Virus detected • Action taken • File or Process where the virus was detected
FAV_ALR_EXP.1	None	Not Applicable
FAV_SCN_EXP.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

SFR	AUDITABLE EVENTS	ADDITIONAL INFORMATION
FMT_SMR.1	None	Not Applicable
FPT_SEP_EXP.1	None	Not Applicable

Table 7 – FAU_GEN.1 Events and Additional Information

5.1.1.2 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.

5.1.1.3 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).

5.1.1.4 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.

Application Note: This SFR applies to read access to the audit records through the TSFIs. The IT Environment (OS) is responsible for prohibiting read access to the audit file via OS interfaces.

5.1.1.5 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches and sorting* of audit data based on

a) [Date and time of the event,

b) Type of event, and

c) Subject identity.

]

5.1.1.6 FAU_STG.1 Protected Audit Trail Storage

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

FAU_STG.1.2 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 applies to both the central management system and the individual workstations.

Application Note: This instance of FAU_STG.1 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.

5.1.1.7 FAU_STG.4 Site-Configurable Prevention of Audit Loss

FAU_STG.4.1 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.4.2 The TSF shall *overwrite the oldest stored audit records* if the audit trail is full and no other action has been selected.

5.1.2 Antivirus (FAV) – Explicitly Stated

5.1.2.1 FAV_ACT_EXP.1 Anti-Virus Actions

FAV_ACT_EXP.1.1 Upon detection of a memory-based virus, the TSF shall prevent the virus from further execution.

FAV_ACT_EXP.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_EXP.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 [TOE policies] and simultaneously permit traffic from authorized processes defined by [TOE policies].

5.1.2.2 FAV_ALR_EXP.1 Antivirus Alerts

FAV_ALR_EXP.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_EXP.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_EXP.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_EXP.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.

5.1.2.3 FAV_SCN_EXP.1 Antivirus Scanning

FAV_SCN_EXP.1.1 The TSF shall perform real-time scans for memory-based viruses based upon known signatures.

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

FAV_SCN_EXP.1.3 The TSF shall perform scheduled scans at the time and frequency configured by the Central Administrator.

FAV_SCN_EXP.1.4 The TSF shall perform manually invoked scans when directed by the Workstation User.

5.1.3 Cryptographic Support (FCS)

5.1.3.1 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 Number 248].

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".

5.1.4 Security Management (FMT)

5.1.4.1 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].

5.1.4.2 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].

5.1.4.3 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

].

5.1.4.4 FMT_SMR.1 Security Roles

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

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.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_SEP_EXP.1 Partial TSF Domain Separation

FPT_SEP_EXP.1.1 The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP.1.2 The TSF shall enforce separation between the security domains of subjects in the TOE Scope of Control.

5.2 Security Functional Requirements for the IT Environment

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The **IT Environment** shall protect the stored audit records in the audit trail **file(s)** from unauthorized deletion.

FAU_STG.1.2 The **IT Environment** shall be able to <u>*prevent*</u> unauthorized modifications to the audit records in the audit trail **file(s)**.

Application Note: This instance of FAU_STG.1 applies to the audit trail file(s) as a whole, while the instance levied against the TOE applies to individual records within the files.

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 The **IT Environment** shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects: [all objects used by the TOE].

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The **IT Environment** shall detect when *[3]* unsuccessful authentication attempts occur related to [the unsuccessful authentication attempts since the last successful authentication for the Central Administrator or Workstation User].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the **IT Environment** shall [lock the respective account and prevent future authentication attempts until reset by an administrator].

5.2.3.2 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The **IT Environment** shall provide a mechanism to verify that secrets meet [strong passwords **sufficient to satisfy SOF-basic requirements**].

5.2.3.3 FIA_UAU.2 User Authentication Before any Action

FIA_UAU.2.1 The **IT Environment** shall require each **Central Administrator or Workstation User** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: Network Users are not subject to the I&A requirements. The Central Administrator and Workstation User are authenticated via the host Operating System.

5.2.3.4 FIA_UAU.6 Re-Authenticating

FIA_UAU.6.1 The **IT Environment** shall re-authenticate the **Central Administrator or Workstation User** under the conditions [the session is locked due to inactivity].

5.2.3.5 FIA_UID.2 User Identification Before any Action

FIA_UID.2.1 The **IT Environment** shall require each **Central Administrator or Workstation User** to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Application Note: Network Users are not subject to the I&A requirements.

5.2.3.6 FIA_PLA_EXP.1 Performance and Log Alerts (EXP)

FIA_PLA_EXP.1.1 The IT environment shall alert the administrator before audit storage reaches capacity.

5.2.4 Protection of the TSF (FPT)

5.2.4.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

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

5.2.4.2 FPT_RVM.1 Non-Bypassability of the TSP

FPT_RVM.1.1 The **IT Environment** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.4.3 FPT_SEP.1 TSF Domain Separation

FPT_SEP.1.1 The **IT Environment** shall maintain a security domain for **the TOE's** own execution that protects **the TOE** from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The **IT Environment** shall enforce separation between the security domains of subjects in the TSC.

5.2.4.4 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The **IT Environment** shall be able to provide reliable time-stamps for **the TOE's** use.

5.2.5 TOE Access (FTA)

5.2.5.1 FTA_SSL.1 TSF-Initiated Session Locking

FTA_SSL.1.1 The **IT Environment** shall lock an interactive session **of the Central Administrator or Workstation User** after [30 minutes] by:

a) Clearing or overwriting display devices, making the current contents unreadable;

b) Disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The **IT Environment** shall require the following events to occur prior to unlocking the **Central Administrator or Workstation User** session: [re-authentication].

5.2.5.2 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Before establishing a user session, the **IT Environment** shall display an advisory warning message regarding unauthorized use of the **system**.

5.3 Security Requirements for the Non-IT Environment

There are no security requirements for the non-IT environment.

5.4 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. The TOE assurance requirements are the Basic Robustness Assurance Package and are equivalent to EAL2 augmented by ALC_FLR.2 and AVA_MSU.1. The assurance components are summarized in the following table:

ASSURANCE CLASS	ASSURANCE COMPONENTS	
Configuration Management	ACM_CAP.2	Configuration items
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Lifecycle Support	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 8 – Security Assurance Requirements

6 TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

The security functions described in the following subsections fulfill the security requirements that are defined in Section 5.1 – TOE Security Functional Requirements. The security functions performed by the TOE are as follows:

- Antivirus
- Audit
- Cryptographic Operations
- Management
- Protection of the TOE

6.1.1 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_EXP.1
- FAV_ALR_EXP.1
- FAV_SCN_EXP.1

6.1.2 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.

REPORT TYPE	DESCRIPTION
Scan	Displays information about antivirus and antispyware scan activity.
System	Displays information about event times, event types, sites, domains, servers, and severity levels.

Table 9 – 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 Sybase 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
- FAU_GEN.2
- FAU_SAR.1
- FAU_SAR.2
- FAU_SAR.3
- FAU_STG.1
- FAU_STG.4

6.1.3 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.

6.1.4 Management

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

6.1.4.1 Security Roles

The TOE maintains three roles: system administrator, administrator, and limited administrator. The AVPP specifies a Central Administrator, Network User, and Workstation User, and these roles are specified in Section 2.2.3 – Operator Roles in the TOE. 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
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 10 – 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 6.1.1 – Antivirus.

6.1.4.2 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.

6.1.4.3 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 10 – 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
- FMT_MTD.1
- FMT_SMF.1
- FMT_SMR.1

6.1.5 TSF Protection

The TOE is integrated into a network, and all SMTP traffic flowing into the network must pass through the services provided by the TOE. Only an approved, authenticated Administrator can install, configure, and modify the TOE components (and all TOE Security Functions), which provides a protected domain for the TSFs.

Communications between the SEPM and Client components are protected via SSL tunnel. Note that this is a configurable option and is not enabled by default.

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

- FPT_SEP_EXP.1

6.2 Security Assurance Measures

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

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES	DESCRIPTION
ACM_CAP.2	CM_DOC	Configuration items: The implementation and documentation of procedures for the development of the TOE, including a configuration list of uniquely identified items. Evidence Title:

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES	DESCRIPTION
		Configuration Management Processes and Procedures: Symantec™ Endpoint Protection Version 11.0
ADO_DEL.1	DEL_DOC	Delivery procedures: The implementation and documentation of procedures for delivering the TOE to a customer in a secure manner. Evidence Title: *Secure Delivery Processes and Procedures: Symantec™ Endpoint Protection Version 11.0*
ADO_IGS.1	IGS_DOC	Installation, generation, and start-up procedures: Documentation provided to the end users instructing the end users how to install and configure the TOE in a secure manner. Evidence Titles: *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Endpoint Protection Version 11.0*
ALC_FLR.2	ALC_DOC	Flaw reporting procedures: Describes how security flaws are tracked and reported. Evidence Title: *Flaw Reporting Procedures: Symantec™ Endpoint Protection Version 11.0*
ADV_FSP.1	FUN_SPEC	Informal functional specification: Functional Specification for the TOE describing the TSF and the TOE's external interfaces. Evidence Title: *Functional Specification: Symantec™ Endpoint Protection Version 11.0*
ADV_HLD.1	HLD_DOC	Descriptive high-level design: System Design for the TOE providing descriptions of the TSF structure in the form of subsystems and the functionality of each subsystem. Evidence Title: *High Level Design and Representation Correspondence Analysis: Symantec™ Endpoint Protection Version 11.0*

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES	DESCRIPTION
ADV_RCR.1	RCR_DOC	Informal correspondence demonstration: The documentation of the correspondence between the TSS, FSP and HLD in specifically provided deliverables. Evidence Title: *High Level Design and Representation Correspondence Analysis: Symantec™ Endpoint Protection Version 11.0*
AGD_ADM.1	ADMIN_GUIDE	Administrator guidance: Documentation provided to the customers instructing the customer how to configure the TOE in a secure manner. Evidence Titles: *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control* *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Endpoint Protection Version 11.0*
AGD_USR.1	USER_GUIDE	User guidance: Documentation provided to the customers instructing the users how to use the TOE. Evidence Title: *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Endpoint Protection Version 11.0*
ATE_COV.1	TEST_COV	Evidence of coverage: Documented correspondence between the security functions and tests. Evidence Title: *Test Plan and Coverage Analysis: Symantec™ Endpoint Protection Version 11.0*
ATE_FUN.1	TEST_DOC	Functional testing: The implementation and documentation of the test procedures including expected and actual results. Evidence Title: *Test Plan and Coverage Analysis: Symantec™ Endpoint Protection Version 11.0*
AVA_MSU.1	ADMIN_GUIDE USER_GUIDE	Examination of guidance: Misleading, unreasonable and conflicting guidance should be absent from the guidance documentation. Evidence Titles:

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES	DESCRIPTION
		Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Endpoint Protection Version 11.0*
AVA_SOF.1	SOF_DOC	Strength of TOE security function evaluation: The documentation for the Strength of Function Assessment. Evidence Title: *Strength of Function Analysis and Vulnerability Assessment: Symantec™ Endpoint Protection Version 11.0*
AVA_VLA.1	VLA_DOC	Developer vulnerability analysis: Vulnerability Assessment of the TOE and its deliverables is performed and documented to ensure that identified security flaws are countered. Evidence Title: *Strength of Function Analysis and Vulnerability Assessment: Symantec™ Endpoint Protection Version 11.0*

Table 11 – Assurance Measures

7 Protection Profile Claims

This Security Target claims conformance to the security requirements, security objectives, and security environment statements for the defined TOE and its environment as they are stated in the *U.S. Government Protection Profile for Anti-Virus Applications for Workstations in Basic Robustness Environments, Version 1.1, April 4, 2006*.

The following table summarizes details that are modified from the Protection Profile and the justification:

ACTION	DESCRIPTION
Addition	FMT_SMF.1 added to O.ADMIN_ROLE rationale in Table 16 – Rationale for TOE Objectives to coincide with mapping in Table 15 – Mapping of TOE Security Functional Requirements and Objectives
Addition	Mapped O.CORRECT_TSF_OPERATION to FAU_GEN.1, FAU_GEN.2, FAU_SAR.1 and FAU_SAR.3 in Table 15 – Mapping of TOE Security Functional Requirements and Objectives based on rationale in Table 16 – Rationale for TOE Objectives
Addition	Mapped O.VIRUS to FAV_ACT_EXP.1, FAV_ALR_EXP.1 and FAV_SCN_EXP.1 in Table 15 – Mapping of TOE Security Functional Requirements and Objectives based on rationale in Table 16 – Rationale for TOE Objectives
Description	Regarding AVA_SOF, the TOE does not have any probabilistic or permutational functions and the only SOF claim that can be made is the overall TOE SOF-basic claim. Thus, the AVA_SOF claims are not applicable.

Table 12 – Modifications from Protection Profile

8 Rationale

8.1 Rationale for Security Objectives of the TOE, IT Environment, and Non-IT Environment

8.1.1 Summary Mapping of Security Objectives

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

THREATS/ ASSUMPTIONS OBJECTIVES	A. AUDIT_BACKUP	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	A.SECURE_UPDATES	T.ACCIDENTAL_ADMIN ERROR	T._AUDIT_COMPROMISE	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.CRYTOGRAPHY																			✓		
O.DOCUMENTED_ DESIGN									✓		✓										
O.MANAGE													✓							✓	
O.PARTIAL_ FUNCTIONAL_TEST										✓	✓										
O.PARTIAL_SELF_ PROTECTION							✓						✓								
O.VIRUS																✓				✓	

THREATS/ ASSUMPTIONS OBJECTIVES	A. AUDIT_BACKUP	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	A.SECURE_UPDATES	T.ACCIDENTAL_ADMIN _ERROR	T._AUDIT_COMPROMISE	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.VULNERABILITY_ ANALYSIS									✓	✓	✓										
OE.AUDIT_ALARM							✓														
OE.AUDIT_BACKUP	✓																				
OE.AUDIT_STORAGE							✓														
OE.DISPLAY_BANNE R																	✓				
OE.DOMAIN_ SEPARATION							✓						✓								
OE.NO_BYPASS							✓						✓								
OE.NO_EVIL		✓																			
OE.PHYSICAL			✓																		
OE.RESIDUAL_ INFORMATION							✓					✓	✓								
OE.SECURE_COMMS				✓																	
OE.SECURE_UPDAT E					✓																
OE.TIME_STAMPS															✓			✓			
OE.TOE_ACCESS								✓						✓				✓			

Table 13 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

8.1.2 Rationale for Security Objectives of the TOE

.

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE

THREAT/POLICY/ ASSUMPTION	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_ALARM:** The IT Environment will provide the capability to produce an audit alarm before the audit log is full. **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 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:**	**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_ALARM** helps prevent the loss of audit records by sending an alarm if the available storage space for the audit log meets a certain threshold. **OE.AUDIT_STORAGE** contributes to 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** con-tributes to countering this threat by ensuring that the

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
	The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	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.
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	**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:**	**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

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
user or program.	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.	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 implementation of the TOE design 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.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.	**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 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	**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

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
	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.	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 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.	**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.

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
	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.NO_BYPASS:** The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	**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** 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.

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
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.	**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.
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

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
		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, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).	**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.
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	**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.

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
distinct from other authorized users.		
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.NO_EVIL: Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	**OE.NO_EVIL:** Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.	**OE.NO_EVIL** restates the assumption.
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.

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
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 14 – Mapping of Threats, Policies, and Assumptions to Objective

8.2 Security Requirements Rationale

8.2.1 Summary of TOE Security Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVE SFR	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_FUNCTIONA_TEST	O.PARTIAL_SELF_PROTECTION	O.VIRUS	O.VULNERABILITY_ANALYSIS
ACM_CAP.2						✓								
ADO_DEL.1	✓													
ADO_IGS.1	✓													
ADV_FSP.1									✓					

OBJECTIVE SFR	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_FUNCTIONA_TEST	O.PARTIAL_SELF_PROTECTION	O.VIRUS	O.VULNERABILITY_ANALYSIS
ADV_HLD.1									✓					
ADV_RCR.1									✓					
AGD_ADM.1	✓													
AGD_USR.1	✓													
ALC_FLR.2						✓								
ATE_COV.1											✓			
ATE_FUN.1											✓			
ATE_IND.2											✓			
AVA_MSU.1	✓													
AVA_SOF.1														✓
AVA_VLA.1														✓
FAU_GEN.1			✓				✓							
FAU_GEN.2			✓				✓							
FAU_SAR.1					✓		✓							
FAU_SAR.2				✓										
FAU_SAR.3					✓		✓							
FAU_STG.1				✓										
FAU_STG.4				✓										
FAV_ACT_EXP.1							✓						✓	
FAV_ALR_EXP.1							✓						✓	
FAV_SCN_EXP.1							✓						✓	
FCS_COP.1								✓						
FMT_MOF.1		✓								✓				

OBJECTIVE SFR	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_FUNCTIONA_TEST	O.PARTIAL_SELF_PROTECTION	O.VIRUS	O.VULNERABILITY_ANALYSIS
FMT_MTD.1		✓								✓				
FMT_SMF.1		✓								✓				
FMT_SMR.1		✓								✓				
FPT_SEP_EXP.1												✓		

Table 15 – Mapping of TOE Security Functional Requirements and Objectives

8.2.2 Sufficiency of Security Requirements

The following table presents a mapping of the TOE Objectives to TOE Security Requirements.

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
O.ADMIN_GUIDANCE: The TOE will provide administrators with the necessary information for secure management.	ADO_DEL.1 ADO_IGS.1 AGD_ADM.1 AGD_USR.1 AVA_MSU.1	**ADO_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, has not been tampered with or corrupted 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. **ADO_IGS.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

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
		and has not been evaluated. The Installation, Generation and Startup (IGS) documentation ensures that once the administrator has followed the installation and configuration guidance the result is a TOE in a secure configuration. **AGD_ADM.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. **AGD_USR.1** is intended for non-administrative users, but could be used to provide guidance on security that is common to both administrators and non-administrators (e.g., password management guidelines). Since the non-administrative users of this TOE are limited to proxy users it is expected that the user guidance would discuss the secure use of proxies and how the single-use authentication mechanism is used. The use of the single-use authentication mechanism would not have to be repeated in the administrator's guide. **AVA_MSU.1** ensures that the guidance documentation is complete and consistent, and notes all requirements for external security measures.
O.ADMIN_ROLE: The TOE will provide an authorized administrator role to	FMT_MOF.1 FMT_MTD.1 FMT_SMF.1	**FMT_SMR.1** requires that the TOE establish a Central Administrator role and **FMT_SMF.1** provides the administrative actions available in

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
isolate administrative actions.	FMT_SMR.1	the TOE. **FMT_MOF.1** and **FMT_MTD.1** specify the privileges that only the Central Administrator may perform.
O.AUDIT_GENERATION: The TOE will provide the capability to detect and create records of security relevant events.	FAU_GEN.1 FAU_GEN.2	**FAU_GEN.1** 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 an ST author adds to this PP. **FAU_GEN.2** 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.2 FAU_STG.1 FAU_STG.4	**FAU_SAR.2** 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 ordinary file). The FAU_STG family dictates how the audit trail is protected. **FAU_STG.1** restricts the ability to delete audit records to the Security Administrator. **FAU_STG.4** defines the actions that must be available to the administrator, as well as the action to be taken if there is no

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
		response. This helps to ensure that audit records are kept until the Security Administrator deems they are no longer necessary. This requirement also ensures that no one has the ability to modify audit records (e.g., edit any of the information contained in an audit record). 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.3	**FAU_SAR.1** and **FAU_SAR.3** provide 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.	ACM_CAP.2 ALC_FLR.2	**ACM_CAP.2** addresses this objective by requiring that 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 by 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.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.3 FAV_SCN_EXP.1 FAV_ALR_EXP.1 FAV_ACT_EXP.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. The **FAU_SAR** family enables the administrator to review the audit events.
O.CRYPTOGRAPHY:	FCS_COP.1	**FCS_COP.1** requires that the

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
The TOE shall use NIST FIPS 140-2 validated cryptographic services.		message digest used to verify integrity of the signature file utilize a FIPS 140-2 Approved cryptographic algorithm.
O.DOCUMENTED_DESIGN: The design of the TOE is adequately and accurately documented.	ADV_FSP.1 ADV_HLD.1 ADV_RCR.1	**ADV_FSP.1** requires that the interfaces to the TOE be documented and specified. **ADV_HLD.1** requires that the high level design of the TOE be documented and specified and that said design be shown to correspond to the interfaces. **ADV_RCR.1** requires that there be a correspondence between adjacent layers of the design decomposition.
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 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1	Restricted privileges are defined for the Central Administrator and Workstation Users. **FMT_MOF.1** defines particular TOE capabilities that may only be used by these 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	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
		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.	FPT_SEP_EXP.1	The explicitly specific component **FPT_SEP_EXP.1** was chosen to ensure the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies. The explicitly specified version was used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the IT environment.
O.VIRUS: The TOE will detect and take action against known viruses introduced to the workstation via network traffic or removable media.	FAV_ACT_EXP.1 FAV_ALR_EXP.1 FAV_SCN_EXP.1	**FAV_SCN_EXP.1** requires that the TOE scan for viruses. **FAV_ACT_EXP.1** requires that the TOE take action against viruses once they detected. **FAV_ALR_EXP.1** defines alerting requirements to ensure the users are aware that a virus was detected.
O.VULNERABILITY_ANALYSIS: The TOE will undergo strength some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	AVA_VLA.1	The **AVA_VLA.1** 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_VLA.1 requires the developer to perform a systematic search for potential vulnerabilities in all the TOE deliverables. For those vulnerabilities that are not eliminated, a rationale must be provided that describes why these vulnerabilities cannot be exploited by a threat agent with a moderate attack potential, which is in keeping with the desired assurance level of this TOE. As with the functional testing, a key element in this component is that an independent assessment of the completeness of

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
		the developer's analysis is made, and more importantly, an independent vulnerability analysis coupled with testing of the TOE is performed. This component provides the confidence that security flaws do not exist in the TOE that could be exploited by a threat agent of moderate (or lower) attack potential to violate the TOE's security policies.

Table 16 – Rationale for TOE Objectives

8.2.3 Summary of IT Environment Security Requirements

The following table provides the correspondence mapping between security objectives for the IT Environment and the requirements that satisfy them.

IT ENVIRONMENT OBJECTIVE SFR	OE.AUDIT_ALARM	OE.AUDIT_STORAGE	OE.DISPLAY_BANNER	OE.DOMAIN_ SEPARATION	OE.NO_BYPASS	OE.RESIDUAL_ INFORMATION	OE.SECURE_COMMS	OE.TIME_STAMPS	OE.TOE_ACCESS
FAU_STG.1		✓							
FDP_RIP.1						✓			
FIA_AFL.1									✓
FIA_SOS.1									✓
FIA_UAU.2									✓
FIA_UAU.6									✓
FIA_UID.2									✓
FIA_PLA_EXP.1	✓								
FPT_ITT.1							✓		
FPT_RVM.1					✓				

IT ENVIRONMENT OBJECTIVE / SFR	OE_AUDIT_ALARM	OE.AUDIT_STORAGE	OE.DISPLAY_BANNER	OE.DOMAIN_ SEPARATION	OE.NO_BYPASS	OE.RESIDUAL_ INFORMATION	OE.SECURE_COMMS	OE.TIME_STAMPS	OE.TOE_ACCESS
FPT_SEP.1				✓					
FPT_STM.1								✓	
FTA_SSL.1									✓
FTA_TAB.1			✓						

Table 17 – Mapping of IT Environment Security Functional Requirements and Objectives

8.2.4 Sufficiency of Security Requirements for the IT Environment

The following table presents a mapping of the IT Environment Objectives to IT Environment Security Functional Requirements.

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
OE.AUDIT_ALARM The IT Environment will provide the capability to produce an audit alarm before the audit log is full.	FIA_PLA_EXP.1	**FIA_PLA_EXP.1** requires the OS to send an alarm if the available storage space for the audit log meets a certain threshold.
OE.AUDIT_STORAGE: The IT environment will provide a means for secure storage of the TOE audit log files.	FAU_STG.1	**FAU_STG.1** requires the OS to protect the audit log file from unauthorized deletion.
OE.DISPLAY_BANNER: The system will display an advisory warning regarding use of the system.	FTA_TAB.1	**FTA_TAB.1** meets this objective by requiring the system to display a banner before a user can establish an authenticated session.
OE.DOMAIN_SEPARATION: The IT environment will provide an isolated domain for the execution of the TOE.	FPT_SEP.1	**FTP_SEP.1** requires the OS to provide an isolated domain for the TOE.

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
OE.NO_BYPASS: The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	FPT_RVM.1	**FPT_RVM.1** requires the OS to ensure that the TOE will not be bypassed.
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.	FPT_RIP.2	**FDP_RIP.2** is used to ensure the contents of resources are not available to subjects other than those explicitly granted access to the data.
OE.SECURE_COMMS: The IT environment will provide a secure line of communications between distributed portions of the TOE.	FPT_ITT.1	**FPT_ITT.1** ensures that secure communication between the central management system and the workstations will be available to the TOE.
OE.TIME_STAMPS: The IT environment will provide reliable time stamps.	FPT_STM.1	**FPT_STM.1** requires that the IT Environment provide time stamps for the TOE's use.
OE.TOE_ACCESS: The IT Environment will provide mechanisms that control a user's logical access to the TOE.	FIA_AFL.1 FIA_SOS.1 FIA_UID.2 FIA_UAU.2 FIA_UAU.6 FTA_SSL.1	**FIA_AFL.1** provides a detection mechanism for unsuccessful authentication attempts by remote administrators, authenticated proxy users and authorized IT entities. The requirement enables a Security Administrator settable threshold that prevents unauthorized users from gaining access to authorized user's account by guessing authentication data by locking the targeted account. Thus, limiting an unauthorized user's ability to gain unauthorized access to the TOE. **FIA_SOS.1** ensures that the strength of the I&A mechanism will be adequate. **FIA_UID.2** requires that a user be identified to the TOE in order to access to the TOE. **FIA_UAU.2** requires that a user be authenticated by the TOE before accessing the TOE. **FIA_UAU.6** requires that a user be re-authenticated after a session is locked. **FTA_SSL.1** requires that sessions be

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
		locked after a period of inactivity. The combination of these SFRs ensures that users will successfully complete an I&A process of sufficient strength before they can gain access to the TOE.

Table 18 – Rationale for IT Environment Objectives

8.3 TOE Summary Specification Rationale

The following table provides a mapping of Security Functional Requirements to IT Security Functions:

IT SECURITY FUNCTION / SFR	ANTIVIRUS	AUDIT	CRYPTOGRAPHIC OPERATION	MANAGEMENT	TSF PROTECTION
FAU_GEN.1		✓			

IT SECURITY FUNCTION SFR	ANTIVIRUS	AUDIT	CRYPTOGRAPHIC OPERATION	MANAGEMENT	TSF PROTECTION
FAU_GEN.2		✓			
FAU_SAR.1		✓			
FAU_SAR.2		✓			
FAU_SAR.3		✓			
FAU_STG.1		✓			
FAU_STG.4		✓			
FAV_ACT_EXP.1	✓				
FAV_ALR_EXP.1	✓				
FAV_SCN_EXP.1	✓				
FCS_COP.1			✓		
FMT_MOF.1				✓	
FMT_MTD.1				✓	
FMT_SMF.1				✓	
FMT_SMR.1				✓	
FPT_SEP_EXP.1					✓

Table 19 – Mapping of Security Functional Requirements to IT Security Functions

8.3.1 Sufficiency of IT Security Functions

This section provides appropriate justification that the IT Security Functions are suitable to meet the TOE Security Functional Requirement and that when implemented, contributes to meeting that requirement.

SFR	RATIONALE TO SUPPORT SUFFICIENCY OF SECURITY FUNCTION
FAU_GEN.1	This TOE SFR is satisfied by the Audit which generates audit logs from the audit of a variety of security events.
FAU_GEN.2	This TOE SFR is satisfied by the Audit function, which generates audit logs with details on the actions of identified users.

SFR	RATIONALE TO SUPPORT SUFFICIENCY OF SECURITY FUNCTION
FAU_SAR.1	This TOE SFR is satisfied by the Audit function, which provides the Central Administrator with the capability to review all TOE audit records.
FAU_SAR.2	This TOE SFR is satisfied by the Audit function by enabling only authorized users to review and query the audit logs based on the certain criteria.
FAU_SAR.3	This TOE SFR is satisfied by the Audit function, which allows users of the TOE to search and sort audit records.
FAU_STG.1	This TOE SFR is satisfied by the Audit function, which protects audit records from unauthorized deletion or modification.
FAU_STG.4	This TOE SFR is satisfied by the Audit function, which allows the administrator to define TOE actions if the audit records consume all available memory.
FAV_ACT_EXP.1	This TOE SFR is satisfied by the Antivirus function, which specifies TOE actions in the event a memory-based or file-based virus is detected.
FAV_ALR_EXP.1	This TOE SFR is satisfied by the Antivirus function, which displays alerts when in the event a memory-based or file-based virus is detected.
FAV_SCN_EXP.1	This TOE SFR is satisfied by the Antivirus function, which specifies scanning parameters (i.e., real-time and on-demand) for viruses.
FCS_COP.1	This TOE SFR is satisfied by the Cryptographic Support function, which requires integrity verification of signatures downloaded to the TOE.
FMT_MOF.1	This TOE SFR is satisfied by the Management function, which specifies that only a Central Administrator is authorized to configure the auditing and virus scanning parameters of the TOE.
FMT_MTD.1	This TOE SFR is satisfied by the Management function, which specifies the configuration actions available to the Central Administrator and Workstation Users.
FMT_SMF.1	This TOE SFR is satisfied by Management function, which specifies the management functions available in the TOE.
FMT_SMR.1	This TOE SFR is satisfied by Management function, which assigns each user to the role of Central Administrator, Workstation User, or Network User.
FPT_SEP_EXP.1	The TOE provides protection mechanisms for its security functions, such as the restricted ability that only TOE Administrators can perform administrative actions on the TOE (e.g., untrusted subjects cannot initiate management TOE actions).

Table 20 – Sufficiency of IT Security Functions

8.4 Rationale for IT Security Requirement Dependencies

Each functional requirement, including explicit requirements was analyzed to determine that all dependencies were satisfied. All requirements were then analyzed to determine that no additional dependencies were introduced as a result of completing each operation. Table 21 – TOE SFR Dependency Rationale identifies the functional requirement and its correspondent dependency. Table 22 – Unsupported SFR Dependency Rationale provides the analysis and rationale for dependencies not required in this PP.

In Table 21 – TOE SFR Dependency Rationale, the “Component” column lists all of the components included in this ST; each one is assigned a unique ID number in the “ID” column. Each component’s dependencies (from the CC) are listed in the “Dependency” column. The “Satisfied” column indicates how the dependencies are satisfied, with the number referencing the ID number of the component included in the PP that satisfies the dependencies. “Not Applicable” is used when there are no dependencies for a component, and a reference to Table 22 – Unsupported SFR Dependency Rationale is included when the dependency is not met but justified in Table 21 – TOE SFR Dependency Rationale.

ID	COMPONENT	DEPENDENCY	SATISFIED
1	FAU_GEN.1	FPT_STM.1	26
2	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	1 17
3	FAU_SAR.1	FAU_GEN.1	1
4	FAU_SAR.2	FAU_SAR.1	3
5	FAU_SAR.3	FAU_SAR.1	3
6	FAU_STG.1	FAU_GEN.1	1
7	FAU_STG.4	FAU_GEN.1 FAU_STG.1	1 6
8	FAV_ACT_EXP.1	FAV_SCN_EXP.1 FMT_SMR.1	10 21
9	FAV_ALR_EXP.1	FAV_SCN_EXP.1 FMT_SMR.1	10 21
10	FAV_SCN_EXP.1	FMT_SMR.1	21
11	FCS_COP.1	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	No – see following table for rationale
12	FDP_RIP.1	None	Not Applicable
13	FIA_AFL.1	FIA_UAU.1	15

ID	COMPONENT	DEPENDENCY	SATISFIED
14	FIA_SOS.1	None	Not Applicable
15	FIA_UAU.2	FIA_UID.1	17
16	FIA_UAU.6	None	Not Applicable
17	FIA_UID.2	None	Not Applicable
18	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	20 21
19	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	20 21
20	FMT_SMF.1	None	Not Applicable
21	FMT_SMR.1	FIA_UID.1	17
22	FPT_ITT.1	None	Not Applicable
23	FPT_RVM.1	None	Not Applicable
24	FPT_SEP.1	None	Not Applicable
25	FPT_SEP_EXP.1	None	Not Applicable
26	FPT_STM.1	None	Not Applicable
27	FTA_SSL.1	FIA_UAU.1	15
28	FTA_TAB.1	None	Not Applicable
29	FIA_PLA_EXP.1	None	Not Applicable

Table 21 – TOE SFR Dependency Rationale

8.4.1 Rationale for Unsupported SFR Dependencies

The following table provides a rationale for dependencies that are not supported:

ID	COMPONENT	DEPENDENCY
FCS_COP.1	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	The only cryptographic function included is a message digest, which does not use keys.

Table 22 – Unsupported SFR Dependency Rationale

8.5 Rationale for Explicitly Stated Requirements

The following table presents the rationale for the inclusion of the explicitly stated requirements found in this document.

EXPLICIT REQUIREMENT	RATIONALE
FAV_ACT_EXP.1	This component defines the actions to be taken by the TOE when a virus is detected. Existing security policy SFRs (e.g., FDP_ACF and FDP_IFF) focus on the access to or flow of user data and are not suitable for the actions taken by Anti-Virus products.
FAV_ALR_EXP.1	This component defines the alerting mechanism to be used to inform users when a virus is detected. The mechanism involves an acknowledgement from Workstation Users or Central Administrators that is not accounted for in CC SFRs.
FAV_SCN_EXP.1	This component defines the scanning to be performed by the TOE to detect viruses. Existing security policy SFRs (e.g., FDP_ACF and FDP_IFF) focus on the access to or flow of user data and are not suitable for the mechanisms used by Anti-Virus products.
FIA_PLA_EXP.1	This component is required to meet PD-0129, which requires an alarm to be generated when the audit log is full.
FPT_SEP_EXP.1	The CC FPT_SEP component cannot be satisfied by application TOEs. This component defines the separation that may be performed by applications. It is drawn from the Basic Robustness Consistency Instruction Manual.

Table 23 – Rationale for Explicitly Stated Requirements

8.6 Rationale for Security Assurance Requirements

The EAL definitions and assurance requirements in Part 3 of the CC were reviewed and the *Basic Robustness Assurance Package* as defined in Section 5.4 was believed to best achieve the goal of addressing circumstances where developers and users require a low level of independently assured security in commercial products. The assurance package was selected because the TOE is an application executing on a system outside the TOE boundary, and basic is the highest robustness level available to application TOEs.

8.7 Rationale for Strength of Function Claim

Part 1 of the CC defines “strength of function” in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels defined in Part 1: SOF-basic, SOF-medium and SOF-high. SOF-basic is the strength of function level chosen for this PP. SOF-basic states, “a level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.” The rationale for choosing SOF-basic was to be consistent with the Basic Robustness guidelines.

8.8 Rationale for Protection Profile Claims

There are no differences in the TOE security requirements and security objectives defined in this Security Target and those of *U.S. Government Protection Profile for Anti-Virus Applications for Workstations in Basic Robustness Environments, Version 1.1, April 4, 2006.*A security requirement was defined for the IT Environment to adhere to PD-0129, and an objective for the environment was respectively added to enforce the requirement.