Security Target

VirusScan 8.5i
and
ePolicy Orchestrator 3.6.1

McAfee ®

System Protection

Industry-leading intrusion prevention solutions

McAfee®
Proven Security™

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

CC ..... Common Criteria
EAL2 ..... Evaluation Assurance Level 2
IT ..... Information Technology
NIAP ..... National Information Assurance Partnership
PP ..... Protection Profile
SF ..... Security Function
SFP ..... Security Function Policy
SOF ..... Strength of Function
ST ..... Security Target
TOE ..... Target of Evaluation
TSC ..... TSF Scope of Control
TSF ..... TOE Security Function
TSFI ..... TSF Interface
TSP ..... TOE Security Policy

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for VirusScan Enterprise v8.5i (VSE) and its management utility ePolicy Orchestrator v3.6.1.(ePO). The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.2*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9* and all National Information Assurance Partnership (NIAP) and international interpretations through May 6, 2006. As such, the terms are presented using internationally accepted English spelling.

1.1 Security Target Reference

VirusScan Enterprise v8.5i, ePolicy Orchestrator Security v3.6.1 Security Target, document number E2-1005-016(6), dated May 23, 2007

1.2 TOE Reference

McAfee VirusScan Enterprise v8.5i and McAfee ePolicy Orchestrator v3.6.1.

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 augmented with ALC_FLR.2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation, Version 2.2*.

1.4 Keywords

Virus, viruses, computer, anti-virus, antivirus, virus scan, virusscan, Trojan, worms, security, security target, McAfee, COACT, Common Criteria.

1.5 TOE Overview

McAfee VirusScan Enterprise v8.5i (VSE) is an anti-virus end-point solution that detects and cleans virus-infected files before they enter the corporate network**.** McAfee ePolicy Orchestrator v3.6.1 (ePO) provides management capabilities to VSE, although a VSE client agent also runs on the ePO server to help it protect itself. VSE and ePO provide a high degree of user configurability to customize the management of viruses and virus-infected files. Together, VSE and ePO comprise the TOE.

This security target describes the evaluated functionality of the TOE that is consistent with the *U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness, v1.1*, April 4, 2006. There may be other security functionality that exists in the products that has not been evaluated because the functionality has been not cited in the Protection Profile.

1.5.1 Security Target Organisation

- Chapter 1 of this ST provides introductory and identifying information for the TOE.
- Chapter 2 describes the TOE and provides some guidance on its use.
- Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

- Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.
- Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.
- Chapter 6 is the TOE Summary Specification, a description of the functions provided by the VSE to satisfy the security functional and assurance requirements.
- Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).
- Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.6 Common Criteria Conformance

The TOE (VSE and ePO) is compliant with the Common Criteria (CC) Version 2.2, functional requirements (Part 2) conformant and assurance requirements (Part 3) conformant for EAL2 augmented with ALC_FLR.2.

1.7 Protection Profile Conformance

The TOE claims conformance to the *U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness, v1.1,* April 4, 2006.

1.8 Conventions

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with Times New Roman bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

Descriptions of Graphic User Interface (GUI) menu titles are indicated in Arial Narrow bold text.

CHAPTER 2

2. TOE Description

This section provides the context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 TOE Description: VSE and ePO

VSE is an anti-virus product. ePO is a security policy management product that integrates with VSE to provide management capabilities. VSE detects, blocks and removes viruses and malware to safeguard multi-tiered enterprise networks. VSE scans inbound and outbound traffic, stopping malicious code at the gateway before it can enters the enterprise network.

This Security Target defines the requirements for VSE and its management system McAfee ePO. The TOE consists of both McAfee products: VSE and ePO. McAfee VSE is a software package designed to protect enterprise networks from viruses, worms, Trojans, as well as unwanted code and programs. VSE can be configured to scan local and network drives, as well as Microsoft Outlook and Lotus Notes email messages and attachments. It is possible to configure VSE to respond to infections and malicious code that it finds by identifying the intrusive files, removing them, and reporting on them. The management capabilities for VSE are provided by ePO.

ePO distributes and manages VSE agents that reside on client systems. By using ePO you can manage a large enterprise network by creating replicated distributed repositories of anti-virus signature files (e.g. DAT files) on disparate networks, in different geographic locations. A centralized but distributed architecture allows the VSE software to be centrally managed and yet decrease network traffic required to update clients. A full DAT update is around 3Mb. If there are 100 client systems at a remote office, pulling up the update from the central server would require the 3Mb DAT file to be pulled across the WAN 100 times. By positioning replica repositories in each office, the update traffic remains isolated on the remote network.

ePO also provides scheduling capabilities to enforce VSE security policies, and maintain event files which are used for auditing.

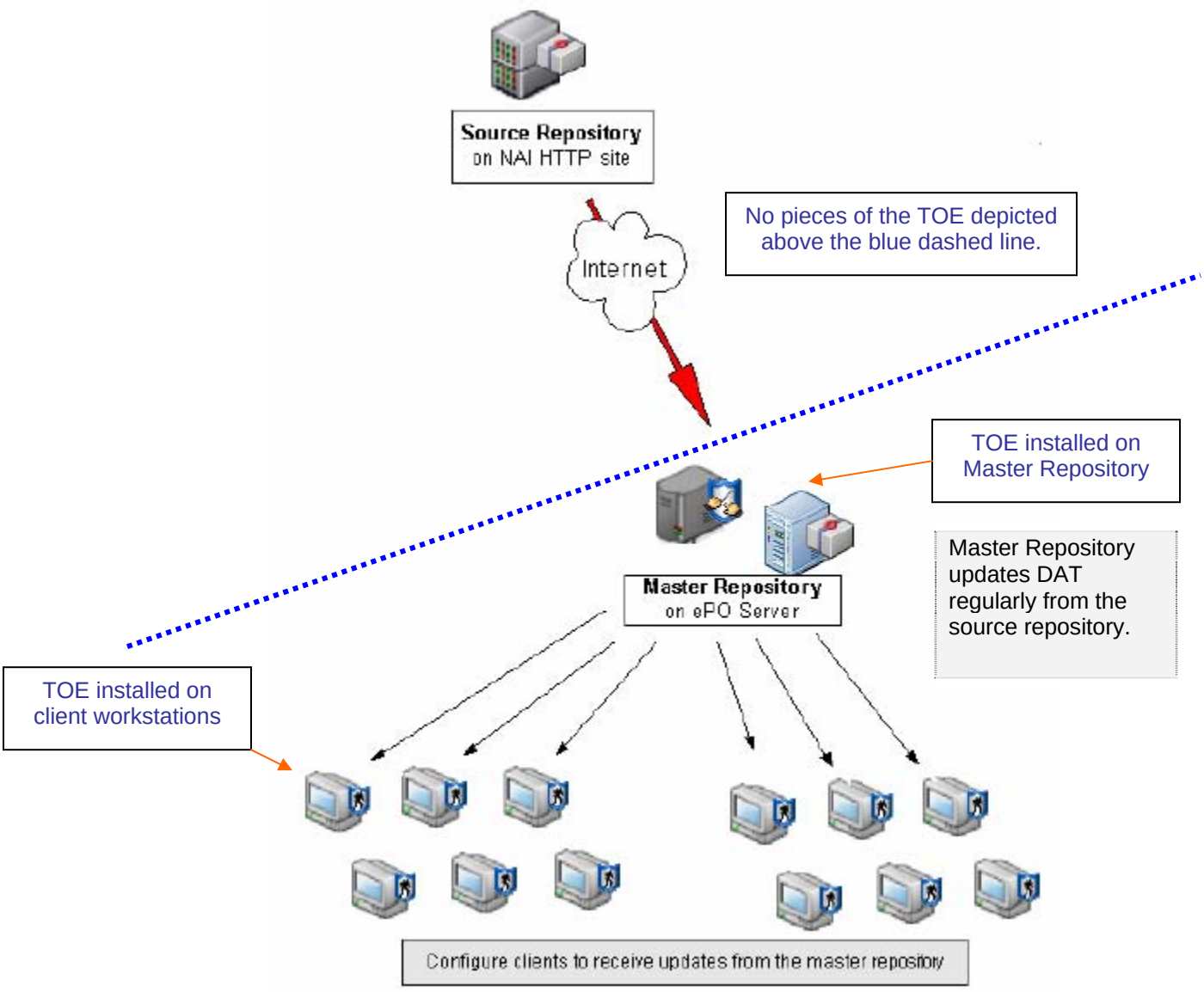
2.1.1 Physical Boundary

The physical components of the TOE includes the software that is installed during installation of both VSE and ePO. The TOE software is installed on a centralized Master Repository server and on client workstations. The computer hardware platform that the TOE software is installed on is not part of the TOE and is outside the boundary of the TOE. All hardware peripherals of the computer hardware platform such as printers and other hardware devices are also outside the boundary of the TOE.

A representation of the TOE is depicted in Figure 1. Both components of the TOE are installed on systems with resident operating systems, but the operating systems are not part of the TOE. The TOE distributes updates of signature files through a Master Repository made available to client systems.

ePO requires a database, but the database is not part of the TOE. Database requirements for the IT environment are noted in Table 5.

Figure 1 - Physical Boundary



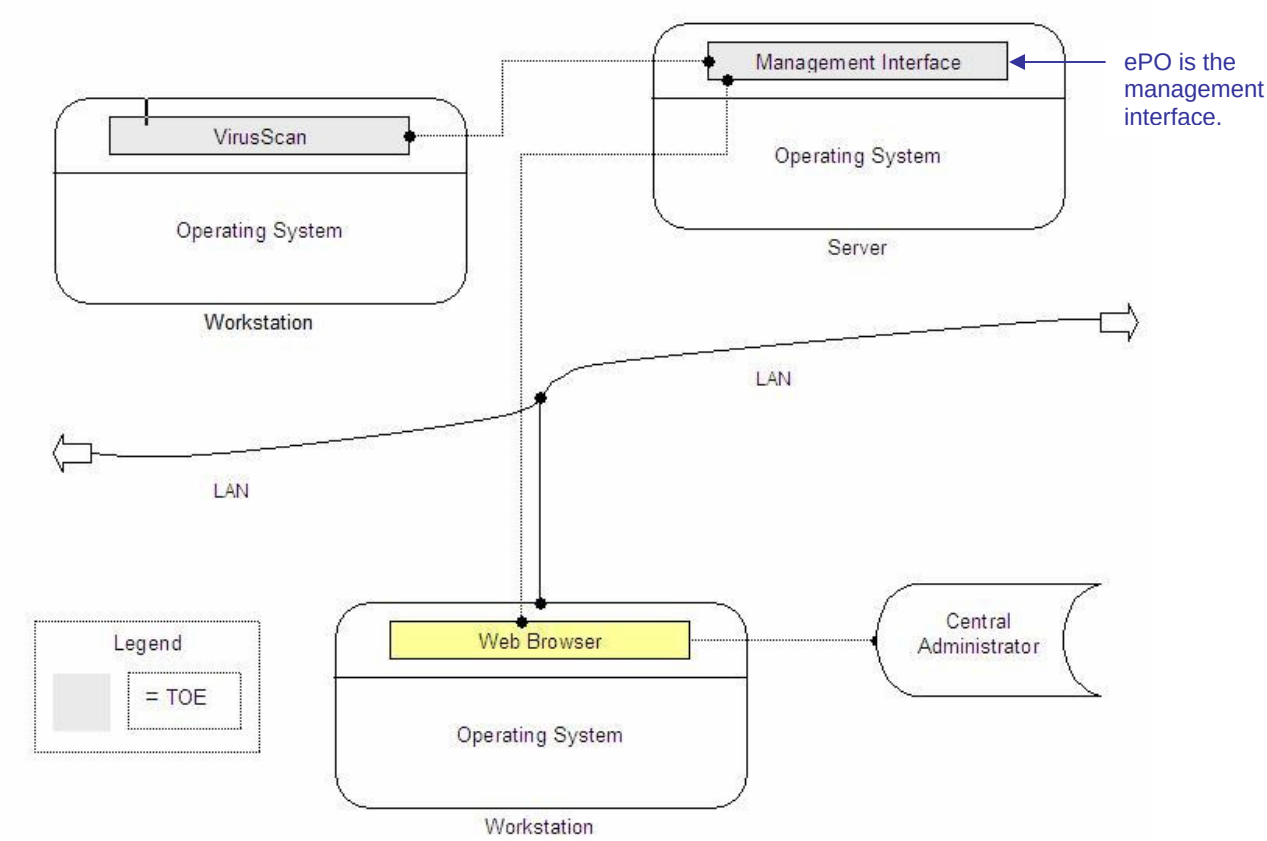
2.1.2 Logical Boundary

The TOE includes management interfaces that the administrator uses to configure and define the information flow policy and review the log files. The Management Interface is provided by ePO and is depicted in Figure 2. The virus scanning functionality is provided by VSE and is depicted in Figure 2.

The logical boundaries of the TOE include the security functionalities that the TOE provides to the system that utilize the product for the detection of viruses and malicious code. The security functions include Audit, Management, Virus Scanning and Alerts, Protection of the TOE, and Cryptographic operations. Identification and authentication

are provided by the TOE environment. The logical boundaries of these functions are depicted in Figure 2.

Figure 2 - Logical Boundaries of the TOE



2.1.3 TSF Functions Summary

Virus Scanning & Alert security functionality:

A) Access Protection - This function protects ports, files, and processes resident in memory from intrusions by restricting access to them. You can create rules to block either inbound or outbound ports, and by doing so, restrict access to files and residual data allocated in memory. If an outbreak occurs, the administrator can restrict access to the infected areas to prevent further infection until new signature files are released.

B) Email Scanning - This function provides scanning of messages and databases in order to identify viruses, worms, and Trojans for the purpose of removing them and reporting on them.

C) Depth of Scan - This function enables the user to set the depth of the scan on manual scans of archive file types.

D) Automatic Updates – Allows signature (DAT) files automatically per the configured schedule.

The TOE's ePO security functions include:

A) Audit –The OnAccess Scan Log provides auditing capabilities and event logs can be reviewed from the EPO console. Auditing also takes place on the workstation being scanned.

B) Management – Enables the Central Administrator to centrally manage virus scan settings on workstations, configure and manage the actions the virus scan component takes when detection of an infection occurs, and manage the audit logs.

C) Cryptographic Operations - VirusScan anti-virus packages are encrypted using a key pair that uses the Digital Signature Algorithm (DSA) and is then encrypted using 168 bit key 3DES and pushed to the workstation.

D) Protection of the TOE – The TOE provides for self protection and ensures that of functions within the TOE's scope of control (TSC). The TOE protects itself from tampering and interference from untrusted subjects at the TSFI's of the TOE.

2.1.4 TSF Data

The TSF data includes virus signatures that the TOE uses for the purpose of identifying viruses. The virus signatures are sometimes alternatively referred to as "virus signature files" or "DAT files." Additionally, Digital signatures and audit records are TSF Data.

2.1.4.1 Security Attributes

The security attributes the TOE uses are user roles for determining actions a user can take and setting the virus scanning for setting to scan all processes, or based on whether a process is classified as having a low-risk or high-risk of infection.

2.1.5 User Data

The virus-detection, monitoring and managing capabilities of the TOE services ensures that the information received from the network is free of any potential risks. The User Data is the files that are either read from, or written to the computer the TOE client agent is installed on that are being scanned.

2.1.6 Rationale for Non-Bypassability and Separation

The TOE is an application that executes on top of an underlying system that includes hardware and software required for operation. Therefore, responsibility for non-bypassability and separation are split between the TOE and the IT Environment.

All access to objects in the TOE IT environment is validated by the IT environment security policies before they can succeed. Unless a user has been authenticated by the IT environment, the user will not be able to access any of the TOE security functions or any of the TOE files or directories. Arbitrary entry into the TOE is not possible and therefore the TSF is protected against external interference by untrusted objects.

Because the TOE is isolated in its own domain, the TOE's IT environment maintains and controls execution for the TSF separately from other processes.

The TOE provides strictly controlled functionality to the users within the TSC. By limiting access through role based access control, the TSF is protected from corruption or compromise from users within the TSC. The TOE interfaces are separated into 2 categories – security enforcing and security supporting. Security enforcing interfaces invoke the TSF and ensure that all enforcement functions complete successfully before allowing the user invoked action to proceed. Security supporting interfaces ensure that the TSF cannot be interfered with via those interfaces (i.e., they are isolated from the TSF). The security enforcing role is separate from the security supporting role and each role has its own unique set of privileges associated with it. Multiple simultaneous users (and roles) are supported.

The TOE associates distinct attributes and privileges with each process and restricts access according to the configured security policies. (A process is a program in execution.) Processes are separate from each other, each with their own memory buffer and it is impossible for one process to directly access the memory of another. The OS and hardware support non-bypassability by ensuring that access to protected resources pass through the TOE and is limited to access within the OS scope of control which is enforced by the security policies for the OS and the IT environment. The hardware and OS provide separate process spaces in which the TOE executes; these process spaces are protected from interference from other processes except through the defined TOE interfaces.

2.2 Evaluated Configuration

In this section, the evaluated environment configurations are described for both components of the TOE.

2.2.1 VirusScan v8.5i Configuration

VSE operates using a client-server architecture. The TOE requires server and client computers with Intel Pentium or Celeron processor of at least 166MHz. The processor is not part of the TOE, but is required by the TOE. Both the server and client workstations also require:

A) Microsoft Internet Explorer version 5.0 or later

B) 32mb of RAM based on the Microsoft operating guidelines of minimum RAM

C) A CD-ROM drive

The server and client workstations have different configuration requirements. There are different configuration options available for the operating system for both the server and client workstations. The operating system is not part of the TOE but is required by the TOE.

Server operating system configuration options (outside the scope of the TOE) for the VSE server are listed in the following table:

Table 1 - Operating System Options for VSE Server

Environment Operating Systems Options for VSE Server	
Operating System (one of the listed versions is required)	Windows NT Server 4.0 with Service Pack 6 or 6a
	Windows Server 2003 Standard Edition
	Windows Server 2003 Enterprise Edition
	Windows 2000 Server with Service Pack 3 or 4

Client workstation operating system configuration options are listed in the following table:

Table 2 - Operating System Options for VSE Client

Environment Operating Systems Options for VSE Client System	
Operating System (one of the listed versions is required)	Windows 2000 Professional with Service Pack 3 or 4
	Windows XP Home and Professional with Service Pack 1, RC2
	Windows XP Table PC

Other requirements for both server and client workstations include adequate disk space and are listed in Table 3.

Table 3 - Disk Space Requirements for VSE

Disk Space Requirements for VSE
38Mb for a complete installation of all the program's features and components
22Mb used during the installation process that is then freed up when the installation is complete.
40Mb if you are using a management tool to deploy VirusScan. This space is normally freed when installation has completed depending on the management tool you are using.

2.2.2 ePO Configuration

ePO operates as a distribution system and management system for a client-server architecture offering components for the server part of the architecture (not the clients).

The ePO server requires a dedicated computer with an Intel Pentium II-class (or higher) processor of at least 500MHz.

Other hardware and network components and configuration requirements for the ePO server (outside the scope of the TOE) are listed in Table 4.

Table 4 - Hardware and Network Components Required for ePO Server

Hardware and Network Environment Requirements	
Memory	512mb RAM, 1GB recommended
Monitor	1024 x 768; 256 color, VGA monitor
NIC	Network Interface Card with 100mb capacity
File system	NTFS partition
IP Address	Static IP Address
Free Disk Space	250 MB minimum for a first time installation, 650 MB minimum for an upgrade; 2Gb recommended

The ePO server also requires a database that is not part of the TOE. If managing more than 5,000 clients, the database server should be a dedicated server with a dedicated network connection. If the database server uses the same computer (hardware) as the ePO server, two-thirds of the memory should be use for the database, e.g. if the server has 1GB RAM, then 660MB should be used as fixed memory for the SQL Server 2000. The database is part of the TOE environment. (The database cannot be installed on a backup Domain Controller.)

Software and operating system components (outside the scope of the TOE) that are required for the ePO server are listed in Table 5.

Table 5 - Software Components and Requirements for the ePO Server

Software Components and Requirements of the Environment	
Operating System (one of the listed versions is required)	Windows 2000 Advanced Server with Service Pack 2
	Windows 2000 Server
	Windows 2003 Enterprise
	Windows 2003 Standard
	Windows 2003 Web
Database (one of the following is required)	Microsoft SQL Server 2000 Standard with SP 3
	Microsoft SQL Server 2000 Enterprise with SP 3
	Microsoft SQL Server 7 Standard with SP 3 or 4
	Microsoft SQL Server 7 Enterprise with SP 3 or 4

Browser	Microsoft Internet Explorer v6.0
Domain Controller	The server must have a trust relationship with the Primary Domain Controller (PDC) on the network.

2.2.3 VSE Functionality Not Included in the Evaluation

The functionality of VSE that is not included in this evaluation includes:

A) The ability to protect against buffer overflows

B) The ability to identify spyware

C) The Scriptscan feature that scans JavaScript and VBScript scripts

D) The ability to update the TOE (scan engine). Note that the ability to update the virus signatures is included in the evaluation.

E) The optional Alert Manager product

F) The ability to scan email

2.2.4 Specific Configuration Options

The following options must be configured in the TOE in order to be in the evaluated configuration:

A) Remote viewing of ePO log files is disabled. On the logging tab of the ePO Agent 3.6.1 Configuration policy page ensure that that Enable remote access to log option is not selected.

B) Only authorized processes may initiate network connections to remote port 25 (SMTP). The Central Administrator configures the list of authorized processes.

CHAPTER 3

3. Security Environment

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

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

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 6 - Assumptions

A.Type	Description
A.AUDIT_BACKUP	Administrators will back up 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 administrative guidance.
A.PHYSICAL	It is assumed that the appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
A.SECURE_COMMS	It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
A.SECURE_UPDATES	Administrators will implement secure mechanisms for receiving and validating updated signature files from the Anti-Virus vendors, and for distributing the updates to the central management systems.

3.3 Threats

The threats to security that are addressed by the TOE are found in the following table:

Table 7 - Threats

T.Type	TOE Threats
T.ACCIDENTAL_ADMIN_ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

T.Type	TOE Threats
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.

3.4 Organisational Security Policies

The TOE requires Organisational Security Policies as listed in the following table:

Table 8 - Organisational Security Policies

Policy	Policy Description
P.ACCESS_BANNER	The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e. encryption, decryption, signature, hashing, key exchange, and random number generation services)

Policy	Policy Description
P.MANUAL_SCAN	The authorized users of the workstations shall initiate manual anti-virus scans of removable media (e.g., floppy disks, CDs) introduced into the workstation before accessing any data on the removable media.
P.ROLES	The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

This page left blank intentionally

CHAPTER 4

4. Security Objectives

This section identifies the security objectives of the TOE, the TOE's environment. The security objectives identify the responsibilities of the TOE, the TOE's environment. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the objectives listed in the following table:

Table 9 - Security Objectives for the TOE

O.Type	Security Objective
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 from unauthorized access.
O.AUDIT_REVIEW	The TOE will provide the capability to view audit information in a human readable form.
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 the customer's site.
O.CRYPTOGRAPHY	The TOE shall use NIST FIPS 140-2 cryptographic services.
O.DOCUMENTED_DESIGN	The design of the TOE is adequately and accurately documented.
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security 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 Environment

The TOE's IT environment must satisfy the objectives listed in the following table:

Table 10 - Security Objectives of the IT Environment

OE.Type	IT Environment Security Objective
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_SEARCH	The IT Environment will provide the capability to search and sort the audit information.
OE.AUDIT_STORAGE	The IT Environment will provide a means for secure storage of the TOE audit log files.
OE.DISPLAY_BANNER	The IT environment will display an advisory warning regarding the use of the system.
OE.DOMAIN_SEPARATION	The IT environment will provide an isolated domain for the execution of the TOE.
OE.NO_BYPASS	The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.
OE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrative guidance.
OE.PHYSICAL	Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
OE.RESIDUAL_INFORMATION	The IT environment will ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated.
OE.SECURE_COMMS	The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
OE.SECURE_UPDATES	Enterprises using the TOE shall ensure that signature file updates are received from the vendor via secure mechanisms, the updates are validated before being used, and the updates are distributed to central management systems with the Enterprise via secure mechanisms.
OE.TIME_STAMPS	The IT Environment will provide reliable time stamps.
OE.TOE_ACCESS	The IT environment will provide mechanisms that control a user's logical access to the TOE.

Application Note: OE.AUDIT_SEARCH has been added to the security objectives of the IT Environment in conformance to the PP errata sheet concerning FAU_SAR.3.

4.3 Security Objectives for the Non-IT Environment

There are no Security Objectives for the TOE's Non-IT environment.

CHAPTER 5

5. IT Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

5.1 TOE Security Functional Requirements

The functional requirements for the TOE consist of the following components derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.2* - with the exception of italicised items listed in brackets. These bracketed items include either "assignments" that are TOE specific or "selections" from the Common Criteria that the TOE enforces. The TOE Security Functional Requirements are listed in the following table:

Table 11 - TOE Security Functional Requirements

Component	Name
FAU_GEN.1-NIAP-0347	Audit Data Generation
FAU_GEN.2-NIAP-0410	User Identity Association
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_STG.1-NIAP-0429	Protected Audit Trail Storage
FAU_STG.NIAP-0414-NIAP-0429	Site-Configurable Prevention of Audit Loss
FAV_ACT_EXP.1	Anti-Virus Actions
FAV_ALR_EXP.1	Anti-Virus Alerts
FAV_SCN_EXP.1	Anti-Virus Scanning
FCS_COP1	Cryptographic Operation
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
FPT_SEP_EXP.1	Partial TSF Domain Separation

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1-NIAP-0347 Audit Data Generation

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

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

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

c) The events identified in Table 12.

Auditable events and details with applicable SFRs are listed in the following table:

Table 12 - Auditable Events and Details

SFR	Event	Details
FAU_GEN.1-NIAP-0347	None	Not applicable
FAU_GEN.2-NIAP-0410	None	Not applicable
FAU_SAR.1	None	Not applicable
FAU_SAR.2	None	Not applicable
FAU_STG.1-NIAP-0429	None	Not applicable
FAU_STG.NIAP-0414-NIAP-0429	Selection of an action	Action selected
FAV_ACT_EXP.1	Action taken in response to detection of a virus	Virus detected, action taken, file or process identified where virus is 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_SMF.1	None	Not applicable
FMT_SMR.1	None	Not applicable
FPT_SEP_EXP.1	None	Not applicable

Application Note: FAU_SAR.3 has been levied on the IT Environment rather than the TOE in conformance to the PP errata sheet. Therefore FAU_SAR.3 was removed from the table above.

FAU_GEN.1.2-NIAP-0347 The TSF shall be able to generate an audit record of the following auditable events:

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

b) For each audit event type, based on the auditable event definitions of the functional components, *the additional information identified in Table 12.*

5.1.1.2 FAU_GEN.2-NIAP-0410 User Identity Association

FAU_GEN.2.1-NIAP-0410 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) **Refinement:** 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.1.1(2) **Refinement:** 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(1) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

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.

5.1.1.5 FAU_STG.1-NIAP-0429 Protected Audit Trail Storage

FAU_STG.1.1-NIAP-0429 **Refinement:** The TSF shall protect the stored audit records in the audit trail from unauthorised deletion **via the TSFI.**

FAU_STG.1.2-NIAP-0429 **Refinement:** The TSF shall be able to *prevent* unauthorised modifications to the audit records in the audit trail **via the TSFI.**

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

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

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

FAU_STG.NIAP-0414-1-NIAP-0429(1) **Refinement:** 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 **permanent workstation** audit trail is full.

FAU_STG.NIAP-0414-2-NIAP-0429(1) **Refinement:** The TSF shall overwrite the oldest stored audit records if the **permanent workstation** audit trail is full and no other action has been selected.

FAU_STG.NIAP-0414-1-NIAP-0429(2) **Refinement:** The TSF shall provide the administrator the capability to select one or more of the following actions ignore auditable events and *no other actions* to be taken if the **transient workstation or central management system** audit trail is full.

FAU_STG.NIAP-0414-2-NIAP-0429(2) **Refinement:** The TSF shall ignore auditable events if the **transient workstation or central management system** audit trail is full and no other action has been selected.

Application Note: The single instance of this SFR from the PP has been iterated and refined. Audit records generated on the workstation are stored locally as well as being forwarded to the central management system. The first iteration applies to the audit file that is permanently maintained on the workstation for review by the local workstation

user. The second iteration applies to audit records being forwarded from the workstations to the central management system and to the database on the central management system in which the audit records are stored.

5.1.2 Anti-Virus (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) No other actions.

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 *comparing a request for network port access to the antivirus rules* and simultaneously permit traffic from authorized process defined by *taking no additional actions*.

5.1.2.2 FAV_ALR_EXP.1 Anti-Virus Alerts

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

FAV_ALR_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 Anti-Virus 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 **Refinement:** The TSF shall perform calculate a message digest to verify the integrity of the signature files in accordance with a specified cryptographic algorithm *Secure Hash Algorithm (SHA-1)* and cryptographic key sizes (not applicable) that meet the following: *FIPS 180-2 (CAVP certificate #431).*

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1(1) The TSF shall restrict the ability to *determine the behaviour 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 behaviour 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 notification 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.

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_SEP_EXP.1 Partial TSF Domain Separation

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_SEP by themselves. This explicitly stated SFR states the portion of FPT_SEP that can be addressed by the TOE. See FPT_SEP (levied on the IT Environment) for the remaining functionality.

FPT_SEP_EXP.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 Requirements for the Environment

This security target provides functional requirements for the Environment. These requirements consist of functional components derived from Part 2 of the CC, CC interpretations, and NIAP interpretations summarized in the following table:

Table 13 - Security Requirements for the Environment

Component	Name
FAU_STG.1-NIAP-0429	Protected Audit Trail Storage

Component	Name
FAU_SAR.3	Selectable Audit Review
FDP_RIP.1	Subset Residual Information Protection
FIA_AFL.1	Authentication Failure Handling
FIA_SOS.1	Verification of Secrets
FIA_UAU.2	User Authentication Before Any Action
FIA_UAU.6	Re-Authenticating
FIA_UID.2	User Identification Before Any Action
FPT_ITT.1	Basic Internal TSF Data Transfer Protection
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps
FTA_SSL.1	TSF-Initiated Session Locking
FTA_TAB.1	Default TOE Access Banners

5.2.1 Security Audit

5.2.1.1 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 **Refinement:** The **IT Environment** shall provide the ability to perform *searches and sorting* of audit data based on

b) Date and time of the event,

c) Type of event, and

d) Subject identity.

Application Note: This functionality is accessed via the TOE GUIs, but the actual searching and sorting is performed by the DBMS. Therefore, in conformance to the PP errata sheet, this SFR is levied on the IT Environment rather than the TOE.

5.2.1.2 FAU_STG.1.1-NIAP-0429 Protected Audit Trail Storage

FAU_STG.1.1-NIAP-0429 **Refinement:** The **IT Environment** shall protect the stored audit records in the audit trail **file(s)** from unauthorised deletion.

FAU_STG.1.2-NIAP-0429 **Refinement:** The **IT Environment** shall be able to *prevent* unauthorised modifications to the audit records in the audit trail **file(s).**

Application Note: This instance of FAU_STG.1-NIAP-0429 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

5.2.2.1 FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 **Refinement:** 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

5.2.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 **Refinement:** The **IT Environment** shall detect when "*an administrator configurable positive integer within range 1 to 5*" unsuccessful authentication attempts occur related to the unsuccessful authentication attempts since the last successful authentication of the Central Administrator or Workstation User.

FIA_AFL.1.2 **Refinement:** When the defined number of unsuccessful authentication attempts has been met or surpassed, the **IT Environment** shall *prevent authentication and log the failed attempts*.

5.2.3.2 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 **Refinement:** The **IT Environment** shall provide a mechanism to verify that secrets meet *a minimum of 8 characters including at least one numeric character*.

5.2.3.3 FIA_UAU.2 User Authentication Before any Action

FIA_UAU.2.1 **Refinement:** 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.

5.2.3.4 FIA_UAU.6 Re-Authenticating

FIA_UAU.6.1 **Refinement:** 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 **Refinement:** The **IT Environment** shall require each **Central Administrator or Workstation User** to identify itself before any other TSF-mediated actions on behalf of that user.

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

5.2.4 Protection of the TSF

5.2.4.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FTP_ITT.1.1 **Refinement:** 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

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

5.2.4.3 FPT_SEP.1 Domain Separation

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

FPT_SEP.1.2 **Refinement:** 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

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

5.2.5 Session Locking

5.2.5.1 FTA_SSL.1 TSF-Initiated Session Locking

FTA_SSL.1.1 **Refinement:** The **IT Environment** shall lock an interactive session **of the Central Administrator or Workstation User** after *1 to five 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 **Refinement:** The **IT Environment** shall require the following events to occur prior to unlocking the **Central Administrator or Workstation User** session: re-authentication.

5.2.6 TOE Access Banners

5.2.6.1 FTA_TAB.1 Default TOE Access Banners

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

5.3 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2 augmented with ALC_FLR.2. These requirements are summarised in the following table:

Table 14 - Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.2	Configuration Items
Delivery and Operation	ADO_DEL.1	Delivery Procedures
	ADO_IGS.1	Installation, Generation, and Start-Up Procedures

Assurance Class	Component ID	Component Title
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
Life Cycle 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

5.4 Strength of Function for the TOE

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.

5.5 CC Component Hierarchies and Dependencies

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

Table 15 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1-NIAP-0347	None	FPT_STM.1	Satisfied by the IT Env.
FAU_GEN.2-NIAP-0410	None	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied by the IT Env.
FAU_SAR.1	None	FAU_GEN.1	Satisfied
FAU_SAR.2	None	FAU_SAR.1	Satisfied

FAU_SAR.3	None	FAU_SAR.1	Satisfied
FAU_STG.1-NIAP-0429	None	FAU_GEN.1	Satisfied
FAU_STG.2-NIAP-0429	FAU_STG.1	FAU_GEN.1	Satisfied
FAU_STG.NIAP-0414-NIAP-0429	FAU_STG.4	FAU_STG.1, FMT_MTD.1	Satisfied Satisfied
FCS_COP.1	None	[FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	See Table 10 for rationale
FMT_MOF.1	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	None	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	None	None	None
FMT_SMR.1	None	FIA_UID.1	Satisfied by the IT Env.
FPT_SEP_EXP.1	None	None	None

Table 16 - Unsupported Dependency Rationale

Requirement	Dependency	Dependency Analysis and Rationale
FCS_COP.1	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	The only cryptographic function is a message digest that does not use keys.

CHAPTER 6

6. TOE Summary Specification

6.1 Security Functions

6.1.1 Audit

6.1.1.1 Audit Review

Audit review components exist in both VSE and ePO. GUI interfaces are provided on both platforms to enable audit information to be reviewed in a user-friendly form.

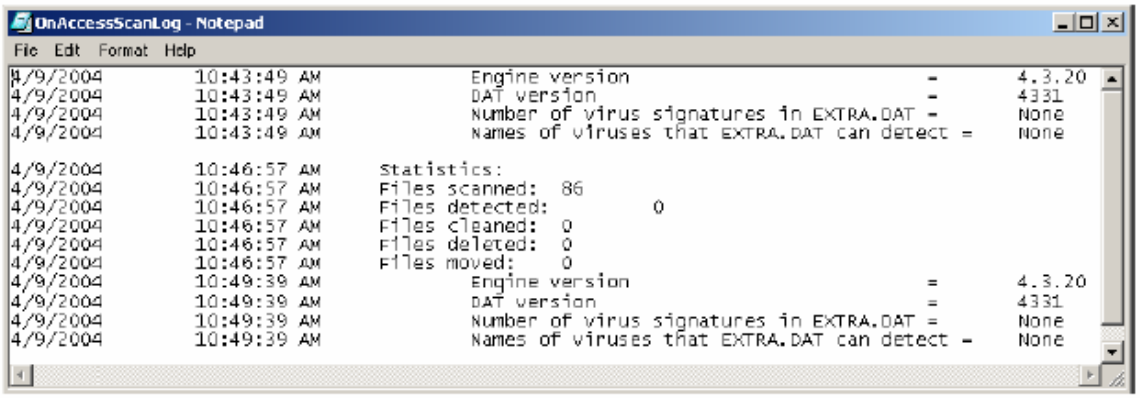
Using the ePO Reporting feature, Central Administrators can review all events that occur on the managed systems in the environment being monitored, including the ePO server itself. All users except Central Administrators are prohibited from obtaining read-access of audit records.

It is possible to customize filters to search the audit records. The way to filter events is to use the Filtering tab that is part of the Reporting feature. Once the Central Administrator is using the Reporting feature, the events that can be filtered are configurable by selecting Events. Searching may be performed on the type of event, the date and time of the event, and the subject identity (userid or workstation identifier). The searching functionality is accessed via these GUIs, but the TOE relies upon the DBMS (in the IT Environment) to perform the search.

Sorting may be performed by using the Custom Query feature of ePO. Sorting may be performed on the type of event, the date and time of the event, and the subject identity (userid or workstation identifier). The sorting functionality is accessed via these GUIs, but the TOE relies upon the DBMS (in the IT Environment) to perform the sort.

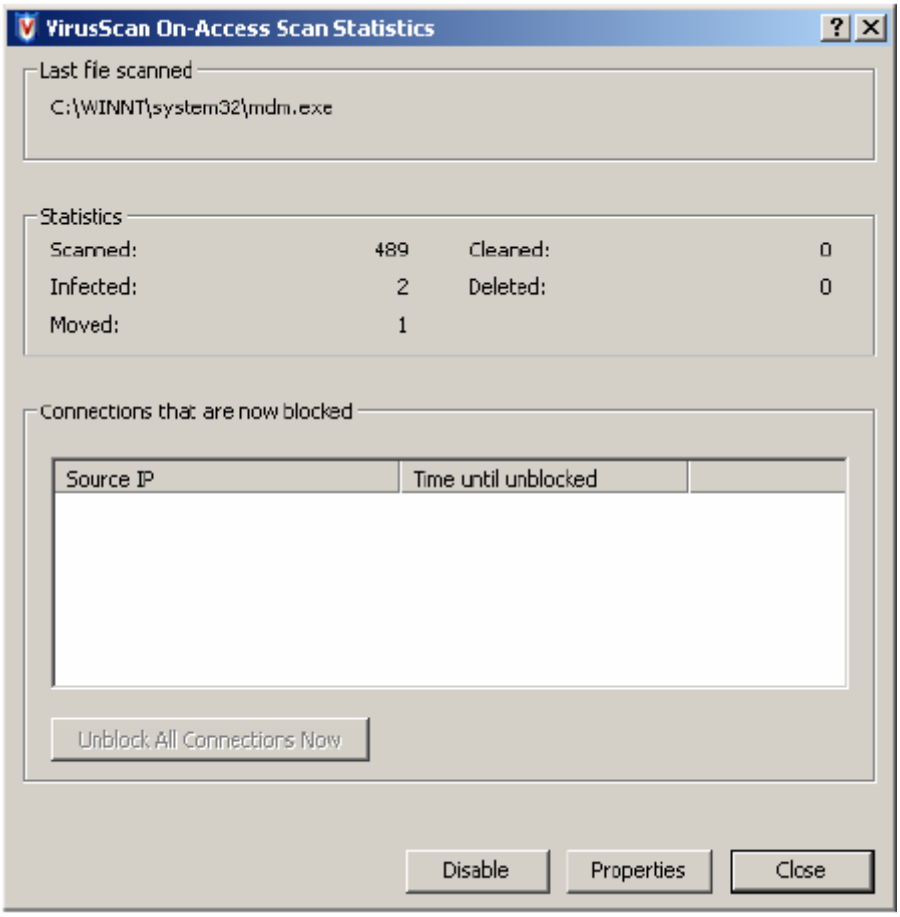
The TOE includes a VirusScan Console that generates an activity log for the virus scanning operations. The activity log is known in the GUI as the OnAccess Scan Log. The OnAccess Scan Log shows the engine and signature file version numbers (a.k.a. version number of DAT files) that were in effect when the scanning took place. The OnAccess Scan Log also shows the number of viruses found, and the actions the scanner took (e.g. cleaned, deleted, moved) in response to the viruses. A screenshot of the OnAccess Scan Log is found in the following figure.

Figure 3 - On Access Scan Log Screenshot



Using the On-Access Scan Statistics on the user workstation, the Workstation User or Central Administrator can find out a variety of information about the files that have been scanned including the number of viruses that were found, and the actions that it took in response to the viruses. A screenshot of the On-Access Scan Statistics is found in the following figure.

Figure 4 - On Access Scan Statistics Screenshot



On the workstation, the VirusScan Console user may delete any or all of the audit records maintained on the workstation. No mechanism is provided to modify audit records. No access to the audit records is provided to unauthorized users.

6.1.1.2 Audit Generation

The TOE generates an activity log for the virus scanning operations. VSE generates audits when viruses are detected. The audit event record includes details of the system on which the virus was detected (subject identity), the specific virus detected, the action taken to counteract the virus, and the file or process in which the virus was detected. The default filename for the OnAccess Scan Log (audit information retained on the workstation) is called ONACCESSSCANLOG.TXT. If storage limits for the audit log file are exceeded, VSE automatically discards the oldest events sufficient to free 20% of the configured file size and continues to record the most recent events. The default file

size is 1 MB, but the administrator is directed to set the file size to a minimum of 10 MB. Therefore, the TOE will retain at least the most recent 8 MB worth of audit records when the oldest events are discarded.

Copies of all audits from the network-attached workstations are sent to a central management system, where they can be reviewed by the Central Administrator. The audit records are queued on the workstations for transmission to the management system. In the unlikely event that the queue space is exhausted, new events are discarded and the oldest events are retained.

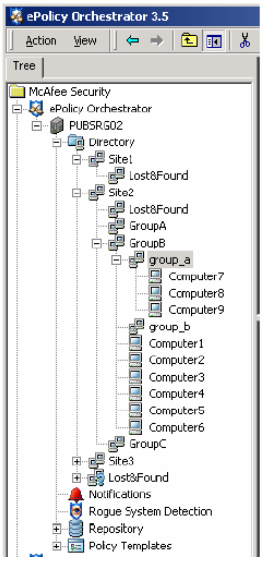
Once events are transferred to a central management system and accepted, they are deleted from the queue on the workstations. Events are temporarily stored on the central management system in an event folder, then processed and inserted into the audit database file. In the unlikely event that the folder space is exhausted, events from the workstations are not accepted (and remain queued on the workstations). In the unlikely event that the database space is exhausted, new events are discarded and the oldest events are retained.

The TOE operates whenever the system is running. If the VSE is enabled or disabled by the Central Administrator, an audit event record is generated.

6.1.2 Management

Most of the Management security functions are provided by ePO. The update function can be automated and allows the user to update the signature files. Signature files are expected to be updated frequently.

Figure 5 - Management Hierarchy for Administrators and Groups



ePO also provides the ability to allow organizations to manage anti-virus security polices through a single point of control and allows the Central Administrator to both enable and disable scanning and scheduling of tasks. Enabling and disabling of scanning and scheduling of tasks can either be performed on a workstation-by-workstation basis, a group basis, a site basis, or on a domain basis.

The Central Administrator enables and disables various security functions by configuring security policies. A policy is a collection of software settings that you create, configure, and enforce on managed systems. Policies ensure that the TOE is configured on a managed network the way you want it to be configured. The policies control scheduling, the depth of file scans, and what files are scanned. Depth of scan refers to whether or not compressed files are scanned for infection. If compressed files are scanned, the scan is said to penetrate the files to a deeper degree.

Using the VSE Console, the Central Administrator or Workstation User may configure the depth of file scans and specify the files to be scanned on a specific workstation. The Central Administrator may also enable and disable operation of the virus scanning function; under normal conditions, this function should always be enabled.

The frequency of the scans on the individual workstation is determined by the Central Administrator using policy enforcement configuration. Policy settings are updated to distributed management systems according to the enforcement interval settings. The policy enforcement interval is determined by the Agent-to-server-communication interval setting on the General tab of the ePO Agent 3.6.1 | Configuration policy pages or the Agent Wakeup tasks schedule. By default, the scheduled wakeup configuration is set to occur every 60 minutes.

ePO permits the Central Administrator to configure the actions to be taken when a virus is detected. Both Primary and Secondary actions may be configured. The primary actions that the TOE may take are:

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

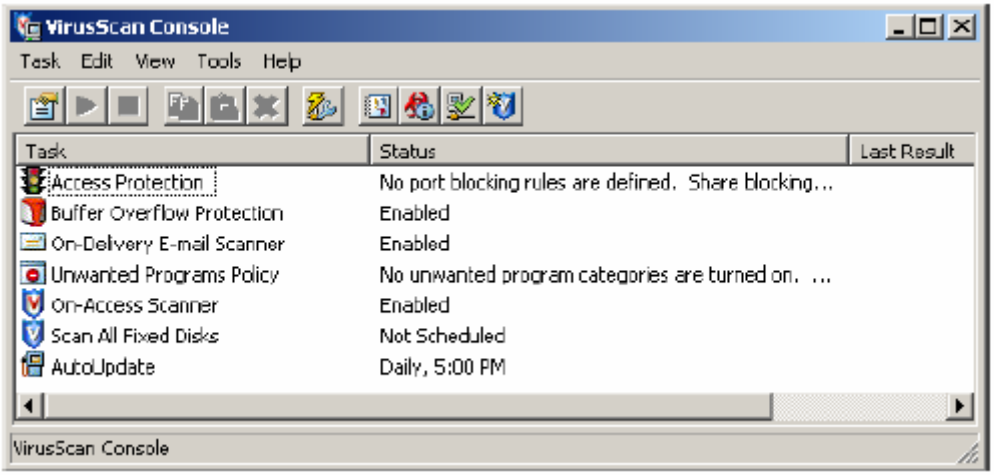
Secondary actions are actions that the TOE may take if the Primary action fails. Secondary actions include:

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

ePO provides the ability to block access to remote network ports from processes on workstations.. The TOE is configured to intercept outgoing network traffic and restrict the source of outgoing SMTP traffic from the workstation to authorized processes (specified by the Central Administrator).

Tasks are enabled or disabled from ePO or the Task Menu of the VirusScan Console. A screenshot of the VSE Console is depicted in the following figure.

Figure 6 - VirusScan Console



6.1.3 Virus Scanning & Alerts

The TOE provides real-time virus detection based on the settings that have been previously configured. The settings can be configured for all processes, or based on whether a process is classified as having a low-risk or high-risk of infection. Scanning occurs when files are either read from, or written to the computer the TOE client agent is installed on. Identification of a virus, worm, or Trojan is referred to as an "infection."

When an infection occurs, the TOE takes certain actions depending on what has been previously configured. There are Primary and Secondary actions that the TOE takes when an infection occurs. The primary actions that the TOE takes when an infection occurs:

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

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

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

When a virus is detected (e.g. an infection occurs) the On-Access Scan Messages box pops up and is displayed and remains on the screen until the user session ends, or until the alert is acknowledged. Using ePO, an alert indicating a virus can be configured to display on the screen of the Central Administrator's console if a session is active. The alert identifies the system where the infection has occurred, the name of the virus, and the action taken by the TOE.

The Virus Scanning & Alert function provides the following capabilities:

- Email Scanning - This function provides scanning of messages in order to identify viruses, worms, and Trojans for the purpose of removing them and reporting on them.
- Archive Scanning - The TOE can scan inside archives such as .zip files and MIME encoded files.
- Memory protection - The TOE provides in-memory process scanning and by doing so, stops viruses, worms, Trojans and their associated files from executing in memory. When a memory-based virus is detected, the process is stopped. Only a single pass of the On-Access scanner is required to remove all instances of a virus from memory.
- The TOE prevents unauthorized processes from sending email (via SMTP port 25) from the end-user's workstation..
- Anti-virus Scanning – By default, VSE examines executables and self-decompressing files by decompressing each file in memory and checking for virus signatures. These scan examinations occur in real-time, and alternatively can be scheduled by the Central Administrator, or performed on an ad-hoc manual basis by the workstation user. When manually invoked, the workstation user may control execution of the scan by specifying the files to be included.

6.1.4 Cryptographic Operations

ePO has the ability to create and deploy VirusScan anti-virus packages. The signature provided with the package includes calculation of a message digest using the Secure Hash Algorithm (SHA-1).

6.1.5 Protection of the TOE

The TOE provides for separation between users under the TSC. On ePO, multiple users of the management GUI may be active simultaneously. Each one is instantiated as a separate OS process and attributes of those processes are individually tracked within the TOE. VSE has components that operate in user memory space and system memory space. Memory space is allocated specifically for each process, which makes it impossible for one user to directly access the memory space of another user. Multiple users may invoke the GUI simultaneously (if supported by the OS). These instances operate as separate OS processes and the attributes are individually tracked within the TOE.

6.2 Assurance Measures

Table 17 - Assurance Documents

Assurance Class	Component ID	Document satisfying Assurance Component
Configuration Management	ACM_CAP.2	The following Configuration Management procedures are described in this documentation: • Use of the CM tool for revision control • Use of documented procedures for product builds • Use of documented procedures for product test • Use of documented procedures for release to

Assurance Class	Component ID	Document satisfying Assurance Component
		manufacturing • Use of documented procedures for distribution to customers • List of configuration items and evidence that they are maintained by the CM tool
Delivery and Operation	ADO_DEL.1	This document includes descriptions of the process used to create distribution copies of the TOE and the procedures used to ensure consistent delivery of the TOE.
	ADO_IGS.1	These documents describe the procedures necessary for secure installation, generation, and start-up of the TOE.
Development	ADV_FSP.1	These documents provide the purpose and method of use of all external TSF interfaces and completely represent the TSF.
	ADV_HLD.1	These documents describe the high-level design and the security functionality provided by each subsystem of the TSF. These documents also identify the interfaces, and the interfaces to the subsystems.
	ADV_RCR.1	The correspondence between the TOE security functions and the high-level design subsystems is described in these documents.
Guidance Documents	AGD_ADM.1	Guidance to administrators is effectively supported by the listed documentation for this requirement.
	AGD_USR.1	Guidance to non-administrative users is effectively supported by the listed documentation for this requirement.
Life Cycle Support	ALC_FLR.2	These documents describe flaw remediation guidance and enables users to submit reports back to the developers
Tests	ATE_COV.1	These documents map tests to the functional specification, and to the testing data.
	ATE_FUN.1	These documents describe the functional tests performed including their results.
	ATE_IND.2	These documents describe the functional tests performed and their results

Assurance Class	Component ID	Document satisfying Assurance Component
Vulnerability Assessment	AVA_MSU.1	The user and admin guidance documents describe the functions expected to be performed by the users of the TOE in a manner that is clear such that they will not misuse the TOE.
	AVA_SOF.1	These documents include a strength of function analysis to support the SOF-basic claim. The analysis includes identifying the TOE password space and probability of a password being compressed.
	AVA_VLA.1	These documents describe the vulnerability analysis performed and the results of the analysis.

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This security target claims conformance with the *U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness, Version 1.1*, April 4, 2006.

7.2 Protection Profile Refinements

In conformance to the errata sheet of the PP, FAU_SAR.3 has been levied on the IT Environment. No other refinements have been made to the SFRs.

7.3 Protection Profile Additions

In conformance to the errata sheet of the PP, OE.AUDIT_SEARCH has been added to the security objectives of the IT Environment. No other additions to the objectives or security requirements have been made. All objectives and security requirements are consistent with the PP.

7.4 Protection Profile Rationale

The TOE complies with *U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness, v1.1*, April 4, 2006. All of the security requirements defined in the *U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness, v1.1*, April 4, 2006 have been reproduced in the Security Target. In conformance to the errata sheet of the PP, FAU_SAR.3 has been levied on the IT Environment.

This Security Target includes all of the assumptions and threats and statements described in the PP, verbatim. This Security Target also includes all of the Security Objectives from the PP, verbatim. In conformance to the errata sheet of the PP, OE.AUDIT_SEARCH has been added to the security objectives of the IT Environment and mapped to T.UNIDENTIFIED_ACTIONS.

All applicable operations left uncompleted in the *U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness, v1.1*, April 4, 2006 have been completed in the Security Target in accordance with the bounds set forth by the *U.S. Government Protection Profile Anti-Virus Applications for Workstations in Basic Robustness, v1.1*, April 4, 2006. This Security Target has introduced no additional security objectives or security requirements.

CHAPTER 8

8. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

8.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat, assumption, and organisational security policy is addressed by a security objective. The following table identifies for each threat and assumption, the security objective(s) that address it:

Table 18 - Threats and Policies Mapped to Security Objectives for the TOE

	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						X															
O.ADMIN_ROLE																					X
O.AUDIT_GENERATION															X			X			
O.AUDIT_PROTECT							X														
O.AUDIT_REVIEW															X						
O.CONFIGURATION_IDENTIFICATION									X	X											
O.CORRECT_TSF_OPERATION											X		X								
O.CRYPTOGRAPHY																			X		
O.DOCUMENTED_DESIGN									X		X										
O.MANAGE													X							X	
O.PARTIAL_FUNCTIONAL_TEST										X	X										
O.PARTIAL_SELF_PROTECTION							X						X								
O.VIRUS																X				X	
O.VULNERABILITY_ANALYSIS									X	X	X										
OE.AUDIT_BACKUP	X																				
OE.AUDIT_SEARCH															X						

	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
OE.AUDIT_STORAGE							X														
OE.DISPLAY_BANNER																	X				
OE.DOMAIN_SEPARATION							X						X								
OE.NO_BYPASS							X						X								
OE.NO_EVIL		X																			
OE.PHYSICAL			X																		
OE.RESIDUAL_INFORMATION							X					X	X								
OE.SECURE_COMMS				X																	
OE.SECURE_UPDATES					X																
OE.TIME_STAMPS															X			X			
OE.TOE_ACCESS								X						X				X			
OE.TRUST_IT																					

8.1.1 Rationale Showing Threats, Assumptions, and Organisational Security Policies to Security Objectives

The following table describes the rationale for the threats, assumptions, and organisational security policies to security objectives mapping:

Table 19 - Threats, Policies, Assumptions Mapped to Security Obj. 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	O.AUDIT_PROTECT: The TOE will provide the capability to protect audit	O.AUDIT_PROTECT contributes to mitigating this threat by controlling access to the individual audit log records. No one is

Threat / Policy / Assumption	Addressed By	Rationale
lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	information. OE.AUDIT_STORAGE: The IT environment will contain mechanisms to provide secure storage and management of the audit log. OE.RESIDUAL_ INFORMATION: The TOE will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. O.PARTIAL_SELF_PROTECTION: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces. OE.DOMAIN_SEPARATION: The IT environment will provide an isolated domain for the execution of the TOE. OE.NO_BYPASS: The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	allowed to modify audit records, the System Administrator is the only one allowed to delete audit records, and the TOE has the capability to prevent auditable actions from occurring if the audit trail is full. OE.AUDIT_STORAGE contributes to mitigating this threat by restricting the ability of users in the IT Environment to access the audit log file. OE.RESIDUAL_INFORMATION prevents a user not authorized to read the audit trail from access to audit information that might otherwise be persistent in a resource used by the TOE (e.g., memory). By preventing residual information in a resource, audit information will not become available to any user or process except those explicitly authorized for that data. O.PARTIAL_SELF_PROTECTION contributes to countering this threat by ensuring that the TSF can protect itself from users via its own interfaces. This limits access to the audit information to the functions defined for the specified roles. OE.DOMAIN_SEPARATION contributes to countering this threat by ensuring that the TSF is protected from users through mechanisms other than its own interfaces. If the OS could not maintain and control a domain of execution for the TSF separate from other processes, the TSF could not be trusted to control access to the resources under its control, which includes the audit trail which are always invoked is also critical to the migration of this threat. OE.NO_BYPASS ensures audit compromise can not occur simply by bypassing the TSF.
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.

Threat / Policy / Assumption	Addressed By	Rationale
T.POOR_DESIGN: Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.	O.CONFIGURATION_IDENTIFICATION: The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified. O.DOCUMENTED_DESIGN: The design of the TOE is adequately and accurately documented. O.VULNERABILITY_ANALYSIS: The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.CONFIGURATION_IDENTIFICATION plays a role in countering this threat by requiring the developer to provide control of the changes made to the TOE's design. O.DOCUMENTED_DESIGN ensures that the design of the TOE is documented, permitting detailed review by evaluators. O.VULNERABILITY_ANALYSIS_TEST ensures that the design of the TOE is analyzed for design flaws.
T.POOR_IMPLEMENTATION: Unintentional errors in 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	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.

Threat / Policy / Assumption	Addressed By	Rationale
	testing that demonstrates the TSF satisfies the security functional requirements. O.CORRECT_TSF_OPERATION: The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site. O.VULNERABILITY_ANALYSIS: The TOE will undergo some vulnerability analysis demonstrate the design and implementation of the TOE does not contain any obvious flaws.	O.PARTIAL_FUNCTIONAL_TESTING increases the likelihood that any errors that do exist in the implementation will be discovered through testing. O.CORRECT_TSF_OPERATION provides assurance that the TSF continues to operate as expected in the field. O.VULNERABILITY_ANALYSIS_TEST addresses this concern by requiring a vulnerability analysis be 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	OE.RESIDUAL_INFORMATION is necessary to mitigate this threat, because even if the security mechanisms do not allow a user to explicitly view TSF data, if TSF data were to inappropriately reside in a resource that was made available to a user, that user would be able to inappropriately view the TSF data. O.PARTIAL_SELF_PROTECTION is necessary so that the TSF protects itself and its resources from inappropriate access through its own interfaces. OE.DOMAIN_SEPARATION is necessary so that the TSF is protected from other processes executing on the workstation. O.MANAGE is necessary because an access control policy is not specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions. O.CORRECT_TSF_OPERATION provides assurance that the TSF continues to operate

Threat / Policy / Assumption	Addressed By	Rationale
	domain for the execution of the TOE. O.MANAGE: The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE. O.CORRECT_TSF_OPERATION: The TOE will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site. OE.NO_BYPASS: The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	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. OE.AUDIT_SEARCH: The IT Environment will provide the capability to search and sort the 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.). OE.AUDIT_SEARCH assists the Administrator in reviewing the audit logs by making it easier to focus on particular events of interest. 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 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.

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

Threat / Policy / Assumption	Addressed By	Rationale
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.	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.	OE.SECURE_COMMS: The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.	OE.SECURE_COMMS restates the assumption. The workstation OS will provide a secure line of communication for the TOE.
A.SECURE_UPDATES: Administrators will implement secure mechanisms for receiving and validating updated signature files from the Anti-Virus vendors, and for distributing the updates to the central management systems.	OE.SECURE_UPDATES: Enterprises using the TOE shall ensure that signature file updates are received from the vendor via secure mechanisms, the updates are validated before being used, and the updates are distributed to central management systems within the Enterprise via secure mechanisms.	OE.SECURE_UPDATES restates the assumption. Administrators use secure mechanisms to receive and validate the updates from the vendor, then use secure mechanisms to distribute the updates to the central management systems.

8.2 Security Requirements Rationale

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives. The following table identifies for each TOE security objective, the SFR(s) that address it:

Table 20 - Mapping of TOE Objectives to TOE SFRs and SARs

	O.ADMIN_GUIDANCE	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.CONFIGURATION_IDENTIFICATION	O.CORRECT_TSF_OPERATION	O.CRYPTOGRAPHY	O.DOCUMENTED_DESIGN	O.MANAGE	O.PARTIAL_FUNCTIONAL_TEST	O.PARTIAL_SELF_PROTECTION	O.VIRUS	O.VULNERABILITY_ANALYSIS
ACM_CAP.2						X								
ADO_DEL.1	X													
ADO_IGS.1	X													
ADV_FSP.1									X					
ADV_HLD.1									X					
ADV_RCR.1									X					
AGD_ADM.1	X													
AGD.USR.1	X													
ALC_FLR.2						X								
ATE_COV.1											X			
ATE_FUN.1											X			
ATE_IND.2											X			
AVA_MSU.1	X													
AVA_VLA.1														X
FAU_GEN.1-NIAP-0347			X				X							
FAU_GEN.2-NIAP-0410			X				X							
FAU_SAR.1					X		X							
FAU_SAR.2				X										
FAU_STG.1-NIAP-0429				X										
FAU_STG.NIAP-0414-NIAP-0429				X										
FAV_ACT_EXP.1							X						X	
FAV_ALR_EXP.1							X						X	
FAV_SCN_EXP.1							X						X	
FCS_COP.1								X						
FMT_MOF.1		X								X				
FMT_MTD.1		X								X				
FMT_SMF.1		X								X				
FMT_SMR.1		X								X				
FPT_SEP_EXP.1												X		

The following table provides the details of TOE security objective(s):

Table 21 - Rationale for Security Objectives (SFRs and SARs)

Security Objective	Requirements that Address the Objective	SFR and Rationale
O.ADMIN_GUIDANCE The TOE will provide the 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, without tampering or corruption during delivery. This requirement ensures the administrator has the ability to begin their TOE installation with a clean (e.g. malicious code has not been inserted once it has left the developer's control) version of the TOE, which is necessary for secure management of the TOE. 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 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 mechanism would not have to be repeated in the administrator's guide. AVA_MSU.1 ensures 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 isolated administrative actions.	FMT_MOF.1 FMT_MTD.1 FMT_SMR.1	FMT_SMR.1 requires that the TOE establish a Central Administrator role. FMT_MOF.1 and FMT_MTD.1 specify the privileges that only the Central Administrator may perform.
O.AUDIT_GEN The TOE will provide the capability to	FAU_GEN.1-NIAP-0347 FAU_GEN.2-NIAP-	FAU_GEN.1-NIAP-0347 defines the set of events that the TOE must be capable of recording. This requirement ensures that the Administrator has the ability to audit any security relevant event that takes place in the TOE. This

Security Objective	Requirements that Address the Objective	SFR and Rationale
detect and create records of security relevant events.	0410	requirement also defines the information that must be contained in the audit record for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements. FAU_GEN.2-NIAP-0410 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the userid. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated.
O.AUDIT_PROTECTION The TOE will provide the capability to protect audit information.	FAU_SAR.1 FAU_STG.1-NIAP-0429 FAU_STG.NIAP-0414-1-NIAP-0429	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-NIAP-0429 restricts the ability to delete audit records to the Security Administrator. FAU_STG.NIAP-0414-0429 defines the actions that must be available to the administrator, as well as the action to be taken if there is no 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.1 provides the ability to review the audits in a user-friendly manner.
O.CONFIGURATION_IDENTIFICATION The configuration of the TOE is fully identified in a manner that will allow implementation errors to be identified.	ACM_CAP.2 ALC_FLR.2	ACM_CAP.2 addresses this objective by requiring that there be a unique reference for the TOE, and that the TOE is labeled with that reference. It also requires that there be a CM system in place, and that the configuration items that comprise the TOE be uniquely identified. This provides a clear identification of the composition of the TOE. ALC_FLR.2 addresses this objective by requiring that there be a mechanism in place for identifying flaws subsequent to fielding, and for distributing those flaws to entities operating the system.
O.CORRECT_TSF_OPERATION The TOE will provide the capability to test	FAU_GEN.1-NIAP-0347 FAU_GEN.2-NIAP-0410 FAU_SAR.1 FAV_SCN_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. FAU_SAR.1 enables the

Security Objective	Requirements that Address the Objective	SFR and Rationale
the TSF to ensure the correct operation of the TSF at a customer's site.	FAV_ALR_EXP.1 FAV_ACT_EXP.1	administrator to review the audit events.
O.CRYPTOGRAPHY The TOE shall use NIST FIPS 140-2 validated cryptographic services.	FCS_COP.1	FCS_COP.1 requires that the message digest used to verify integrity of the signature file utilizes a FIPS 140-2 Approved cryptographic algorithm.
O.DOCUMENTED_DESIGN The design of the TOE is adequately and accurately documented.	ADV_FSP.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 the users. FMT_MTD.1 defines particular TOE data that may only be altered by these users. FMT_SMF.1 and FMT_SMR.1 define the administrative functions and roles provided by the TOE.
O.PARTIAL_FUNCTIONAL_TEST The TOE will undergo some security functional testing that demonstrates the TSF satisfies some of its security functional requirements.	ATE_COV.1 ATE_FUN.1 ATE_IND.2	ATE_FUN.1 requires that developer provide test documentation for the TOE, including test plans, test procedure descriptions, expected test results, and actual test results. These needs to identify the functions tested, the tests performed, and test scenarios. They require that the developer run those tests, and show that the expected results were achieved. ATE_COV.1 requires that there be a correspondence between the tests in the test documentation and the TSF as described in the functional specification. 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	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 specific version was used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the environment.

Security Objective	Requirements that Address the Objective	SFR and Rationale
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.	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 are detected. FAV_ALR_EXP.1 defines alerting requirements to ensure the users aware that a virus was detected.
O.VULNERABILITY_ANALYSIS The TOE will undergo some vulnerability analysis to demonstrate the design and implementation of the TOE does not contain any obvious flaws.	AVA_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 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.

8.2.2 Rationale for Security Functional Requirements of the Environment Objectives

This section provides rationale for the Security Functional Requirements for the environment, demonstrating that the SFRs are suitable to address the environment security objectives. The following table identifies for each SFR, and the environment security objective(s) that address it:

Table 22 - Environment Security Objectives Mapped to SFRs

Security Requirements for the Environment	OE.AUDIT_SEARCH	OE.AUDIT_STORAGE	OE.DISPLAY_BANNER	OE.DOMAIN_SEPARATION	OE.NO_BYPASS	OE.RESIDUAL_INFORMATION	OE.SECURE_COMMS	OE.TIME_STAMP	OE.TOE_ACCESS
FAU_SAR.3	X								
FAU_STG.1-NIAP-0429		X							
FDP_RIP.1						X			
FIA_AFL.1									X
FIA_SOS.1									X
FIA_UAU.2									X
FIA_UAU.6									X
FIA_UID.2									X
FPT_ITT.1							X		
FPT_RVM.1					X				
FPT_SEP.1				X					
FPT_STM.1								X	
FTA_SSL.1									X
FTA_TAB.1			X						

The following table provides the rational for the SFRs of the Environment security objective(s):

Table 23 - Environment Security Objectives and SFR Rationale

Environment Security Objective	SFR and Rationale
OE.AUDIT_SEARCH The IT Environment will provide the capability to search and sort the audit information.	FAU_SAR.3 requires the IT Environment to provide searching and sorting functionality to the Administrator.
OE.AUDIT_STORAGE The IT Environment will provide a means for secure storage of the TOE audit log files.	FAU_STG.1-NIAP-0429 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 meets this objective by requiring the system to display a banner before a use can establish an authenticated session.
OE.DOMAIN_SEPARATION The Environment will provide an isolated domain for the execution of the TOE.	FPT_SEP.1 requires the OS to provide an isolated domain for the TOE.
OE.NO_BYPASS The Environment shall ensure the TOE security mechanism cannot be bypassed in order to gain access to the TOE resources.	FTP_RVM.1 requires the OS to ensure that the TOE will not be bypassed.
OE.RESIDUAL_INFORMATION The 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.	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.

Environment Security Objective	SFR and Rationale
OE.SECURE_COMMS The Environment will provide a secure line of communications between distributed portions of the TOE.	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 Environment will provide reliable time stamps.	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 provides a detection mechanism for unsuccessful authentication attempts by remote administrators, authenticated proxy users and authorized IT entities. The requirement enables a Central 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, limited 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 authenticated by the TOE in order to access 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 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 then can gain access to the TOE.

8.2.3 Security Assurance Requirements Rationale

8.2.3.1 TOE Security Assurance Requirements Rationale

The TOE meets the assurance requirements for EAL2 augmented with ALC_FLR.2. Table 21 provides a reference between each TOE assurance requirement and the information found in the related vendor documentation that satisfies each requirement.

8.2.3.2 Rationale for TOE Assurance Requirements Selection

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

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented with ALC_FLR.2 from part 3 of the Common Criteria.

8.2.4 Rationale for Explicit Requirements

The following table presents the rationale for the explicit security requirements found in this security target:

Table 24 - Rationale for Explicit Security Requirements

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 User or Central Administrators that it not accounted for in CC SFRs.
FAV_SCN_EXP.1	This component defines the scanning mechanism to be performed by the TOE to detect viruses. Existing security policy SFRs (e.g., FDP_ACT 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.
FPT_SEP_EXP.1	The CC FPT_SEP component can not be satisfied by application TOEs. This component defines the separation that may be performed by applications.

8.3 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs. The following table provides a mapping between the TOE's Security Functions and the SFRs:

Table 25 - SFRs to TOE Security Functions Mapping

	Audit Generation	Audit Review	Management	Virus Scanning & Alerts	Cryptographic Operations	Protection of the TOE
FAU_GEN.1-NIAP-0347	X					

	Audit Generation	Audit Review	Management	Virus Scanning & Alerts	Cryptographic Operations	Protection of the TOE
FAU_GEN.2-NIAP-0410	X					
FAU_SAR.1		X				
FAU_SAR.2		X				
FAU_STG.1-NIAP-0429		X				
FAU_STG.NIAP-0414-NIAP-0429	X					
FAV_ACT_EXP.1				X		
FAV_ALR_EXP.1				X		
FAV_SCN_EXP.1				X		
FCS_COP.1					X	
FMT_MOF.1(1)			X			
FMT_MOF.1(2)				X		
FMT_MTD.1	X		X			
FMT_SMF.1		X	X	X		
FMT_SMR.1			X			
FPT_SEP_EXP.1						X

Table 26 - SFR to SF Rationale

SFR	SF and Rationale
FAU_GEN.1-NIAP-0347	**Audit Generation -** The TOE generates audit event records when TOE components start or stop (enable and disable) and when viruses are detected. The audit records include the date and time, type of event, subject identity, outcome, as well as (for virus detection events) the virus, action taken, and the file or process in which the virus was detected.
FAU_GEN.2-NIAP-0410	**Audit Generation -** The TOE ensures that the audit records associate a user identity with the auditable event. In the case of ePO events, the association is accomplished with the userid. In all other cases, the association is based on the workstation identifier.

SFR	SF and Rationale
FAU_SAR.1	**Audit Review -** On ePO, the Central Administrtaor may use the GUIs to review the audits from all workstations in a user-friendly manner. On the workstations, the VSE Console may be used by the workstation user or Central Administrator to review audits generated on that workstation in a user-friendly manner.
FAU_SAR.2	**Audit Review -** The TOE does not provide any mechanism for unauthorized users to access the audit information. Authorized users are Central Administrators (on ePO) and workstation users that successfully authenticate to the OS.
FAU_STG.1-NIAP-0429	**Audit Review –** No users may modify audit records, and only authorized users may delete records.
FAU_STG.NIAP-0414-NIAP-0429	**Audit Generation -** The TOE always overwrites the oldest stored audit records when space is exhausted while saving audit records to the file maintained on the workstation for local review. For audit records queued for transmission to the central management system and for audit records being inserted into the database on the central management system, new audit records are discarded (ignored) if space is exhausted.
FAV_ACT_EXP.1	**Virus Scanning & Alerts -** VSE scans for memory-based viruses and terminates the process containing a virus when one is detected. VSE scans files for viruses. Configurable actions that may be taken are cleaning the file, quarantining the file, and deleting the file. VSE is configured to prevent unauthorized processes from initiating an outgoing network connection to remote port 25 (SMTP).
FAV_ALR_EXP.1	**Virus Scanning & Alerts -** When a virus is detected, an alert is presented to both the workstation and ePO users. The alert remains displayed until acknowledged by the users.
FAV_SCN_EXP.1	**Virus Scanning & Alerts -** VSE performs real-time scans for memory-based viruses. VSE performs real-time, scheduled, and on-demand scans of files for viruses. Scheduled scans are configured by the Central Administrator. On-demand scans are initiated by the workstation user.
FCS_COP.1	**Cryptographic Operations -** The TOE calculates SHA-1 message digests on DAT file updates to ensure their integrity.
FMT_MOF.1(1)	**Management -** The Central Administrator has the ability via ePO GUIs to configure auditing, real-time virus scanning, and scheduled virus scanning
FMT_MOF.1(2)	**Virus Scanning & Alerts** – The workstation user modifies the behavior of the scan by specifying the files to be scanned.
FMT_MTD.1	**Audit Review, Management -** The Central Administrator has the ability via ePO to query, modify and delete: • Actions to be taken on workstations when a virus is detected, • Files to be scanned automatically on workstations, • Minimum depth of file scans on workstations, • Scheduled scan frequency on workstations, • Processes authorized to transmit data to a remote system using TCP or UDP remote port 25 (SMTP) • Virus scan signatures and • Audit logs on the central management system

SFR	SF and Rationale
	The Central Administrator and workstation users may modify the depth of file scans and files to be scanned, as well as review audit logs, via the VSE console. The Central Administrator and workstation users may also view and delete audit records in the audit log maintained on the workstations.
FMT_SMF.1	**Audit Review, Management, Virus Scanning & Alerts -** The Central Administrator may use ePO or VSE GUIs to: • Enable and disable operation of the TOE on workstations, • Configure operation of the TOE on workstations, • Update virus scan signatures, • Acknowledge alert notification from the central management system, • Review audit logs on the central management system, • Increase the depth of file scans on manually invoked scans, • Acknowledge alert notifications on the workstation being used, and • Review audit logs on the workstation being used
FMT_SMR.1	**Management -** The TOE maintains the Central Administrator role on both ePO and VSE and the workstation user role on VSE. The Network User role is automatically assigned by the TOE for all incoming network traffic.
FPT_SEP_EXP.1	**Protection of the TOE -** The TOE provides separation between multiple users by utilizing separate processes and tracking attributes for each separately.

8.4 PP Claims Rationale

The rationale for the Protection Profile conformance claims is defined in Chapter 7, Section 7.4 Protection Profile Rationale.