CA Inc.

Integrated Threat Management r8.0.445

Security Target V1.8

May 1, 2007

Prepared By:

CYGNACOM
SOLUTIONS

Suite 5200 ♦7925 Jones Branch Drive♦McLean, VA 22102-3321♦703 848-0883♦Fax 703 848-0960

TABLE OF CONTENTS

SECTION **PAGE**

Table of Tables and Figures

Table or Figure **Page**

1 Security Target Introduction

This section presents the following information:

- Identification of the Security Target (ST) and Target of Evaluation (TOE);
- Specification of the ST conventions, terminology, and ST conformance claims; and
- Description of the ST document organization.

1.1 Security Target Identification

Table 1-1 below provides ST Identification Information.

Table 1-1 Security Target Identification

Label	Descriptive Information
TOE Identification:	CA Integrated Threat Management r8.0 which includes eTrust PestPatrol Anti-Spyware Corporate Edition r8.0 and eTrust Antivirus r8.0
ST Title:	CA Integrated Threat Management r8.0.445 Security Target
ST Version:	Version 1.8
ST Author(s):	Debra Baker
ST Date:	May 1, 2007
Assurance Level:	EAL3
Common Criteria Version	Version 2.3
Strength of Function:	SOF-basic
Registration:	<To be filled in upon registration>
Keywords:	Anti-Virus, Anti-Spyware, Anti-Malware, Virus, Spyware, Pest

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for CA Integrated Threat Management. CA Integrated Threat Management is comprised of the eTrust Antivirus r8.0 and eTrust PestPatrol r8.0 products. eTrust Antivirus (eAV) provides anti-virus protection for devices on an enterprise network. It detects and eliminates both file and memory based viruses such as worms and Trojan horses. eTrust PestPatrol (ePP) software is a spyware solution for Windows based enterprise networks. It detects and eliminates trojan horses, keyloggers, distributed denial-of-service attack agents, adware, spyware, and hijacker tools. Additionally CA ITM provides centralized management capabilities for both eAV and ePP through the ITM Console.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 3 from the Common Criteria Version 2.3. There are no PP claims.

1.4 Document Organization

- Section 1, Introduction, identifies the Security Target, includes an Overview, CC Claims, Acronyms, References, Terminology, and Document Conventions.
- Section 2, TOE Description, describes the product type and the scope and boundaries of the TOE.
- Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment, any applicable organizational security policies, and threats relevant to secure TOE operation.
- Section 4, Security Objectives, defines the security objectives for the TOE and its environment.
- Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.
- Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.
- Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.
- Section 8, Rationale presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

1.5 Conventions and Terminology

This section specifies the formatting information used in this ST.

1.5.1 Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.3 of the Common Criteria for Information Technology Security Evaluation. All of the components in this ST are taken directly from Part 2 of the CC except the ones noted with "_EXP" and "-NIAP-xxxx" in the component name. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1 and section 6.3.1.4.2 as:

- iteration: allows a component to be used more than once with varying operations;
- assignment: allows the specification of parameters;
- selection: allows the specification of one or more items from a list; and
- refinement: allows the addition of details.

This ST indicates which text is affected by each of these operations in the following manner:

- *Iterations* are identified with a dash and a number "-#". These follow the short family name and allow components to be used more than once with varying operations. "*" refers to all iterations of a component.

- *Assignments* and *Selections* specified by the ST author are in **[*italicized bold text*]**.
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***<u>italicized bold and underlined text</u>***.
- *Explicitly Stated Requirements* will be noted with a "_EXP" added to the component name.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *Application Note: italicized text.*
- *NIAP and CCIMB Interpretations* have been reviewed. NIAP interpretations are denoted with "-NIAP-xxxx" added to the component name. These are handled as explicitly stated requirements in this ST. The original CC text modified by the interpretation is not denoted nor explained.

1.5.2 Terminology

Table 1-2 Customer Specific Terminology

Term	Definition
Administrator	A trusted user who has full control access rights to administer the TOE.
Adware	Software that displays pop-up/pop-under advertisements when the primary user interface is not visible, or which do not appear to be associated with the product.
Authorized user	An administrator or workstation user that has been identified and authenticated by the TOE.
Device	A device is a personal computer or which hosts the ITM Client software and resides on the target network. The device provides the TOE system data about the target network.
Discovery	The process that detects and profiles devices on the target network. The ITM Server discovers devices on the target network.
ITM Client	A device that has both eTrust Anti-Virus (eAV) and eTrust PestPatrol (ePP) installed on it.
Malware	Malware is software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse. Malware includes both virus and spyware. In this ST, malware refers to both file and memory based malware which includes worms, trojan horses, keyloggers, distributed denial-of-service attack agents, adware, spyware, and hijacker tools.
Organization Tree	The Organization tree is a hierarchical representation of the devices managed on the target network. Through the ITM console, the tree is used to apply policies to groups of computers that require the same protection settings against malicious programs or code. [1]
Policies	A scan policy contains the settings that will be applied to multiple computers to safeguard them against malicious programs or code.
Content Updates	Content updates contain the latest version of signature files, scan engines and program updates. • **Program updates** download patches and other ITM software updates to the TOE. Note: Program updates must be disabled to ensure the TOE remains in the evaluated configuration. See section 2.3.2 for a list of the Program Updates. • **Signature File updates** enables the ITM to recognize new malware and provide protection against them. • **Scan Engine updates** permit the most current signature files to be incorporated into the most current Malware search engine.
DAT files	DAT files contain the signature information that allows ITM to recognize new viruses and spyware and to protect computers from being harmed by them. Also referred to as Signature File Updates.

[1] [ePP Admin] ch 5, p. 35

Term	Definition
Pests	1. Installs even when the user selects "no" in response to question about installing the application. 2. Installs itself or any other item without user permission or knowledge at time of installation. 3. Installs without providing explicit opt-out option from vendor’s site or associated application. 4. Changes browser settings without the user’s permission or knowledge. 5. Changes system configuration in any way without user permission at time of change. 6. Creates or modifies "hosts" file to divert domain reference without user permission or knowledge at time of change. 7. Defends against removal of, or changes to, its components. 8. Dials phone numbers or holds connections open without user permission or knowledge. 9. Displays popup/popunder ads when main product is not actively in use, or which do not appear to be connected with the product. 10. Displays popup/popunder ads that cannot be closed by clicking a clearly visible close button. 11. Updates itself or any other item without user permission or notice at time of update. 12. Silently connects to an unintended location to transmit User Data . 13. Silently modifies another program’s information or website content as displayed – for example, changing search results, substituting ads for other ads, etc. 14. Silently tracks input or personally identifiable information without user permission. 15. Includes mechanisms to thwart removal by security or anti-spyware products (such as requiring manual entry of special code to run its uninstaller). 16. Silently re-installs components after they are removed. 17. Violates or bypasses the access permissions schema inherent to the computer's operating system without permission of each of the users whose rights are being impacted. 18. Cannot be uninstalled by Windows Add/Remove Programs and no uninstaller is provided with application. 19. Uninstaller is actually a silent re-installer. 20. Uninstaller leaves running objects, executables or other unwanted components after reboot. 21. Interferes with the regular operation of another program with out permission. Meets eTrust PestPatrol’s definitions of ANSI Bomb, AOL Pest, AV Killer, Backdoor, Binder, Commercial Remote Access Tool, DDoS, Dialer, DoS, Downloader, Dropper, Firewall Killer, Flooder, Hostile ActiveX, Hostile Java, IRC War, Key Generator, Key Logger, Nuker, Password Capture, RAT, Rootkit, Spoofer, Stealth Installer, Surveillance, Trackware, Trojan, Trojan Creation Tool, Virus Creation Tool, Virus Source, Virus Tutorial or War Dialer . The eTrust PestPatrol pest category definitions can be found here: http://research.pestpatrol.com/KnowledgeBase/Glossary.asp[2]
Spyware	Any application that employs a user's network connection in the background without their permission or knowledge, and gathers or transmits information on the user or their behavior. Many spyware applications collect referrer data (that is, information from the user's web browser that reveals the URL of the page that was linked from), IP address (a number that is used by computers on the network to locate a particular computer), and system information (such as time of visit, type of browser used, operating system and platform, and CPU speed). Spyware applications are sometimes bundled with other commercial products, and may be introduced to machines when those commercial products are installed. Note: The term 'Spyware' is often used to denote a broad category of non-viral malware. In the context of this ST, however, and in the eTrust Pest Patrol product line, the use of the term 'Spyware' is intended to represent a specific category of application as defined here.

[2] CA Spyware Information Center web site, eTrust™ PestPatrol® Spyware Scorecard v2.05.09, 09/30/05

Term	Definition
Target network	The domain of devices that have the ITM Client installed on them.
Virus	In general terminology, “virus” is used generically to refer to an entire suite of exploits of security vulnerabilities, such as worms and trojan horses. The same term is used more specifically to refer to exploits that replicate themselves. A virus is a program or piece of code that is loaded onto a computer without the user’s knowledge and runs against a user’s wishes. Viruses can also replicate themselves. In this instance, a virus can quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.
Workstation User	The Workstation user is considered an authorized user of the TOE on their own computer. The computer they have been assigned.

Table 1-3 CC Specific Terminology

Term	Definition
Authorized user	A user who may, in accordance with the TSP, perform an operation.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

1.5.3 Acronyms

Table 1-4 Acronyms

Acronym	Definition
ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AGD	Guidance Documents
ALC	Life cycle support
ATE	Tests
AVA	Vulnerability assessment
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
EIS	Enterprise Information Systems
FAU	Security Audit
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TSF
FTA	TOE Access
FTP	Trusted Channels/Path

Acronym	Definition
GUI	Graphical User Interface
ICMP	Internet Control Message Protocol
ID	Identifier
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IT	Information Technology
MAU	Media Access Unit
MIB	Management Information Base
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
UDP	User Datagram Protocol

1.5.4 References

Table 1-5 References

Reference Title	ID
Common Criteria for Information Technology Security Evaluation, CCMB-2005-08-002, Version 2.3, August 2005.	[CC]
eTrust PestPatrol Administrator Guide r8.0	[ePP Admin]
eTrust Anti-Virus Administrator Guide r8.0	[eAV Admin]
eTrust PestPatrol Implementation Guide r8.0	[ePP Imp]
eTrust Anti-Virus Implementation Guide r8.0	[eAV Imp]
eTrust Integrated Threat Management Release Summary r8	[REL]
US Government Protection Profile for Anti-Virus Applications for Workstations in Basic Robustness Environments Version 1.0 January 6 2005	[AV PP]
Consistency Instruction Manual for the development of Protection Profiles (PP) for use in Medium Robustness Environments Release 2.0 1 March 2004	[MED ROB]
Text for ISO/IEC WD 15446, Information technology – Security techniques – Guide for production of Protection Profiles and Security Targets 1999-07-07 PROJECT: 1.27.22	[PP Guide]

2 TOE Description

2.1 Product Type

CA Integrated Threat Management r8.0.445 (ITM) is comprised of the eTrust Antivirus r8.0 and eTrust PestPatrol r8.0 products. eTrust Antivirus (eAV) provides anti-virus protection for devices on an enterprise network. It detects and eliminates both file and memory based viruses such as worms and trojan horses. eTrust PestPatrol (ePP) software is a spyware solution for Windows based networks. It detects and eliminates Trojan horses, keyloggers, distributed denial-of-service attack agents, adware, spyware, and hijacker tools. Both virus and spyware will be referred to as malware in this ST. Using eAV and ePP together provides both an anti-virus and anti-spyware solution; thus an anti-malware solution. Additionally CA ITM provides centralized management capabilities for both eAV and ePP through the ITM Console.

2.2 Product Environment

ITM is used on workstations in a trusted network configuration, as illustrated in Figure 2-1. The Firewall/Guard at the boundary of the trusted network represents one or more systems that perform protection services for the trusted network as a whole. It is assumed that protocols commonly used to transport viruses, such as SMTP, HTTP, and FTP, are screened at the Firewall/Guard function. This provides a “defense in depth” since the TOE (executing on the workstations) performs similar functions.

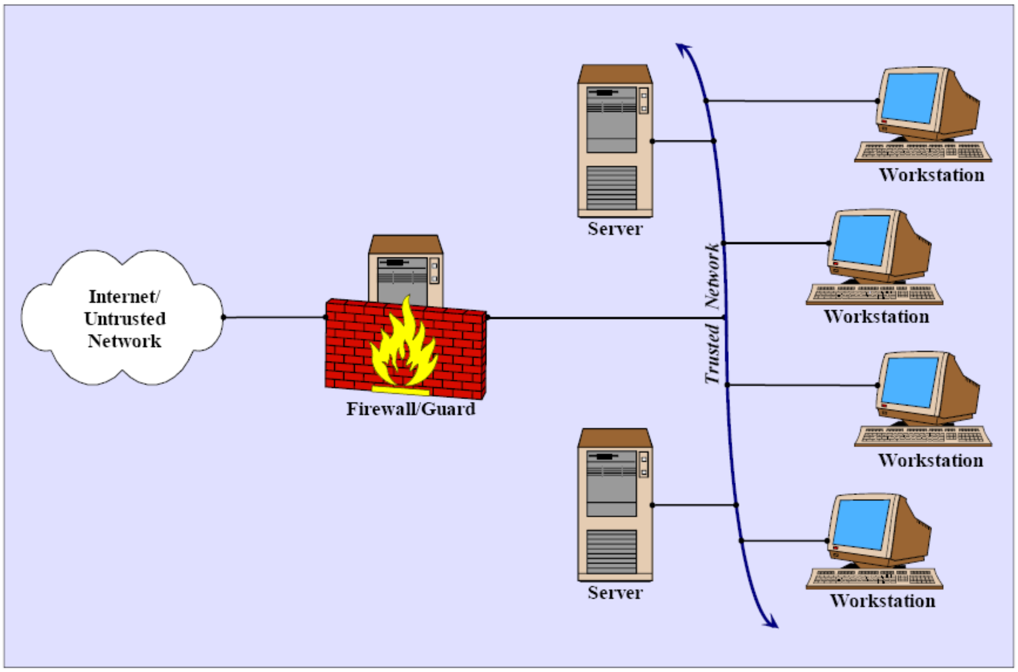

Figure 2-1 Network Environment of the TOE

It is expected that ePP and eAV may be executing on both the servers (e.g., network attached storage, email servers, web servers) and workstations within the trusted network.

2.3 CA Integrated Threat Management Components

The TOE components that comprise CA ITM are as follows: Integrated Threat Management Server and the Integrated Threat Management Client. The ITM Server includes the ITM Console which is used to administer the TOE and the Alert Manager which is used to administer alerts. The ITM Client includes the PestPatrol Client Software and Anti-Virus Client Software.

2.3.1 ITM Server

The Integrated Threat Management Server is the software that tracks all instances of ePP and eAV running on the target network. Authorized administrators are able to perform remote management of security functions via the ITM Console. One function of the ITM Server is to automatically discover clients on the target network. The ITM Console runs on the ITM Server and can be accessed via a web browser from remote clients. The network path between the ITM Server and browser is secured by HTTPS.

2.3.1.1 ITM Console

ITM Console is a Java-based interface that runs on the computer hosting the ITM Server. The Administrator(s) can use the console to remotely manage all ITM Clients, propagate configurations, and set and enforce security policy. The ITM Console allows the central administrator to:

- Discover and manage the configuration of CA Integrated Threat Management products running on computers in the target network
- Create and enforce policies for virus, pest, and spyware scanning
- Distribute scanning policies to ITM Clients throughout the target network
- Download ITM Client content updates from the trusted CA site to the ITM Server
- Distribute the ITM content updates from the ITM Server to the ITM Clients
- Configure distribution proxies to increase network traffic efficiency
- Grant other users permissions to use the ITM Console
- View logs of remote computers and scheduled scan jobs
- Schedule and view reports that provide detailed information about the health of ITM Clients on the target network [3]

From the ITM Console, an authorized administrator can manage the organization of all computers in the target network that are running instances of ePP and eAV using an organizational structure similar to a directory tree, called the Organization tree. Policies can then be assigned to the various branches of the tree.

2.3.1.2 Alert Manager

The Alert Manager is a component that allows an Administrator to configure how and where alerts will be sent. It is a separate interface from the ITM Console that is used to manage ePP and eAV alerts.

There are two basic components to the Alert Manager: the Alert Manager service, which is responsible for the reception, processing, and distribution of Alert messages, and the Alert Manager interface, where an administrator configures how Alert should send its messages.

[3] [ePP Admin] ch 2, p.17

2.3.2 ITM Client

The ITM Client refers to a workstation that has both the eTrust PestPatrol and Anti-virus clients installed on it. These are two separate executables that can be installed independently. In the evaluated configuration, the ITM Client has both ePP and eAV installed on it. The client user interface also referred to as the ITM Agent Interface exists only for eAV. ePP is an executable that runs in the background and has no user interface. For the purposes of simplicity, in the rest of the ST, the term malware includes viruses, pests, and spyware. See Table 1-3 for more information.

The ITM Client can be configured to be a proxy server. There are two settings: Redistribution option and Policy Proxy Server.

The Redistribution option enables an ITM Client to redistribute content updates to other ITM Clients. Content updates include product updates, signature updates, and scan engine updates.

Application Note: To ensure the TOE is maintained in the evaluated configuration the following Content Update components (Product Updates) must be disabled using the Components sub-tab under the Policy Management Tab.:

- *eTrust Antivirus Base*
- *eTrust Antivirus Local GUI*
- *eTrust PestPatrol Base*
- *eTrust ITM Admin GUI*
- *eTrust ITM Console Server*
- *eTrust ITM Common*
- *iGateway*

The following Content Update components (Scan Engine and Signature Updates) may be enabled in the evaluated configuration to allow signature and scan engine updates:

- *eTrust InoculateIT Engine*
- *eTrust Vet Engine*
- *eTrust PestPatrol Clean*
- *eTrust PestPatrol Engine*
- *eTrust PestPatrol Signatures*
- *eTrust Antivirus Arclib archive library*
- *eTrust Antivirus Realtime Drivers*

Note: The eTrust Antivirus Signature Updates are embedded within the InoculateIT and Vet Engine components

A policy proxy server redistributes policies. By designating one or more policy proxy and redistribution servers, network efficiency is improved because the workload of distributing policy and content updates is shared with the Threat Management Server.

2.3.2.1 PestPatrol Client Software

The PestPatrol Client software enables spyware and pest scanning on the client computer. The ePP Software runs on Windows platforms and can be managed centrally using the ITM Console.

ePP includes the following features:

- **Active Protection** which runs in the background of a computer and constantly scans the computer's memory for pests and spyware. When known spyware and/or pests are detected in active memory, the affected process is terminated.[4] When configured to monitor cookies, ePP detects and deletes known spyware cookies. Active Protection auto starts when the computer is rebooted.
- **Alert Forwarding** is used to forward alerts to the ITM Console.
- **Command line scanner** is used to invoke scanning tasks on client computers.
- **Proxy services** used to distribute content updates and scan policies

2.3.2.2 Anti-Virus Client Software

eTrust AntiVirus is the software that enables anti-virus scanning on the client computer. eAV runs on Windows platforms and can be managed centrally using the ITM Console. eAV includes a web-based interface (eAV agent interface) that lets end-users scan their local computers for viruses and apply the latest signature to them. [5] eAV includes the following features:

- **Real time Monitor** which is an automatic, intercept driven scanner that checks a local computer for virus infections each time a file is executed, accessed, or opened.[6] The Real time Monitor automatically starts up on reboot of the workstation.[7]
- **Local Scanner** that checks a local computer for virus infections at the user's request. Using the ITM Agent interface, scans can be manually initiated or scheduled to run at a specific date and time or at repeated intervals.
- **Shell Scanner** is a scanner that integrates with the Microsoft Windows operating system so the end user can right-click on any item on the desktop or in Windows Explorer and run a scan.
- **Alert Forwarding** is used to forward alerts to the ITM Console.
- **Proxy services** used to distribute content updates and scan policies

[4] [ePP Admin] ch 1, p.10

[5] [eAV Admin] ch 1, p.10

[6] [eAV Admin] ch 1, p.11

[7] [eAV Admin] ch 6, p. 49

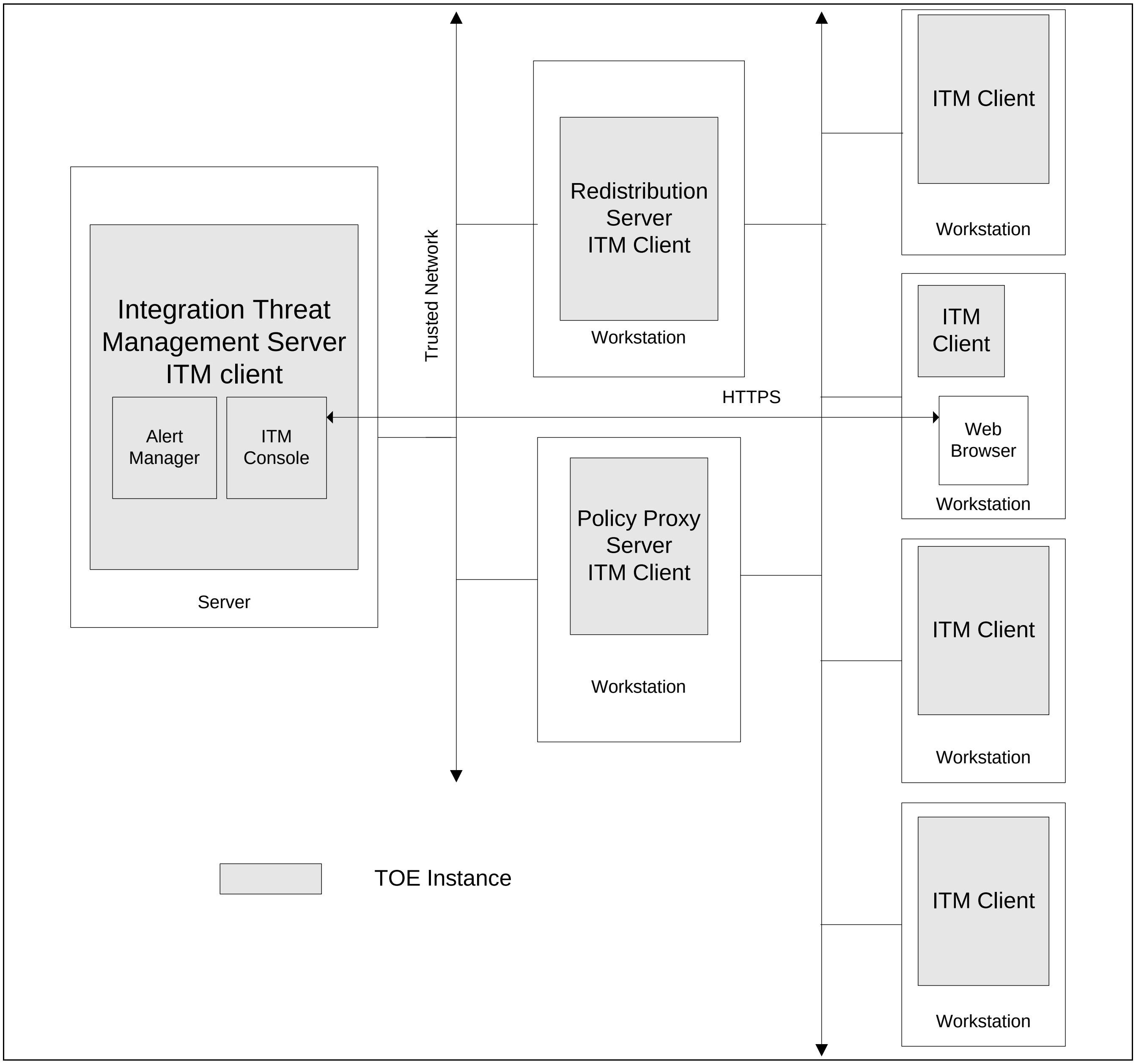

Figure 2-2 Example of Typical CA ITM Deployment

In a typical CA ITM deployment, there would be one centralized ITM Server running the ITM Console, and Alert Manager. In order to distribute the workload of distributing content updates and scan policies multiple redistribution and policy proxy servers would be deployed. Each redistribution and policy proxy server would serve multiple ITM Client machines. Every workstation and server in the target network would have the ITM Client installed on it.

2.4 TSF Physical Boundary and Scope of the Evaluation

The TOE is the CA Integrated Threat Management software product. There is no difference between the TOE and the CA ITM product. All of the components described in section 2.3 are included in the TOE (See Figure 2-3 below).

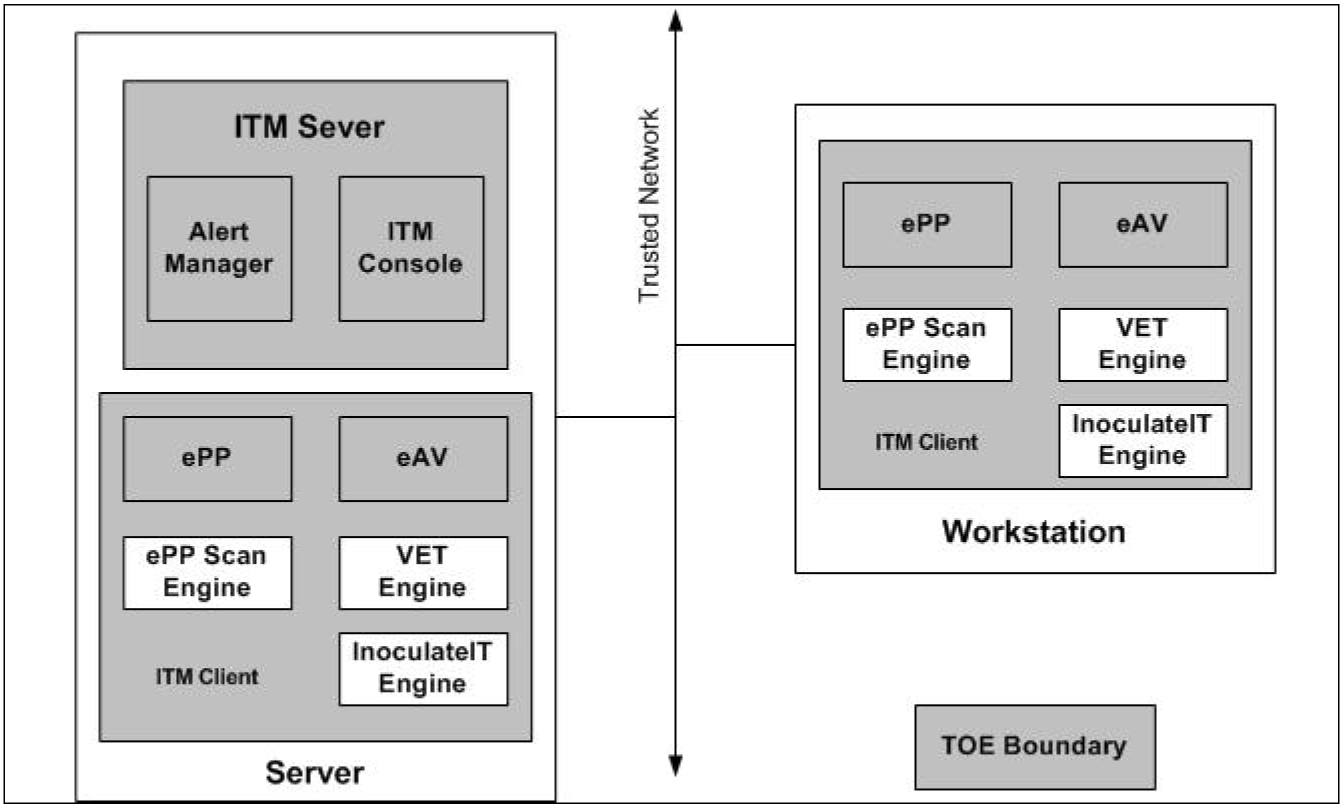

Figure 2-3 TOE Boundary

<u>The TOE includes the following software only components</u>:

- ITM Server r8 which includes the java based interfaces (ITM Console, Alert Manager)
- ePP r8,
- eAV r8.

<u>The evaluated configuration includes the following:</u>

- CA Integrated Threat Management Server r8.0 running on Windows 2003
- ITM Client on the ITM Server running on Windows 2003
- One or more ITM Clients (eTrust PestPatrol r8.0 and eTrust Anti-Virus r8.0) running on 3 Windows XP machines.

In the evaluated configuration, ePP will be configured to monitor cookies.

<u>The TOE does not include the following:</u>

- ePP Scan Engine
- VET Engine
- InoculateIT Engine
- Underlying operating system (OS) software and hardware
- SSL implementation

- Transport standards HTTP, HTTPS, and FTP implementations
- SMTP implementation
- Web server and browser software

2.5 Logical Boundary

The ITM product is included in the TOE's Logical Boundary. All of the TOE features described in section 2.3 of this ST are included in the TOE Boundary except for the scan engines. In particular, the TOE includes the ITM Console provided to the administrator primarily to define the scan policies and to review the logs. In addition, it includes the eAV client GUI that is used to manage the eAV client on the workstation.

The logical boundaries of the TOE can be described in the terms of the security functionalities that the TOE provides to the system that utilizes this product for the detection of viruses and malicious code.

The logical boundary of the TOE will be broken down into the following security class features which are further described in sections 5 and 6. CA Integrated Threat Management provides the following security features:

- **Security audit** – ITM provides security auditing capabilities. The ITM Server audits the discovery information of devices, information malware scans, and information on the scan policies that are created and propagated to the ITM Clients. The ITM Clients audit the scans that have been run and the actions taken when malware is detected.
- **Anti-Malware** – ITM provides for discovery data collection of the devices on the target network. The ITM Client invokes scans, detects, and takes action against malware. Alerts and data reporting are provided by the TOE.
- **Identification and authentication** - ITM provides user identification and authentication through the use of user accounts and passwords for Administrators. Administrators have to identify and authenticate themselves before being allowed access to the ITM Console.
- **Security management** - ITM provides security management through the use of the ITM Console. Administrators are able to discover devices, configure and propagate scan policies, and manage access permissions. Through the enforcement of access permissions, the ability to manage access to TSF data is controlled.
- **Partial protection of TSF** – The ITM Server and client provides partial protection of TSF data. The TOE presents limited access to end users. It maintains and controls individual sessions for Administrators.

2.6 TOE Security Environment

It is assumed that there will be no untrusted users or software on the ITM Server hosts. The ITM Server and ITM Client rely upon the underlying operating system and platform to provide reliable time stamps and to protect the ITM Server and ITM Client hosts from interference or tampering. See Table 2-1 below for more detailed information regarding the supported operating systems. The TOE environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

The TOE security environment can be categorized as follows:

- **Anti-Malware** – ITM relies on the IT Environment scan engines to perform the anti-malware scans.

- **Identification and authentication** - ITM relies on the IT Environment to provide user identification and authentication at the Operating System level. The root or Windows administrator user on the ITM Server is automatically granted full control of the root categories of the subnets and the Organization tree. This account, therefore, has administrative control over both the Threat Management Server computer and the features available from the eTrust Threat Management Console. On the ITM Client, once the user has identified and authenticated to the OS, it has access to the eAV GUI
- **Cryptographic support** - ITM relies on the IT environment to provide cryptographic support. These include:
  - All communications between the web browser accessing the ITM Console and the ITM Server are encrypted using SSL. This applies when the ITM Console is being accessed from another machine as in Figure 2-2. Note: The Alert Manager is a Java Based GUI that is not web enabled, and it sits on the ITM Server.
  - All communications between the ITM Server and the ITM Clients are encrypted. This applies when scan polices, malware signature updates, and product software updates are being propagated. This also applies to Redistribution and Policy Servers communicating with the ITM Clients.

  Application Note: During the discovery process, standard broadcasts (an IP-directed broadcast, a UDP multicast, or a UDP unicast) are used and these sessions are not encrypted.

  - Calculation of the message digest to verify the integrity of the signature files.
  - Communications between the ITM Server and CA server are encrypted when product software updates and malware signature files are downloaded from the trusted CA site.
  - The download method for gathering the updates from the CA website is HTTP. In communicating with the CA web site, the client embeds it's version information and component into the URL. Based on the embedded information the web site returns a digitally signed XML file. Based upon information in the XML file the client determines which updates are needed and downloads the appropriate package.
- **Partial protection of TSF** - ITM relies on the underlying OS to provide security capabilities for the TOE's protection. The TSF relies on the host OS to prevent other applications from:
  - Interfering with an executing TSF
  - Bypassing the TOE security functions at the OS level, and
  - Modifying TSF configuration and executable images on disk.
- **Reliable Time –** the ITM Server and ITM Client rely on the underlying OS for reliable time.

Table 2-1 Supported Operating Systems[8]

Product Component	Version	Platforms
ITM Server	r8	Microsoft Windows NT/2000/2003
Anti-Virus Client Software	r8	Microsoft Windows NT/2000/2003/XP
PestPatrol Client Software	r8	Microsoft Windows NT/2000/2003/XP
Java-based Interfaces (ITM Console, Alert Manager)	r8	Microsoft Windows NT/2000/2003/XP

[8] [REL] p.20

3 TOE Security Environment

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1 Assumptions

Item	Assumption ID	Assumption Description
1.	A.AuditBackup	Administrators will back up the audit files and monitor disk usage to ensure audit information is not lost.
2.	A.NoEvil	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
3.	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the ITM Server.
4.	A.Physical	It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
5.	A.Users	It is assumed that TOE users will protect their authentication data.
6.	A.SecureUpdates	Administrators will implement secure mechanisms for receiving and validating updated signature files from the Anti-Malware vendors.

3.2 Threats

There are threats to the assets against which protection will be required. A ‘threat’ is simply an undesirable event, possibly caused by an identified threat agent, which places, or may place, the assets at risk.[9] The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product.

Table 3-2 Threats

Item	Threat ID	Threat Description
1.	T.AdminError	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
2.	T.AuditCompromise	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.
3.	T.Masquerade	A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain access to TSF data or TOE resources.
4.	T.MaliciousTSFCompromise	A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
5.	T.Malware	A malicious agent may attempt to introduce malware onto a workstation via network traffic or removable media to compromise data on that workstation, or use that workstation to attack additional systems.
6.	T.RemoteTransmit	TSF data may be disclosed or modified by an attacker while being transmitted between the TOE and remote trusted IT products.
7.	T.Transmit	TSF data may be disclosed or modified by an attacker while being transmitted between distributed portions of the TOE and between the TOE and remote administrators.
8.	T.UnidentifiedActions	Failure of the authorized administrator to identify and act upon unauthorized actions may occur.

[9] [PP Guide], p.19

3.3 Organizational Security Policies

Table 3-3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to this TOE.

Item	OSP ID	OSP Description
1.	P.Accountability	The authorized users of the TOE shall be held accountable for their actions within the TOE.
2.	P.ManualScan	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

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives for the TOE are as follows:

Table 4-1 TOE Security Objectives

Item	TOE Objective	TOE Objective Description
1.	O.AdminRole	The TOE will provide administrator roles to isolate administrative actions.
2.	O.AuditGeneration	The TOE will provide the capability to detect and create records of security-relevant events.
3.	O.AuditReview	The TOE will provide the capability to selectively view audit information
4.	O.AuditProtection	The TOE will provide the capability to protect audit information.
5.	O.DataScan	The TOE will collect and store discovery data from the devices on the target network.
6.	O.Manage	The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
7.	O.PartialSelfProtection	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.
8.	O.RobustTOEAccess	The TOE will provide mechanisms that control a user's logical access to the TOE.
9.	O.Malware	The TOE will invoke the detection of malware and will take action against known malware introduced to the workstation via network traffic or removable media.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Table 4-2 Security Objectives for the IT Environment

Item	Environment Objective	Environment Objective Description
10.	OE.AuditStorage	The IT environment will provide a means for secure storage of the TOE audit log files.
11.	OE.Malware	The IT environment will detect and take action against known malware introduced to the workstation via network traffic or removable media.
12.	OE.Manage	The IT environment will provide all the functions and facilities necessary to support the authorized users in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
13.	OE.PartialSelfProtection	The IT environment 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.
14.	OE.RemoteSecureComms	The IT environment will provide a secure line of communications between the TOE and remote trusted IT products.
15.	OE.SecureComms	The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
16.	OE.TimeStamps	The underlying operating system will provide reliable time stamps.
17.	OE.TOEAccess	The IT Environment will provide mechanisms that control a user's logical access to the TOE.

4.2.2 Security Objectives for Non-IT Security Environment

The Non-IT security objectives are as follows:

Table 4-3 Security Objectives for Non-IT Security Environment

Item	Non-IT Environment Objective	Non-IT Environment Description Objective
18.	ON.AuditBackup	Those responsible for the TOE must ensure that the audit files will be backed up and will monitor disk usage to ensure audit information is not lost.
19.	ON.Install	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
20.	ON.NoUntrusted	Those responsible for the TOE must ensure that there are no untrusted users and no untrusted software on the ITM Server host.
21.	ON.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
22.	ON.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.
23.	ON.ProtectAuth	Users must ensure that their authentication data is held securely and not disclosed to unauthorized persons.
24.	ON.SecureUpdates	Those responsible for the TOE will implement secure mechanisms for receiving and validating updated signature files from the Anti-Malware vendors.

5 IT Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies are described. These requirements consist of functional components from Part 2 of the CC as well as explicitly stated components derived from Part 2 of the CC, assurance components from Part 3 of the CC, and relevant interpretations.

5.1 TOE Security Functional Requirements

The functional security requirements for the TOE consist of the following components derived from Part 2 of the CC and NIAP interpretations, summarized in the Table 5-1 below. This section contains the TOE Functional components for CA Integrated Threat Management.

Table 5-1 Functional Components

Item	SFR ID	SFR Title
1.	FAU_GEN.1	Audit data generation
2.	FAU_SAR_EXP.1	Audit review
3.	FAU_STG_EXP.1-1	Protected audit trail storage
4.	FAM_SDC_EXP.1	Discovery data collection
5.	FAM_SCN_EXP.1-1	Anti-Malware scanning
6.	FAM_ACT_EXP.1	Anti-Malware actions
7.	FAM_ALR_EXP.1	Anti-Malware alerts
8.	FAM_DRS_EXP.1	Data reporting
9.	FIA_ATD.1*	User attribute definition
10.	FIA_UAU_EXP.2 -1	User authentication before any action
11.	FIA_UID_EXP.2 -1	User identification before any action
12.	FMT_MOF.1*	Management of security functions behaviour
13.	FMT_MTD.1-1	Management of TSF data
14.	FMT_SMF.1	Specification of management functions
15.	FMT_SMR.1	Security roles
16.	FPT_SEP_EXP.1-1	TSF domain separation

5.1.1 Class FAU: Security Audit

5.1.1.1 FAU_GEN.1 Audit data generation

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

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

b) All auditable events for the **[*not specified*]** level of audit; and

c) **[*the audit events specified in Table 5-2*]**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[*the additional information identified in Table 5-2*]**.

Table 5-2 Audit Events

Item	SFR	Auditable Events	Additional Information
1.	FAU_GEN.1	None	Not Applicable
2.	FAU_SAR_EXP.1	None	Not Applicable
3.	FAU_STG_EXP.1-1	None	Not Applicable
4.	FAM_SDC_EXP.1	Discovery information	hostname, IP Address, MAC Address, malware signature or DAT file version information, product version information, policy settings, and OS version. The packets also include updates for any changes since the previous discovery.
5.	FAM_SCN_EXP.1-1	Malware scans	Malware detected
6.	FAM_ACT_EXP.1	Action taken in response to detection of a malware	Malware detected Action taken File or process identifier where the virus was detected
7.	FAM_ALR_EXP.1	None	Not Applicable
8.	FAM_DRS_EXP.1	None	Not Applicable
9.	FIA_ATD.1*	None	Not Applicable
10.	FIA_UAU_EXP.2 -1	None	Not Applicable
11.	FIA_UID_EXP.2 -1	None	Not Applicable
12.	FMT_MOF.1	None	Not Applicable
13.	FMT_MTD.1	None	Not Applicable
14.	FMT_SMF.1	None	Not Applicable
15.	FMT_SMR.1	None	Not Applicable
16.	FPT_SEP_EXP.1	None	Not Applicable

5.1.1.2 FAU_SAR_EXP.1 Audit review

FAU_SAR_EXP.1.1 The TSF shall provide the Administrator and workstation users with the capability to read all anti-virus related audit information from the audit records on the workstation being used.

FAU_SAR_EXP.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: This SFR only covers the viewing of the anti-virus related audit logs through the ITM Console and on a workstation through the eAV GUI running the ITM Client.

5.1.1.3 FAU_STG_EXP.1-1 Protected Audit Trail Storage

FAU_STG_EXP.1.1-1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion via the TSFI.

FAU_STG_EXP.1.2-1 The TSF shall be able to prevent unauthorised modifications to the audit records in the audit trail via the TSFI.

Application Note: FAU_STG_EXP.1 applies to both the ITM Server and the ITM Clients.

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

5.1.2 Class FAM: Anti-Malware (Explicitly Stated)

5.1.2.1 FAM_SDC_EXP.1 Discovery data collection

FAM_SDC_EXP.1.1 The TSF shall be able to collect the information from the devices on the target network (see column 1 of Table 5-3).

FAM_SDC_EXP.1.2 At a minimum, the TSF shall collect and record the following information:

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

b) The additional information specified in the Details column of Table 5-3 Discovery Data.

Table 5-3 Discovery Data

Devices	Discovery Process Event	Data Details
Devices (personal computer, server)	IP-directed broadcast	hostname, IP Address, MAC Address, malware signature or DAT file version information, product version information, policy settings, and OS version. The packets also include updates for any changes since the previous discovery.
	UDP multicast	
	UDP unicast	

5.1.2.2 FAM_SCN_EXP.1-1 Anti-Malware scanning

FAM_SCN_EXP.1.1-1 The TSF shall invoke real-time scans for memory-based malware based upon known signatures.

FAM_SCN_EXP.1.2-1 The TSF shall invoke real-time, scheduled, and on-demand scans for file-based malware based upon known signatures.

FAM_SCN_EXP.1.3-1 The TSF shall invoke scheduled scans at the time and frequency configured by the Administrator.

FAM_SCN_EXP.1.4-1 The TSF shall invoke manual scans when directed by the Workstation User.

5.1.2.3 FAM_ACT_EXP.1 Anti-Malware actions

FAM_ACT_EXP.1.1 Upon detection of memory-based malware, the TSF shall prevent the malware from further execution.

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

a) Clean the malware from the file,

b) Quarantine the file,

c) Delete the file,

d) Quarantine the user.

5.1.2.4 FAM_ALR_EXP.1 Anti-Malware alerts

FAM_ALR_EXP.1.1 Upon detection of a virus, the TSF shall display an alert on the screen of the workstation on which the virus is detected. The alert shall identify the virus that was detected and the name of the infected file.

FAM_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 logs out of the workstation.

Application Note: The only alerts that are sent to the console on the workstation are from eAV Realtime Monitor scans.

FAM_ALR_EXP.1.3 Upon receipt of an audit event from a workstation indicating detection of malware, the TSF shall display an alert on the screen of the Console if a session is active. The alert shall identify the workstation originating the audit event, the malware that was detected, and the name of the infected file..

FAM_ALR_EXP.1.4 The TSF shall continue to display the alerts on the screen of the Console until they are acknowledged by the Administrator, or the Administrator session ends.

5.1.2.5 FAM_DRS_EXP.1 Data Reporting

FAM_DRS_EXP.1.1 The TSF shall be able to report on collected Discovery Data using automatically generated reports.

FAM_DRS_EXP.1.2 The TSF shall be capable of generating the following reports:

- Discovery Statisitcs Reports
- Managed Machine Reports
- Scheduled Job Reports
- Top Ten Reports
- Categorized Reports
- Mail Option Reports

5.1.3 Class FIA: Identification and Authentication

5.1.3.1 FIA_ATD.1-1 User attribute definition

FIA_ATD.1.1-1 **Refinement:** The TSF shall maintain the following list of security attributes belonging to individual ***administrators***:

- **[*User name***
- ***Password***
- ***Access permissions.*]**

5.1.3.2 FIA_ATD.1-2 User attribute definition

FIA_ATD.1.1-2 **Refinement:** The TSF shall maintain the following list of security attributes belonging to individual ***workstation*** users:

- **[*none.*]**

5.1.3.3 FIA_UAU_EXP.2-1 User authentication before any action

FIA_UAU_EXP.2.1-1 The TSF shall require each administrator to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.4 FIA_UID_EXP.2-1 User identification before any action

FIA_UID_EXP.2.1-1 The TSF shall require each administrator to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.4 Class FMT: Security Management

5.1.4.1 FMT_MOF.1-1 Management of Security Functions Behaviour

FMT_MOF.1.1-1 The TSF shall restrict the ability to **[*determine the behaviour of, disable, and enable*]** the functions **[**

b) Real-time malware scanning, and

***c) Scheduled malware scanning*]**

to **[*the Administrator*]**.

5.1.4.2 FMT_MOF.1-2 Management of Security Functions Behaviour

FMT_MOF.1.1-2 The TSF shall restrict the ability to **[*modify the behaviour of*]** the functions **[*manually invoked malware scanning*]** to **[*Workstation Users*]**.

Application Note: Allows user to manually invoke a scan on his/her own workstation.

5.1.4.3 FMT_MTD.1-1 Management of TSF Data

FMT_MTD.1.1-1 The TSF shall restrict the ability to **[*query, modify, delete* [*see operations specified in Table 5-4*]]** the **[*TSF Data listed in Table 5-4*] to [*the role as specified in Table 5-4*]**

Table 5-4 Management of TSF Data

Roles	Allowed Operations on TSF Data (Management Functions
Administrator	view, add, remove, and modify users and their permissions
	view, add, modify, and delete discovery of subnets
	view, add, modify, and delete scan policies
	Disable product updates
	view audit logs on the ITM Server and ITM Client workstations; delete audit logs on ITM client workstations
	modify files to be scanned manually on workstations
	view alerts, modify alert policy
Workstation User	Modify files to be scanned manually on workstations Note: The Scan Policy issued from the ITM Server takes precedence over any client policy settings.
	view audit logs on the workstation being used

5.1.4.4 FMT_SMF.1 Specification of management functions

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

- ***determine the behavior of, disable, and enable the behavior of the functions real time and scheduled malware scanning (see FMT_MOF.1-1),***
- ***modify the behaviour of the function manually invoked malware scanning (see FMT_MOF.1-2),***
- ***the operations as specified in Table 5-4 on the TSF Data as specified in Table 5-4 (See FMT_MTD.1-1)*].**

5.1.4.5 FMT_SMR.1 Security roles

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

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

5.1.5 Class FPT: Protection of the TOE Security Functions

5.1.5.1 FPT_SEP_EXP.1-1 TSF Domain Separation

FPT_SEP_EXP.1.1-1 The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP.1.2-1 The TSF shall enforce separation between the security domains of subjects in the TOE Scope of Control.

5.2 Security Requirements for the IT Environment

The ITM Server requires that the operating system platform provide reliable time stamps, non-bypassability, and TSF domain separation. All cryptographic functions are part of the IT environment, not part of the TOE.

Table 5-5 Functional Components for the IT environment

Item	SFR ID	SFR Title
17.	FAM_SCN_EXP.1-2	Anti-Malware scanning
18.	FAU_STG_EXP.1-2	Protected Audit Trail Storage
19.	FIA_UAU_EXP.2-2	User authentication before any action
20.	FIA_UID_EXP.2-2	User identification before any action
21.	FMT_MTD.1-2	Management of TSF data
22.	FPT_ITT.1	Basic Internal TSF Data Transfer Protection
23.	FPT_RVM.1	Non-Bypassability of the TSP
24.	FPT_SEP_EXP.1-2	TSF domain separation
25.	FPT_STM.1	Reliable time stamps
26.	FTP_ITC.1	Inter-TSF trusted channel

5.2.1 Class FAM: Anti-Malware (Explicitly Stated)

5.2.1.1 FAM_SCN_EXP.1-2 Anti-Malware scanning

FAM_SCN_EXP.1.1-2 The IT Environment shall perform real-time scans for memory-based malware based upon known signatures.

FAM_SCN_EXP.1.2-2 The IT Environment shall perform real-time, scheduled, and on-demand scans for file-based malware based upon known signatures.

FAM_SCN_EXP.1.3-2 The IT Environment shall perform scheduled scans at the time and frequency configured by the Administrator.

FAM_SCN_EXP.1.4-2 The IT Environment shall perform manually invoked scans when directed by the Workstation User.

5.2.2 Class FAU: Security audit

5.2.2.1 FAU_STG_EXP.1-2 Protected Audit Trail Storage

FAU_STG_EXP.1.1-2 The IT Environment shall protect the stored audit records in the audit trail file(s) from unauthorised deletion via the Operating System's Interface.

FAU_STG_EXP.1.2-2 The IT Environment shall be able to prevent unauthorised modifications to the audit records in the audit trail file(s) via the Operating System's Interface.

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

5.2.3 Class FIA: Identification and Authentication

5.2.3.1 FIA_UAU_EXP.2-2 User authentication before any action

FIA_UAU_EXP.2.1-2 The IT Environment shall require each user to be successfully authenticated either by the TSF or by an authentication service invoked by the TSF before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID_EXP.2-2 User identification before any action

FIA_UID_EXP.2.1-2 The IT Environment shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.3.2 FMT_MTD.1-2 Management of TSF Data

FMT_MTD.1.1-2 The TSF shall restrict the ability to **[*query, modify, delete* [*see operations specified in Table 5-6*]]** the **[*TSF Data listed in Table 5-6*] to [*the role as specified in Table 5-6*]**

Table 5-6 Management of TSF Data

Roles	Allowed Operations on TSF Data (Management Functions)
Windows Administrator	view, add, remove, and modify users and their permissions
	view, add, modify, and delete discovery of subnets
	view, add, modify, and delete scan policies
	Disable product updates
	view audit logs on the ITM Server and ITM Client workstations; delete audit logs on ITM client workstations
	modify files to be scanned manually on workstations
	view alerts, modify alert policy

5.2.4 Class FPT: Protection of the TSF

5.2.4.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 Refinement: The ***IT Environment*** shall protect TSF data from **[*disclosure and modification*]** when it is transmitted between separate parts of the TOE.

Application Note: FPT_ITT.1 has to do with the connection between the ITM Server/Proxy Server and ITM Clients being secured by SSL. This applies to the distribution of scanning policies and content updates. In addition, this SFR ensures the connection between the workstation running the ITM Console and ITM Server is secured by HTTPS.

5.2.4.2 FPT_RVM.1 Non-Bypassability of the TSP

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

5.2.4.3 FPT_SEP_EXP.1-2 TSF domain separation

FPT_SEP_EXP.1-2 TSF domain separation

FPT_SEP_EXP1.1-2 The security functions of the host OS shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host OS**.**

FPT_SEP_EXP.1.2-2 The security functions of the host OS shall enforce separation between the security domains of subjects in the scope of control of the host OS.

5.2.4.4 FPT_STM.1 Reliable time stamps

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

5.2.5 Class FTP: Trusted Path/channels

5.2.5.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 **Refinement:** The ***IT Environment*** shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 **Refinement:** The ***IT Environment*** shall permit **[*the TSF*]** to initiate communication via the trusted channel.

FTP_ITC.1.3 **Refinement:** The ***IT Environment*** shall initiate communication via the trusted channel for **[*download of content updates*]**.

5.2.6 Strength of Function

The overall strength of function requirement is SOF-basic. The strength of function requirement applies to FIA_UAU_EXP.2-1. The SOF claim for FIA_UAU_EXP.2 -1 is SOF-basic. The strength of the “secrets” mechanism is consistent with the objectives of authenticating users (O.RobustTOEAccess). Strength of Function shall be demonstrated for the non-certificate based authentication mechanisms to be SOF-basic, as defined in Part 1 of the CC. Specifically, the local authentication mechanism must demonstrate adequate protection against attackers possessing a low-level attack potential.

5.3 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 3 (EAL3) taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 5-7.

Table 5-7 EAL3 Assurance Components

Item	Assurance Components	
1	ACM_CAP.3	Authorisation controls
2	ACM_SCP.1	TOE CM coverage
3	ADO_DEL.1	Delivery procedures
4	ADO_IGS.1	Installation, generation, and start-up procedures
5	ADV_FSP.1	Informal functional specification
6	ADV_HLD.2	Security enforcing high-level design
7	ADV_RCR.1	Informal correspondence demonstration
8	AGD_ADM.1	Administrator guidance
9	AGD_USR.1	User guidance
10	ALC_DVS.1	Identification of security measures
11	ATE_COV.2	Analysis of coverage
12	ATE_DPT.1	Testing: high-level design
13	ATE_FUN.1	Functional testing
14	ATE_IND.2	Independent testing - sample
15	AVA_MSU.1	Examination of guidance
16	AVA_SOF.1	Strength of TOE security function evaluation
17	AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 TOE Summary Specification

6.1 IT Security Functions

6.1.1 Overview

Section 6 describes the specific security functions that meet the criteria of the security class features that are described in section 2.5. The following sections describe the IT Security Functions of CA Integrated Threat Management. These interfaces provide the security functions which satisfy the TOE security functional requirements. This section includes a bi-directional mapping between functions and requirements that clearly shows which functions satisfy which requirements and that all requirements are met.

Table 6-1 Security Functional Requirements mapped to Security Functions

Security Class	SFR Item	SFRs	Security Functions
Security audit	1	FAU_GEN.1	SA-1
	2	FAU_SAR_EXP.1	SA-2
	3	FAU_STG_EXP.1-1	SA-3
Anti-Malware	4	FAM_SDC_EXP.1	AM-1
	5	FAM_SCN_EXP.1-1	AM-2
	6	FAM_ACT_EXP.1	AM-3
	7	FAM_ALR_EXP.1	AM-4
	8	FAM_DRS_EXP.1	AM-5
Identification and authentication	9	FIA_ATD.1*	IA-1
	10	FIA_UAU_EXP.2	IA-2
	11	FIA_UID_EXP.2	
Security management	12a	FMT_MOF.1-1	SM-1
	12b	FMT_MOF.1-2	SM-2
	13a	FMT_MTD.1-1	SM-3
	14	FMT_SMF.1	SM-4
	15	FMT_SMR.1	SM-5
Partial Protection of the TSF	16	FPT_SEP_EXP.1-1	TP-1

6.1.2 Security Audit

SA-1 Audit events (FAU_GEN.1)

FAU_GEN.1 describes the TOE‘s auditing capabilities. ITM’s auditing capabilities include recording information about the processing the ITM Server and clients have been performing. The ITM Server audits discovery information of devices, information on the e-mail related malware scans, and information on the scan policies that are created and propagated to the ITM Clients. The ITM Clients audit the scans that have been run and the actions taken when a virus or pest is detected. The ITM Clients send their logs to ITM Server.

Auditing is done both on the ITM Server and at the client. See Table 5-2 and SA-3 for more information.

Failed logins are readable in a file stored on the ITM Server. It is only accessible through the OS.

All log information is stored in a DB directory on the ITM Server, in a file format that is accessible by standard database tools that support the ODBC (Open DataBase Connectivity) standards. This log file is named by the month, day, year, and time of day that it is created and has an extension of .DBF (.dbf on UNIX and OS X systems). [10] An administrator can specify the computer whose logs they are trying to view by entering the Computer Name in the proper field.

Each audit record includes the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

SA-2 Audit review of Workstation (FAU_SAR_EXP.1)

eAV has a user GUI that the workstation user can use to view the anti-virus related audit logs. Since ePP does not have a user GUI, the workstation user cannot view the logs for ePP.

Through the ITM console, the administrator can use the Logs subtab to view the logs for a specific computer. The following types of logs can be viewed:

- Quarantine - Displays logging information for malwarees that were detected during a scan and placed in quarantine.
- Scan Jobs - Displays logging information for scheduled malware scans.
- General Events

  Displays logging information of general events for each day. Operating system error codes are displayed here. This category displays the following types of messages:

  - Critical Message - This is the highest level message. It requires immediate attention once logged. This message could mean there is a serious threat was detected, or there is a problem with the service, such as an error loading an engine.
  - Warning Message - This second priority message provides non-critical warning information.
  - Informational Message - This type of message provides information on events such as a service starting or stopping.

SA-3 Protected Audit Trail Storage (FAU_STG_EXP.1-1)

ITM protects the stored audit records on the ITM Server and clients in the audit trail from unauthorised deletion and modifications via the TSFI. Through the ITM Console, only authorized individuals are able to delete the audit logs. In addition, through the ITM Console, no one is allowed to modify the audit logs. Since the client logs are sent to the ITM Server, they are protected via the TSFI.

For each client computer under the client tab in the ITM console, the administrator can determine whether they want to save all logs or delete them after a certain number of days. The client computer can be configured to forward logs to the ITM Server. The logs stored on the client computer are protected from unauthorized deletion and modification by the operating system interface.

On a client computer, the Alert options can be set to forward logs to the Threat Management Server (or the policy proxy server if the network is setup to forward in an escalation hierarchy level).

[10] [ePP Admin] ch 7, p.58

6.1.3 Anti-Malware (AM)

6.1.3.1 AM-1 Discovery data collection (FAM_SDC_EXP.1)[11]

The ITM Server is able to discover devices on the target network. At a minimum, the ITM Server shall collect and record the following information: date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; as well as the additional details specified in the Details column of Table 5-3 Discovery Data.

The discovery process works as follows:

1. An authorized administrator specifies subnets for the Threat Management Server to query. The administrator also specifies a discovery frequency that sets how often the subnet is polled.

Note: Once a subnet is queried, this frequency dictates how often the discovery information for each client is refreshed.

2. When the subnet definition is saved, an IP-directed broadcast, a UDP multicast, or a UDP unicast is sent (using UDP port 42508) to the defined subnet depending on the election method selected.

3. Through a transparent election process, a computer in that subnet is elected to reply to the Threat Management Server.

4. The elected computer returns response packets to the Threat Management Server (using TCP port 42509). These packets contain information about computers in the subnet that are running eTrust Threat Management products. This information includes: hostname, IP Address, MAC Address, malware signature or DAT file version information, product version information, policy settings, and other general data. The packets also include updates for any changes since the previous discovery.

5. The Threat Management Server stores the discovered data in its database. From this information, the Threat Management Server takes an inventory of the available computers in the security network.

6. This inventory appears on the Discovery tab of the eTrust Threat Management Console. If specified in the subnet definition, each computer also appears on the Organization tab and is automatically associated with a branch of the Organization tree.

The discovery process automatically maintains current information about the status of the eTrust Threat Management products running on each computer on the subnet.

6.1.3.2 AM-2 Anti-Malware Scanning (FAM_SCN_EXP.1-1)

The eITM client invokes anti-malware scanning. ePP and eAV have their own separate scanning capabilities which are described below. The scanning is performed by the IT Environment since the scan engines are located outside the TOE Boundary. ePP runs in the background (in memory) constantly scanning for spyware and pests. eAV runs on demand as either a scheduled scan or on-demand by the user. What scans are run and when is determined by the scanning policy that has been set by the Administrator. See SM-3, *Using the Policy Management tab* for more information.

[11] [ePP Admin] ch 4, p. 29

ePP provides the following scanning methods: [12]

ePP invokes several scanning methods to protect the target network from all types of pests. The following types of scans are invoked by the TOE and performed by the ePP Scan engine that is in the IT Environment:

- **Active Protection -** Runs in the background of a computer (in memory) and continuously checks for and deletes pests in memory. An administrator can create Active Protection policies using the ITM Console for monitoring client computers for spyware and pest processes.
- **Scheduled Scans -** Performs scans at a specific time or interval. An Administrator can create Scheduled Jobs policies using the ITM Console to enforce settings for scheduled scans on client computers.
- **Interactive Scans -** Performs an on-demand scan of a client computer. Using the ITM Console, an Administrator can schedule a scan to run on-demand when requested.
- **Command Line Scan -** Performs scans from the command line. Scan results are written to a log file.

eAV provides the following scanning methods[13]:

eTrust Antivirus provides several scanning methods to protect the target network from all types of infections. The following types of scans are invoked by the TOE and performed by the eAV scanning engines (VET Engine and InoculateIT Engine) that are in the IT Environment:

- **Realtime Monitor Scan**

  Checks for viruses are invoked automatically, each time a file is executed, accessed, or opened. An administrator can create Realtime Monitor policies using the eTrust Threat Management Console to enforce settings for realtime scanning on client computers.

- **Scheduled Scan**

  Performs scans at a specific time or interval. An administrator can create Scheduled Jobs policies using the eTrust Threat Management Console to enforce settings for scheduled scans on client computers.

- **Command Line Scan**

  Invokes scans from the command line. Scan results are displayed on the screen during the course of the scan.

- **Manual Scan**

  Lets end-users initiate interactive scans on their local computer using the eTrust Threat Management Agent interface.

6.1.3.3 AM-3 Anti-Malware Actions (FAM_ACT_EXP.1)

When the ePP/eAV clients invoke a scan, the scanning engine creates a copy of the information (memory or file-based) in a temporary location and opens the copy for malware checking. If the information is clean, ePP/eAV deletes the copy and releases the information. If malware is

[12] [ePP Admin] ch 1, p.12

[13] [eAV Admin] ch.1, p. 13

found, ePP/eAV takes action based on the configured scan policy.[14] Upon detection of both memory and file based malware, the ITM client takes appropriate actions based on the policy that has been set by the Administrator. The management of the scanning policies is described in SM-3 under *Using the Policy Management tab*. The specific actions that can be taken by each agent (ePP and eAV) are described below.

When the ePP client detects memory-based spyware and pests, it prevents the spyware and pests from further execution. The spyware or pest process is stopped and deleted. When known spyware cookies are detected, they are deleted[15]. eAV is also able to scan for infections in programs that are currently running in memory.[16]

When the ePP client detects file-based spyware and pests, it performs the action(s) specified by the Administrator. Actions are administratively configurable on a per-workstation basis and consist of:

a) Clean the pest/spyware from the file by deleting the pest/spyware code from the file.

b) Quarantine the file by placing the file in a zipped file and moving it to a new location.[17]

c) Delete the file by deleting the infected file from the workstation.

When the eAV client detects file-based viruses, it performs the action(s) specified by the Administrator. When the Realtime Monitor finds a virus and a treatment action is unsuccessful, file access is denied, which prevents the infection from being spread further.[18] Actions are administratively configurable on a per-workstation basis and consist of:

a) Clean the virus from the file by deleting the virus/malicious code from the file. This is also referred to as curing the file[19].

b) Quarantine the file by renaming the infected file with a .AVB extension. The infected file can also be moved from its current directory into the Move folder.

c) Delete the file by deleting the infected file from the workstation.

d) Quarantine the user – This feature is only on Windows eAV clients. Enabling the quarantine feature on eAV clients causes users who are detected attempting to copy infected files to a server to be automatically suspended from any further access to that server, thereby helping to isolate the infected user and prevent the spread of the infection.[20]

Although the policy is configurable on a per-workstation basis, it is easier to manage many computers by applying the same scan policy to multiple computers. The Administrator can create and enforce policy settings and assign them to branches in the Organization tree to ensure that all computers are equally protected (See SM-3 for more information). In addition, the Policies that are applied to a

[14] [ePP Admin] ch 1, p.12

[15] [ePP Admin] ch 1, p. 10

[16] [eAV Admin] Appendix A, p. 108

[17] [ePP Admin] ch 6, p.45

[18] [eAV Admin] ch 6, p. 46

[19] [eAV Admin] Appendix A, p. 106

[20] [eAV Admin] ch 6, p.46

branch always take precedence over settings that an end user may have applied to his or her computer locally. [21]

Any time ITM is set to clean a file, the file is automatically quarantined before starting the clean action. Consequently, if the clean action is not completed, the file remains quarantined. Likewise, when ITM is set to delete a file, the file is automatically quarantined before deleting it. Consequently, if the delete action is not able to be performed, the file remains quarantined.

6.1.3.4 AM-4 Anti-Malware alerts (FAM_ALR_EXP.1)

Upon detection of a virus, the eAV Client more specifically the Realtime Monitor will display an alert on the screen of the workstation on which the virus is detected. The alert will remain on the console until the user closes the alert or logs out of the Windows OS.

In addition, the ITM Client will send an alert to the ITM Server which will be displayed on the ITM Console if an administrator is currently logged in. The alert will identify the workstation originating the audit event, the malware that was detected, and the name of the infected file.

The TSF will continue to display the alert on the screen of the ITM Console until it is acknowledged by the Administrator, or the Administrator logs out of the ITM Console.

The following Alert features of ITM allow the receipt of information and messages from client computers:

- Remote management and configuration of Alert Service
- Clients can send alerts using IP, in addition to the standard IPX protocol
- Messages contain full paths of any virus-infected files

The alerts that are sent from the client are fully configurable (See *Using the Alert Manager* under SM-3).

6.1.3.5 AM-5 Data Reporting (FAM_DRS_EXP.1)[22]

The ITM Server collects and collates the logs of computers that are running the ITM Client. The ITM Server will automatically report on collected Discovery Data in the dashboard which displays Top 10 detection information. The dashboard tab provides a quick review of the most common detections on the target network. [23]

The Reports tab of the ITM Console provides access to a wide variety of reports. From this tab an administrator can generate and view reports for discovery statistics, managed machines, scheduled jobs, Top 10 threats, categorized reports, and mail option reports. [24] Many reports provide color graphs, augmented by summary and detailed information, as well. An administrator can also view domain reports for computers in the target network that are grouped into domains that were discovered by the Threat Management Server, whether they are running eTrust Threat Management products or not.

The Threat Management Server generates the reports based on the information collected from each client computer. An administrator determines the start date for the reports, and how often they are generated by using the Report Scheduler options located on the Report tab.

[21] [ePP Admin] ch 6, p.41

[22] [ePP Admin] ch 9

[23] [ePP Admin] ch 3, p.27

[24] [ePP Admin] ch 9, p.69

Discovery Statistics Reports

The Discovery Statistics reports provide statistical information from the Threat Management Server for all discovered computers, as well as those that have expired. Expired computers are those that missed being discovered beyond the number specified in Max Missed Discoveries option on the Discovery tab. An administrator can view these reports by clicking the Machine Information Report folder, which contains the following reports:

- **Deployment -** Displays a list of all eTrust Threat Management products currently installed, grouped by operating system. If a Windows XP computer has both eTrust Antivirus and eTrust PestPatrol installed, the report increments both Antivirus and PestPatrol numbers by 1 for that operating system. If the computer has only eTrust Antivirus, only Antivirus is incremented by 1 for that operating system.
- **Load Per Server -** Displays the load on the downloads sources assigned for content update download in the top three preferences. The report shows the number of computers that have each server listed as a primary or a secondary distribution source.
- **Load Per Policy -** Displays the distribution load on a per policy basis. The report shows the number of computers that have each policy listed.
- **Signatures -** Displays the number of computers that have the virus and pest scanning engines installed. It includes the engine name, number of computers with the engine installed, as well as the counts for each signature or DAT file version detected in the subnets.
- **Signature Exception -** Displays the current version of the signature or DAT file versions for this Threat Management Server, and using this information as a benchmark, shows up to three out-dated signature versions detected for each engine on discovered computers. Note that the most recent, not the oldest, outdated version is shown.
- **Signature Exception Details -** Displays the details of all computers with any of the three outdated signature versions detected in the Signature Exception report. The computer's name, IP address, and MAC address is shown, as well as the Threat Management Server and branch to which the computer belongs.

Managed Machine Reports

The Managed Machines reports display information about managed and unmanaged machines. Computers that have eTrust Threat Management products installed and are being managed by this Threat Management Server are considered *managed* machines. Computers that do not match this criteria are considered *unmanaged* machines. The Threat Management Server must have a discovery definition for the subnet where a computer resides in order to manage it. The reports are generated by enumerating and comparing all domains in a network to the discovered computers in the Threat Management Server database. A match indicates a managed machine; otherwise, the machine is unmanaged.

- **Domain Summary -** Displays every domain detected, and the number of managed and unmanaged machines for each domain.
- **Protected Machines Total -** Displays information about the computers that have eTrust Threat Management products installed, with details including domain name, IP address, branch name, and product version.

- **Unprotected Machines Total -** Displays information about the computers that do not have eTrust Threat Management products installed, with details including associated computer name and domain name.
- **Microsoft Windows Network -**Displays managed and unmanaged machines, by domain name.

Scheduled Job Reports

The Scheduled Job reports displays summary information about the scheduled virus and pest scanning jobs. The report contains the following information:

- **Machine Name -** Name of the computer the job is pushed to by the Threat Management Server.
- **Report Time -** The time that the scan job reports back to the Threat Management Server as completed.
- **Error -** The number of errors encountered by the scan job.
- **Files Scanned -** The number of files scanned by the scan job.
- **Files Cured -** The number of files cured by the scan job.

Top 10 Reports

The Top 10 reports display the most widely detected threats on the target network, grouped into various time-frames. The time frame is calculated based on the local time zone where Threat Management Server is located.

An administrator can also view this information by computers and users. The following reports are available:

- **Top 10 Virus Report -** Displays a top-ten virus summary and a list of all viruses detected grouped into time-frames.
- **Top 10 Pests Report -** Displays a top-ten pest summary and a list of all pests detected grouped into time-frames.
- **Top 10 Machines Report -** Displays discovered computers most often infected by viruses and pests, grouped into time-frames.
- **Top 10 Users Report -** Displays user most often infected by viruses and pests, grouped into time-frames.

Categorized Reports

These reports are broken down into categories by subnet, branch, user, computer, and by the action taken on the threat. The following reports are available:

- **Per Virus Reports / Per Pest Report -** Virus report displays detailed information for each virus detected. Pest reports displays detailed information for each pest detected. An administrator can get specific information about a particular virus or pest by clicking the virus or pest name.

  These two reports provide the following subdivisions:

  - By Subnet - Displays detailed information about the detected virus or pest using the subnet category.

    - By Branch - Displays detailed information about the detected virus or pest using the branch category.
    - By User - Displays detailed information about the detected virus or pest using the user category.
    - By Computer - Displays detailed information about the detected virus or pest using the computer.
    - By Action - Displays detailed information about the detected virus or pest using the action category.
- **Per Pest Category Report -** Displays detailed information about detected pests by pest category.
- **Per Machine Reports -** Displays summary information for each virus or pest found, categorized by computer name.
- **Per User Reports -** Displays summary information for each virus or pest found, categorized by user name.

6.1.4 Identification and Authentication

IA-1 User attribute definition (FIA_ATD.1-1, FIA_ATD.1-2)

The ITM Server maintains the following user security attributes for administrators:

- User name
- Password
- Access permissions

Administrators can be granted access to the ITM Server and ITM Console based on existing user accounts on the computer where the ITM Server resides or elsewhere on the network.

Administrators are granted access to the Alert Manager by logging into the Operating System. There is not a separate login for the Alert Manager Console. In order to be granted access the user has to have a valid account on the Threat Manager Server computer.

To connect to the Threat Management Server computer, a user must have a valid account on the computer where the Threat Management Server resides. Before a user can manage branch policies in the Organization tree, an authorized administrator must first set access permissions for that user's account (see Table 6-2). These permissions determine the user's ability to change policy settings and perform other management tasks. Note that if the user wants to add a computer to a branch, he or she must have administrative authority for that computer.

Authorized administrator accounts do not have any special permission on the operating system where the Threat Management Server resides. They can be granted different levels of permissions within the eTrust Threat Management Console; from full access to all features of the eTrust Threat Management Console, to read-only access. [25]

The ITM Server does not maintain user security attributes for workstation users. Workstation users are only identified by their windows id and password. This is handled by the OS. Once a user has been identified and authenticated by the OS, they have access to the eAV GUI and command line scanners on their own workstation.

[25] [eAV Admin] ch 8, p. 78

The Administrator is the authorized administrator of the TOE who has full control of the ITM Console. Access rights apply to containers in the Organization tree and to subnets. The following table lists the types of access and the associated permissions:

Table 6-2 Access Permissions[26]

Type of Access	Permissions
None	User has no access to the ITM console
Read	User has read access to the Organization and Discovery tabs. Access to view an object in the list and its associated properties, but no access to make changes or move a computer to a different branch.
Change	User has change access to the Organization and the Discovery tabs. Access to see an object and its properties in the list, access to make changes to the policy settings applied to a branch, and ability to move a computer to a different branch.
Delete	User has access rights to delete the selected item. Includes changing permissions, but cannot add users.
Full Control	User has full control. Can add users and grant access for managing access permissions to other accounts.

IA-2 User identification and authentication (FIA_UAU_EXP.2-1, FIA_UID_EXP.2-1)[27]

Each administrator user must be successfully identified and authenticated with a password by the TSF before access is allowed to the ITM Server and Console.

Administrators are granted access to the Alert Manager by logging into the Operating System. There is not a separate login for the Alert Manager Console. In order to be granted access the user has to have a valid account on the Threat Manager Server computer.

The following types of accounts can have access to the Integrated Threat Management Server: (note: see the *Identification and authentication for the IT Environment* below for more information regarding the IT Environment).

- Authorized administrator accounts

The eTrust Threat Management Console's built-in security features lets an authorized administrator grant control to personnel charged with managing the ITM Clients in the target network as needed[28]. The access permissions for authorized administrator accounts on the Integrated Threat Management Server are independent of the authority granted to the account by the operating system.

Only valid, authorized administrator user accounts can access the eTrust Integrated Threat Management Console to manage the ITM Server and clients. The management functions the authorized administrator can perform are based upon the permissions granted to that user account. Authorized administrator accounts can, in turn, grant permissions to other accounts.

The authorized administrator defines a user's privileges in the eTrust Integrated Threat Management Console by setting access permissions for that user. These permissions are applied to the subnets and branches in the Organization tree. When a user attempts to log onto the Integrated Threat Management Server, the server examines these settings to determine if the user is valid and what

[26] [ePP Admin] ch 8 p. 65 [eAV Admin] p. 79

[27] [ePP Admin] ch 8, p.62

permissions he or she has. To do so, the Threat Management Server component consults its own internal security table.

Operating System Administrator Account

The operating system administrator or root account on the computer where the Threat Management Server resides is automatically granted full control of the root categories of the subnets and the Organization tree. This account, therefore, has administrative control over both the Threat Management Server computer and the features available from the eTrust Threat Management Console. For Windows, this is the Administrator account. This administrator account on the Threat Management Server can in turn designate another user with a valid account on the Threat Management Server to have authorized access to the eTrust Integrated Threat Management Console.

Threat Management Server Installer Account

Similar to the privileges that are automatically assigned to the operating system administrator account, the account that installs the Threat Management Server is also automatically granted full control of the root categories of the subnets and the Organization tree.

If the operating system administrator account is used to install the Threat Management Server, then a separate installer account will not be created, otherwise, a separate installer account appears in the list of user accounts, when the access permissions are displayed.

Authorized Administrator Accounts

The operating system administrator account can grant access permissions to other users that have valid operating system accounts on the computer where the Threat Management Server resides, or to existing accounts on the network. Users that are given these rights are referred to as authorized administrators for the security network.

To connect to the Threat Management Server computer, a user must have a valid account on the computer where the Threat Management Server resides. Before a user can manage branch policies in the Organization tree, an authorized administrator must first set access permissions for that user's account. These permissions determine the user's ability to change policy settings and perform other management tasks. Note that if the user wants to add a computer to a branch, he or she must have administrative authority for that computer.

Authorized administrator accounts do not have any special permission on the operating system where the Threat Management Server resides. They can be granted different levels of permissions within the eTrust Threat Management Console; from full access to all features of the eTrust Threat Management Console, to read-only access. An authorized administrator can set permission levels based upon the needs of the enterprise. An authorized administrator has great flexibility in assigning these access permissions. See Table 6-2 for more detailed information on access rights.

Identification and authentication for the IT Environment (FIA_UAU_EXP.2-2, FIA_UAU_EXP.2-2)

ITM also relies on the underlying OS to provide identification and authentication of users who are able to login directly to the server OS hosting the ITM Server software.

The following types of accounts can have access to the Integrated Threat Management Server:

- The operating system administrator or root account on the computer where the Integrated Threat Management Server resides. Note: The OS is outside the TOE Boundary.
- The account used to install the Threat Management Server (a user with administrative privilege on Windows OS)   Note: The evaluated configuration is on a Windows OS. See section 2.3 for more information.

Workstation users are only identified and authenticated by the OS on the user’s workstation.

6.1.5 Security management

SM-1 Management of Security Functions Behaviour (FMT_MOF.1-1)

The ITM Administrator is able to create and manage the following eTrust Antivirus policies:

- **Realtime Monitor -** Scans a file before it is accessed to ensure the file is not infected. Temporarily disables realtime scanning. The disable realtime option on the client suspends the activity of the Realtime Monitor, but does not remove it from memory or shut it down.
- **Scheduled Jobs -** Determines when and how scheduled scans occur.

The ITM Administrator is able to create and manage the following eTrust PestPatrol policies:

- **Active Protection -** Invokes continuous scanning of the client computer's memory and removes any active pests. Can also monitor and delete spyware cookies. Active Protection can be enabled or disabled by the "Enable=0/1" in the eaps.ini file.[29] "/stop" will disable any currently running pest scan operations.[30]
- **Scheduled Jobs -** Determines when and how scheduled scans occur.

SM-2 Management of Security Functions Behaviour (FMT_MOF.1-2)[31]

eAV has a web based GUI (eAV agent interface) which allows users to invoke real time scans on their own workstation. On Windows systems, an end user can access the Realtime Monitor settings on their workstation and manage the monitoring of files from the Realtime Monitor icon in the system tray. The policies that an administrator applies to a branch always take precedence over settings that an end user may have applied to his or her computer locally. If a user changes an assigned policy setting, the Threat Management Server detects the change and automatically returns the settings to those defined by the administrator, thereby enforcing the policy.

The following Realtime Monitor options are available to end-users:

- **Realtime Options -** Starts eTrust Threat Management Agent interface and displays the Settings tab, where an end-user can modify the realtime scan settings.
- **Disable Realtime -** Temporarily disables realtime scanning. This option suspends the activity of the Realtime Monitor, but does not remove it from memory or shut it down.
- **Monitor Outgoing Files -** Monitors files sent out from a local drive. Outgoing files are files being copied from a local drive and files that are executed from a local drive. Outgoing files are scanned when they are opened. If the file is infected, the end user is denied access to it.
- **Monitor Outgoing and Incoming Files -** Monitors both incoming files and outgoing files. Incoming files are files received by the local workstation. Incoming files are scanned only when they are closed.
- **Snooze -** Disable the Realtime Monitor for a specified number of minutes only.
- **Policy Job Delay Settings -** Lets the end user choose whether to run a policy update now or postpone it a specified number of hours.

[29] [ePP Admin] Appendix A, p. 98

[30] [ePP Admin] Appendix A, p. 90

[31] [eAV Admin] ch. 6, p. 50

- **Launch eTrust ITM -** Starts eTrust Threat Management Agent interface and displays the Scan tab.
- **Download Updates Now -** Opens the eTrust ITM Download Progress window, runs a content update for the local computer, and displays the progress of the update in the window.

SM-3 Management of TSF Data (FMT_MTD.1-1 and FMT_MTD.1-2)

The management of TSF data is done through the ITM Console. Both the ePP and eAV clients are managed by the ITM Console.

The Organization tree is a hierarchical representation of the devices on the target network. The tree is used to apply policies to groups of computers that require the same protection settings against malicious programs or code.

Using the Organization tab, an administrator can create an Organization tree with containers, called *branches*. These branches are typically organized to mirror the physical locations of computers on the target network. The organization of the tree is completely flexible and is often organized to segment computers into various categories by department, function, type of user, or any other arrangement that suits the business needs.

Using the User Management Tab:

Use the User Management tab to perform the following tasks:

- View current users and their permissions
- Add users and permissions
- Remove users and permissions
- Modify user permissions

The User Management tab lists current users in the Current Users area, and provides options for adding new users in the Add user area. In addition, an authorized user can delete existing users from the Current Users area by selecting a user and clicking Delete. To modify an existing user, select the checkbox next to the user's name, and click Edit.

Using the Organization Tab:

Use the Organization tab to perform the following tasks:

- Create branches and sub-branches
- View the computers contained in a branch
- View, assign and remove policies and scheduled jobs to or from branches and sub-branches
- View the users who have permissions for managing a branch or sub-branch
- Configure policy proxy servers and assign them to branches

Using the Discovery tab: [32]

Use the Discovery tab to perform the following subnet management tasks:

- Add (discover) a new subnet. The discovery process queries the subnet for clients running ITM Client.

[32] [ePP Admin] ch 4, p. 32-33

- Modify the configuration options of an existing subnet
- Delete one or more subnets
- Perform an immediate refresh of a subnet using the Discover Now option
- View product and organizational information for each computer on a subnet

Use the Discovery Configuration subtab to configure the policy settings for the subnet, the frequency the discovery is repeated, and the polling method used to perform the discovery.

Using the Policy Management tab:[33]

Policy Enforcement:

A policy contains the settings that will be applied to one or multiple computers to safeguard them against malicious programs or code. The Administrator can create and enforce policy settings and assign them to branches in the Organization tree to ensure that all computers are equally protected. There are separate policies applied to ePP and eAV. The separate policies are described below.

Policies that are applied to a branch always take precedence over settings that an end user may have applied to his or her computer locally. If a user changes an assigned policy setting, the Threat Management Server detects the change and automatically returns the settings to those defined by the administrator, thereby enforcing the policy.

When the Threat Management Server discovers a new subnet, or refreshes its database of existing subnets, it receives information on all policies for each client, along with the product version, signature information, and operating system information, such as the computer name, IP address, OS version and MAC address. The Threat Management Server updates its database and examines the information. If it finds that a policy setting on the client computer does not match the policy setting assigned to the branch the computer resides in, it flags the discrepancy and resets the policy.

Note: The policy settings on the client machine can be locked so that the end-user is prevented from changing the policy settings.

Use the Policy Management tab to create and manage the following **eTrust PestPatrol** policies:

ePP Policy Settings[34]:

- **Active Protection -** Invokes continuous scanning of the client computer's memory and removes any active pests. Can also monitor and delete spyware cookies.
- **Scheduled Jobs -** Specifies the time, date, and interval for the scan, and CPU usage level. Specifies the objects to scan and the action to perform on detected pests. Specifies directories to scan.
- **Quarantine Restore Jobs -** Restores quarantined pests based on a target restore date.
- **Pests Exclusions -** Specifies the files, applications, spyware, and pests to ignore during a scan.
- **Alert Forwarding -** Specifies where to send notification information and how frequently to send it. Lets the administrator manage notification severity levels, customize sets of notification messages to be reported for different service components, and determine the types of messages that should be passed to the Alert Manager.

[33] [ePP Admin] ch 6, p. 41

[34] [ePP Admin] ch 6, p. 43

eAV Policy Settings:

Use the Policy Management tab to create and manage the following **eTrust Antivirus** policies:

- **Realtime Monitor** - The Realtime Monitor automatically invokes a file scan each time a file is executed, written to, or opened. When an infection is found and a treatment action is unsuccessful, file access is denied, which prevents the infection being spread further. On Windows systems, the interception is accomplished by using a VxD (Virtual Device Driver). The Realtime Monitor has options available to the end-user.
- **Scheduled Jobs -** Determines when and how scheduled scans occur.
- **Content Update -** Specifies how and when software updates and signature files will be downloaded to clients.
- **Alert Forwarding -** Specifies where to send notification information and how frequently to send it. Lets the administrator manage notification severity levels, customize sets of notification messages to be reported for different service components, and determine the types of messages that should be passed to the Alert Manager.

Manual scan on workstation

The ITM Client restricts the ability to modify the directories and files that will be scanned manually on the ITM Client workstations to the Administrator and Workstation Users.

Viewing Client Audit logs[35]

Use the Logs subtab under the Clients tab to view the logs for a specific computer. An administrator can locate the computer whose logs will be viewed by entering the name of the computer in the Node Name field and clicking Find. Once the client is found, click the Logs subtab and select the type of log to be viewed from the drop-down list. See SA-2 for more information regarding viewing client logs.

For each client computer under the client tab in the ITM console, the administrator can determine whether they want to save all logs or delete them after a certain number of days. [36]

Using the Alert Manager[37]

ITM allows an administrator to create customized alerts for multiple computers which reduces message traffic and minimizes the dissemination of notifications that are not critical.

An Administrator can customize alert policies for different systems and their uses. A policy for a workstation may be configured differently than one for a server, and another may be configured for the Threat Management Server, based on the roles each of these device types. An Administrator can send critical, warning, and informational alerts.

Additionally, an administrator should establish an alert policy to send realtime alerts to the Alert Manager for handling. By default, each connected client will get a notification message when malicious code is found, even though only one of the clients triggered the alert. To minimize confusion, it is good practice to disable the Realtime Pop-up Messages option on the Advanced subtab in the Realtime Monitor policy and instead have the realtime alerts sent to the Alert Manager for handling. This ensures that the alerts will be directed to the right location where they can be handled most efficiently

[35] [eAV Admin Guide] ch 7, p.72

[36] [eAV Admin Guide] ch 7, p.74

[37] [ePP Admin Guide] ch 11, p.79

The Report To options found under the Alert subtab define where the alert messages should be sent. Alerts will be sent based on the configuration of the Alert Manager. Choosing Local Alert Manager requires that the Alert Manager is installed locally on the desktop or server. Choosing Event Log lets an Administrator use the Windows Event Logs to review the alerts. On the server running the Alert Manager, an Administrator must have a policy in place to send all received alerts to the Local Alert Manager.

There are two basic components to the Alert Manager: the Alert Manager service, which is responsible for the reception, processing, and distribution of Alert messages, and the Alert Manager interface, where an Administrator can configure how Alert should send its messages. [38]

Alert Filter Subtab

The Alert Filter subtab offers an Administrator the option of receiving all informational, warning, and/or critical alert messages generated. Alternately, an Administrator can select specific alerts in the custom notification options. By selecting only those alerts that are required, excessive and unnecessary alerts are reduced.

SM-4 Specification of Management Functions (FMT_SMF.1)

ITM is capable of performing the following security management functions:

- Determine the behavior of, disable, and enable the behavior of the functions: real time and scheduled malware scanning (see SM-1),
- Modify the behaviour of the function: manually invoked malware scanning (see SM-2),
- The operations as specified in Table 5-4 (See SM-3).

SM-5 Security roles (FMT_SMR.1)

The TOE maintains the roles of Administrator and Workstation User.

6.1.6 Partial Protection of the TSF

TP-1 TSF domain separation (FPT_SEP_EXP.1-1)

The ITM Console is a web based interface. IT maintains individual sessions associated with administrators. The TSF maintains a session ID as part of a session to prevent interference between administrator actions.

The administrator sessions are not locked. If two different administrators are making changes at the same time, this is allowed. ITM enforces the last configuration changes saved by any session.

The TSF when invoked by the underlying host OS maintains a security domain that protects it from interference and tampering by untrusted subjects in the TOE's Scope of Control.

The ITM Server and client hosts are passive devices in that they indirectly connect to networks via other devices' e.g. network interface. The ITM Server and client's protected domain includes the ITM Server and client software.

In addition to the ITM Server and client - specific software, other software files such as configuration files are also stored on disk. The ITM Server and client relies partially on the Operating System to provide file access permissions at the OS level. In addition, the ITM Server and client relies on the OS for file process separation. These files can be modified by an authorized user accessing them through the ITM Console. Access Permissions are enforced to provide protection from unauthorized

[38] [eAV Admin] ch 1, p.11

users accessing these files. The underlying assumption regarding the operation of the ITM Server and client is that they are maintained in a physically secure environment.

6.1.7 SOF Claims

The threat level for the TOE authentication function is assumed to be SOF-basic. This defines a level of authentication strength of function where analysis shows that the function provides basic protection against straightforward or intentional breach of TOE security by attackers possessing a minimum attack potential.

IA-2 Identification and authentication, is realized by probabilistic or permutational mechanisms.   The methods used to provide difficult-to-guess passwords are probabilistic. The specific password policy is specified in the ITM Common Criteria Supplement to the Administration Guide V1.0 as the following:

- Minimum length of 8,
- At least one special character,
- At least one numeric character,
- At least one uppercase and one lowercase character
- 30 day expiration date
- Must not be a common word, a word in any existing password dictionaries, or a word easily guessed (such as “password”).

The SOF claim for IA-2 is SOF-basic.

6.2 *Assurance Measures*

The TOE satisfies the assurance requirements for EAL3. The following items are provided as evaluation evidence to satisfy the EAL3 assurance requirements.

Table 6-3 Assurance Measures and How Satisfied

Component	Evidence Requirements	How Satisfied	Rationale
ACM_CAP.3	CM Documentation • CM Plan • Configuration Item List • CM Usage Evidence	• CA eTrust VSS_CM_Plan-V0.1Draft_ 2006-08-30	• CM Proof - Shows the CM system is being used.
ACM_SCP.1	TOE CM Coverage	• Configuration Item List	• Configuration Item List(s) • is comprised of a list of the source code files and version numbers • is comprised of a list of design documents with version numbers • is comprised of test documents with version numbers • user and administrator documentation with version numbers
ADO_DEL.1	Delivery Procedures	Distribution_Centers_Procedures_Manual-NorthAmerica-2004Mar01.doc (DCPM) Preservation of Product (1Apr2004)	Provides a description of all procedures that are necessary to maintain security when distributing TOE software to the user's site. - Applicable across all phases of delivery from packaging, storage, and distribution
ADO_IGS.1	Installation, generation, and start-up procedures	• eTrust Antivirus Implementation Guide r8 • eTrust PestPatrol Implementation Guide r8 • Common Criteria Supplement to the Computer Associates Integrated Threat Management Administrator Guide V1.0	Provides detailed instructions on how to install and configure TOE.

Component	Evidence Requirements	How Satisfied	Rationale
ADV_FSP.1	Functional Specification	• ITM r8 EAL3 Common Criteria Proprietary Development Specification V0.3	Provides rationale that TSF is fully represented Describes the TSF interfaces and TOE functionality
ADV_HLD.2	Security Enforcing High-Level Design	• ITM r8 EAL3 Common Criteria Proprietary Development Specification V0.3	Describes the TOE in terms of subsystems and their associated security functionality
ADV_RCR.1	Representation Correspondence	• ITM r8 EAL3 Common Criteria Proprietary Development Specification V0.3	Provides the following two dimensional mappings: 1. TSS and functional specification; 2. functional specification and high-level design.
AGD_ADM.1	Administrator Guidance	• eTrust Antivirus Administration Guide r8 • eTrust PestPatrol Administration Guide r8 • Common Criteria Supplement to the Computer Associates Integrated Threat Management Administrator Guide V1.1	Describes how to administer the TOE securely.
AGD_USR.1	User Guidance	• eTrust Antivirus Administration Guide r8 • eTrust PestPatrol Administration Guide r8 • Common Criteria Supplement to the Computer Associates Integrated Threat Management Administrator Guide V1.1	Describes how to administer the TOE securely.
ALC_DVS.1	Identification of Security Measures	• CA_Development Security Procedures Manual_(2006-07-11)	Describes the physical, procedural, personnel, other security measures that may be used to protect the TOE.
ATE_COV.2	Analysis of Coverage	• CA ITM Test Coverage Analysis-15 Jan 2007	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE.DPT.1	Testing: High-Level Design	• ITM r8 EAL3 Common Criteria Proprietary Development Specification V0.3	Shows the depth or level of detail at which the TSF is tested.

Component	Evidence Requirements	How Satisfied	Rationale
ATE_FUN.1	Test Documentation	• Various test procedures were provided which can be traced to each security function in section 6 of the ST. There are too many test procedures to list here. See AM evidence for ATE_IND.2	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_IND.2	TOE for Testing	• ITM r8 (TOE for Testing) • ITM Test Plan and Report v0.2	Test documentation includes test plans and procedures and expected and actual results.
AVA_MSU.1	Examination of Guidance	• eTrust Antivirus Administration Guide r8 • eTrust PestPatrol Administration Guide r8 • eTrust Antivirus Implementation Guide r8 • eTrust PestPatrol Implementation Guide r8 • Security Target • ITM r8 EAL3 Common Criteria Proprietary Development Specification • ITM Test Plan and Report	Provides an analysis if the TOE can be used in amanner which is insecure, but the administrator believes to be secure.
AVA_SOF.1	SOF Analysis	• Integrated Threat Management r8.0 Strength of Function Analysis, Version 0.1	The TOE will be provided for testing.
AVA_VLA.1	Vulnerability Analysis	• Integrated Threat Management r8.0 Vulnerability Analysis, Version 0.1	Provides an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

7 PP Claims

This ST was not written to address any existing Protection Profile.Rationale

8 Rationale

8.1 Security Objectives Rationale

8.1.1 Assumptions

Table 8-1 shows that all of the assumptions are addressed by Non-IT security objectives. Rationale is provided for each Assumption in the table.

Table 8-1 All Assumptions Addressed

Item	Assumption ID	Non-IT Objective Addressing Assumption	Rationale
1.	A.AuditBackup	ON.AuditBackup	This objective provides for the backing up of audit files and makes sure that disk usage is monitored.
2.	A.NoEvil	ON.Person	This objective provides for competent personnel to administer the TOE.
		ON.Install	This objective ensures the TOE is delivered, installed, managed, and operated by competent individuals.
3.	A.NoUntrusted	ON.NoUntrusted	This objective provides for the protection of the TOE from untrusted software and users.
4.	A.Physical	ON.Physical	This objective provides for the physical protection of the TOE software.
5.	A.Users	ON.ProtectAuth	This objective provides for users protecting their authentication data.
6.	A.SecureUpdates	ON.SecureUpdates	This objective provides for the secure receipt and validation of updated signature files from Anti-Malware vendors.

8.1.2 Threats to Security

Table 8-2 shows that all the identified threats to security are countered by Security Objectives for the TOE and IT Environment. Rationale is provided for each threat in the table.

Table 8-2 All Threats to Security Countered

Item	Threat ID	Security Objective Addressing the Threat	Rationale
1	T.AdminError	O.AdminRole	This objective plays a role in mitigating this threat by limiting the functions an administrator can perform in a given role.
		O.Manage	This objective also contributes to mitigating this threat by providing management tools to make it easier for administrators to manage the TOE security functions. More specifically, providing administrators the capability to view configuration settings within a GUI.
		OE.Manage	This objective also contributes to mitigating this threat by providing the root user on Unix and the Administrator on Windows to have full control of the ITM Console.

Item	Threat ID	Security Objective Addressing the Threat	Rationale
2	T.AuditCompromise	O.AuditProtection	O.AuditProtection contributes to mitigating this threat by controlling access to the individual audit log records. No one is allowed to modify audit records, the Administrator is the only one allowed to delete audit records from the ITM Server.
		OE.AuditStorage	OE.AuditStorage contributes to mitigating this threat by restricting the ability of users in the IT Environment to access the audit log file.
		O.PartialSelfProtection	O.PartialSelfProtection 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.PartialSelfProtection	OE.PartialSelfProtection 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 mitigation of this threat.
3	T.Masquerade	O.RobustTOEAccess	This objective mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how authorized administrators and workstation users can access the TOE, and by mandating the type and strength of the authentication mechanisms, this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective allows the TOE to correctly interpret information used during the authentication process so that it can make the correct decisions when identifying and authenticating users.
		OE.TOEAccess	OE.TOEAccess 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.

Item	Threat ID	Security Objective Addressing the Threat	Rationale
4	T.MaliciousTSFCompromise	O.PartialSelfProtection	O.PartialSelfProtection is necessary so that the TSF protects itself and its resources from inappropriate access through its own interfaces.
		OE.PartialSelfProtection	OE.PartialSelfProtection is necessary so that the TSF is protected from other processes executing on the workstation.
		O.Manage	O.Manage provides the capability to restrict access to the TSF to those that are authorized to use the functions. Satisfaction of this objective (and its associated requirements) prevents unauthorized access to TSF functions and data through the ITM Console
5	T.Malware	O.DataScan	O.DataScan mitigates this threat by providing a mechanism that discovers devices on the target network. As a result, ITM will know when a new workstation that does not have the ITM client installed on it is added to the target network.
		O.Malware	O.Malware mitigates this threat by providing mechanisms to prevent malware from being introduced onto a workstation.
		OE.Malware	OE.Malware mitigates this threat by providing mechanisms to prevent malware from being introduced onto a workstation.
6	T.RemoteTransmit	OE.RemoteSecureComms	OE.RemoteSecureComms mitigates this threat by the IT Environment providing a secure line of communication between the TOE and remote trusted IT products.
7	T.Transmit	OE.SecureComms	OE.SecureComms mitigates this threat by the IT Environment providing a secure line of communication between distributed portions of the TOE and between the TOE and remote administrators.
8	T.UnidentifiedActions	O.AuditReview	O.AuditReview helps to mitigate this threat by providing the 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. failed logins, self-test failures, etc.).
		O.AuditGeneration	O.AuditGeneration helps to mitigate this threat by recording actions for later review.
		OE.TimeStamps	OE.TimeStamps helps to mitigate this threat by ensuring that audit records have correct timestamps.

8.1.3 Organizational Security Policies

Table 8-3 shows that all the identified organizational security policies are covered by Security Objectives for the TOE and IT Environment. Rationale is provided for each OSP in the table.

Table 8-3 All Organizational Security Policies are addressed

Item	OSP ID	Security Objective Addressing Policy	Rationale
1.	P.Accountability	O.AuditGeneration	This objective addresses this policy by providing an audit mechanism to record the actions of a specific user. Additionally the administrator's user name is recorded when any security relevant change is made to the TOE (ex. Access rule modification or start/stop of the audit function).
		OE.TimeStamps	This objective plays a role in supporting this policy by requiring the IT Environment to provide reliable time stamps. The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user name will also include the date and time that the event occurred.
		O.RobustTOEAccess	This objective supports this policy by requiring the TOE to identify and authenticate all authorized users prior to allowing any TOE access or any TOE mediated access on behalf of those users.
		OE.TOEAccess	OE.TOEAccess supports this policy by requiring the IT environment to identify and authenticate all authorized administrators and workstation users prior to allowing any TOE access.
2.	P.ManualScan	O.Manage	O.Manage provides the workstation user with the ability to invoke the manual scan capability
		O.Malware	O.Malware requires the TOE to provide the capability to invoke manual scans of removable media.

Table 8-4 Reverse Mapping of Security Objectives to Threats/Policies

Note: This table is provided to show completeness by demonstrating all security objectives for the TOE map to at least one threat.

Item	TOE Objective	Threat/Policy
1.	O.AdminRole	T.Admin_Error
2.	O.AuditGeneration	P.Accountability T.UnidentifiedActions
3.	O.AuditReview	T.UnidentifiedActions
4.	O.AuditProtection	T.AuditCompromise
5.	O.DataScan	T.Malware
6.	O.Manage	T.AdminError T.MaliciousTSFCompromise P.ManualScan
7.	O.PartialSelfProtection	T.MaliciousTSFCompromise T.AuditCompromise
8.	O.RobustTOEAccess	T.Masquerade P.Accountability
9.	O.Malware	T.Malware

Table 8-5 Reverse Mapping of Security Objectives for the Environment to Assumptions/Threats/Policies

Note: This table is provided to show completeness by demonstrating all security objectives for the environment map to at least one assumption, threat, or policy.

Item	Security Objective for Environment	Assumption/Threat/Policy
10	OE.AuditStorage	T.AuditCompromise
11	OE.Malware	T.Malware
12	OE.Manage	T.AdminError
13	OE.PartialSelfProtection	T.AuditCompromise T.MaliciousTSFCompromise
14	OE.RemoteSecureComms	T.RemoteTransmit
15	OE.SecureComms	T.Transmit
16	OE.TimeStamps	P.Accountability T.UnidentifiedActions
17	OE.TOEAccess	T.Masquerade P.Accountability
18	ON.AuditBackup	A.AuditBackup
19	ON.Install	A.NoEvil
20	ON.NoUntrusted	A.NoUntrusted
21	ON.Person	A.NoEvil
22	ON.Physical	A.Physical
23	ON.ProtectAuth	A.Users
24	ON.SecureUpdates	A.SecureUpdates

8.2 Security Requirements Rationale

8.2.1 Functional Requirements

Table 8-6 shows that all of the security objectives of the TOE are satisfied. Rationale for each objective is included in the below table.

Table 8-6 All Objectives Met by Functional Requirements

Item	Objective ID	SFR ID	SFR Title	Rationale
1.	O.AdminRole	FMT_SMR.1	Security roles	FMT_SMR.1 requires that the TSF maintain multiple roles. The TSF is able to associate a human user with one or more roles and these roles isolate administrative functions in that the functions of these roles do not overlap. If a security administrator were to perform a malicious action, the auditing requirements afford some measure of detectability of the rogue administrator’s actions.

Item	Objective ID	SFR ID	SFR Title	Rationale
2.	O.AuditGeneration	FAU_GEN.1	Audit data generation	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that an administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. There is a minimum of information that must be present in every audit record and this requirement defines that, as well as the additional information that must be recorded for each auditable event.
3.	O.AuditReview	FAU_SAR_EXP.1	Audit review	FAU_SAR_EXP.1 provides the ability to review the audits in a user-friendly manner.
4.	O.AuditProtection	FAU_STG_EXP.1-1	Protected Audit Trail Storage	The FAU_STG family dictates how the audit trail is protected. FAU_STG_EXP.1-1 restricts the ability to delete audit records to the Administrator through the ITM Console on the ITM Server. This requirement also ensures that no one has the ability to modify audit records through the ITM Console (e.g., edit any of the information contained in an audit record). This ensures the integrity of the audit trail is maintained.
5.	O.DataScan	FAM_SDC_EXP.1	Discovery data collection	FAM_SDC_EXP.1 requires that the TSF collect discovery data from the devices on the target network. ITM does a compare to the devices it already knows about to see what new devices are on the network.

Item	Objective ID	SFR ID	SFR Title	Rationale
6.	O.Manage	FAM_DRS_EXP.1	Data reporting	FAM_DRS_EXP.1 requires the TSF to be able to provide automatically generated reports of the system data.
		FMT_MOF.1*	Management of security functions behaviour	Restricted privileges are defined for the Administrator and Workstation Users. FMT_MOF.1 defines particular TOE capabilities that may only be used by these users.
		FMT_MTD.1-1	Management of TSF data	The FMT requirements are used to satisfy this management objective, as well as other objectives that specify the control of functionality. The requirement's rationale for this objective focuses on the administrator's capability to perform management functions in order to control the behavior of security functions. FMT_MTD.1-1 specifies the management of TSF Data according to assigned roles. It defines what specific operations on TSF Data that Administrators, and workstation users are allowed to perform.
		FMT_SMF.1	Specification of management functions	FMT_SMF.1 requires the TSF be capable of performing the specified security management functions.
7.	O.PartialSelfProtection	FPT_SEP_EXP.1-1	TSF domain separation	FPT_SEP_EXP.1 was chosen to ensure the TSF provides a domain that protects itself from untrusted users. If the TSF cannot protect itself it cannot be relied upon to enforce its security policies. The explicitly specified version was used to distinguish the aspects of FPT_SEP provided by the TOE vs. the aspects provided by the IT environment.

Item	Objective ID	SFR ID	SFR Title	Rationale
8.	O.RobustTOEAccess	FIA_ATD.1*	User attribute definition	FIA_ATD.1 defines the attributes of users, including a user name that is used by the TOE to determine a user's identity and enforce what type of access the user has to the TOE. The TOE associates an administrator user with access permissions. The access permissions. They can be granted different levels of permissions within the eTrust Threat Management Console; from full access to all features of the eTrust Threat Management Console, to read-only access. The workstation user does not have any attributes held by the TOE as their access is not separated by any specific roles on the workstation machines.
		FIA_UAU_EXP.2 -1	User authentication before any action	FIA_UAU_EXP.2 -1 requires that administrators and other users authenticate themselves to the TOE before performing administrative duties.
		FIA_UID_EXP.2 -1	User identification before any action	FIA_UID.2 -1 plays a small role in satisfying this objective by ensuring that every user is identified before the TOE performs any mediated functions.
9.	O.Malware	FAM_SCN_EXP.1-1	Anti-Malware Scanning	FAM_SCN_EXP.1-1 requires that the TOE invoke a scan for malware.
		FAM_ACT_EXP.1	Anti-Malware Actions	FAM_ACT_EXP.1 requires that the TOE take action against malware once it is detected.
		FAM_ALR_EXP.1	Anti-Malware Alerts	FAM_ALR_EXP.1 defines alerting requirements to ensure the users are aware that a malware was detected

Table 8-7 Reverse mapping of TOE SFRs to TOE Security Objectives

Note: This table has been provided for completeness to show that all security functional requirements map to at least one TOE Security Objective.

Item	SFR ID	TOE Security Objective
1	FAU_GEN.1	O.AuditGeneration
2	FAU_SAR_EXP.1	O.AuditReview
4	FAU_STG_EXP.1-1	O.AuditProtection
5	FAM_SDC_EXP.1	O.DataScan
6	FAM_SCN_EXP.1-1	O.Malware
7	FAM_ACT_EXP.1	O.Malware
8	FAM_ALR_EXP.1	O.Malware
9	FAM_DRS_EXP.1	O.Manage
10	FIA_ATD.1*	O.RobustTOEAccess

Item	SFR ID	TOE Security Objective
11	FIA_UAU_EXP.2-1	O.RobustTOEAccess
12	FIA_UID_EXP.2-1	O.RobustTOEAccess
13	FMT_MOF.1*	O.Manage
14	FMT_MTD.1-1	O.Manage
15	FMT_SMF.1	O.Manage
16	FMT_SMR.1	O.AdminRole
17	FPT_SEP_EXP.1-1	O.PartialSelfProtection

8.2.2 Dependencies

Table 8-8 shows the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference. If the TOE dependency is met by an SFR in the IT environment an (E) will be next to the reference number.

Table 8-8 TOE Dependencies Satisfied

Item	SFR ID	SFR Title	Dependencies	Item Reference
1.	FAU_GEN.1	Audit data generation	FPT_STM.1	24(E)
2.	FAU_SAR_EXP.1	Audit review	FAU_GEN.1	1
3.	FAU_STG_EXP.1-1	Protected audit trail storage	FAU_GEN.1	1
4.	FAM_SDC_EXP.1	Discovery data collection	FMT_SMR.1	15
			FAU_GEN.1	1
5.	FAM_SCN_EXP.1-1	Anti-Malware scanning	FMT_SMR.1	15
6.	FAM_ACT_EXP.1	Anti-Malware actions	FAM_SCN_EXP.1-1	5
			FMT_SMR.1	15
7.	FAM_ALR_EXP.1	Anti-Malware alerts	FAM_SCN_EXP.1-1	5
			FMT_SMR.1	15
8.	FAM_DRS_EXP.1	Data reporting	FAM_SDC_EXP.1	5
			FMT_SMR.1	15
9.	FIA_ATD.1*	User attribute definition	None	None
10.	FIA_UAU_EXP.2 -1	User authentication before any action	FIA_UID.1	11 (H)
11.	FIA_UID_EXP.2 -1	User identification before any action	None	None
12.	FMT_MOF.1*	Management of security functions behaviour	FMT_SMF.1	14
			FMT_SMR.1	15
13.	FMT_MTD.1-1	Management of TSF data	FMT_SMF.1	14
			FMT_SMR.1	15
14.	FMT_SMF.1	Specification of management functions	None	None
15.	FMT_SMR.1	Security roles	FIA_UID.1	11 (H)
16.	FPT_SEP_EXP.1-1	TSF domain separation	None	None

Table 8-9 IT Environment Dependencies are Satisfied

Item	SFR ID	SFR Title	Dependencies	Reference
17.	FAM_SCN_EXP.1-2	Anti-Malware scanning	FMT_SMR.1	15
18.	FAU_STG_EXP.1-2	Protected Audit Trail Storage	FAU_GEN.1	1

Item	SFR ID	SFR Title	Dependencies	Reference
19.	FIA_UAU_EXP.2 -2	User authentication before any action	FIA_UID.1	11 (H)
20.	FIA_UID_EXP.2 -2	User identification before any action	None	None
21.	FMT_MTD.1-2	Management of TSF data	FMT_SMF.1	14
			FMT_SMR.1	15
22.	FPT_ITT.1	Basic Internal TSF Data Transfer Protection	None	None
23.	FPT_RVM.1	Non-Bypassability of the TSP	None	None
24.	FPT_SEP_EXP.1-2	TSF domain separation	None	None
25.	FPT_STM.1	Reliable time stamps	None	None
26.	FTP_ITC.1	Inter-TSF trusted channel	None	None

8.2.3 Strength of Function Rationale

A strength of function level of SOF-basic counters an attack level of low. The environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product. As stated in section 6.1.7, there is one security function based on probabilistic methods, IA-2. See section 5.3.4 for the objective that SOF supports. The specific "strength" required of the methods used to provide difficult-to-guess passwords are defined administratively in the CC Supplement to the Administration Guide.

8.2.4 Assurance Rationale

Evaluation Assurance Level (EAL) 3 was chosen because it provides appropriate assurance measures for the expected application of the product. EAL3 was selected because the TOE requires a moderate level of independently assured security and requires a thorough investigation of the TOE and its development without substantial re-engineering.

8.2.5 Requirements for the IT Environment

Table 8-10 shows that all of the security objectives for the IT environment are satisfied. Rationale for each objective is included in the below table.

Table 8-10 All Objectives for the IT Environment map to Requirements in the IT environment

Item	Objective	Env SFR ID	SFR Title	Rationale
10	OE.AuditStorage	FAU_STG_EXP.1-2	Protected Audit Trail Storage	FAU_STG_EXP.1-2 requires the Operating System to protect the audit log file from unauthorized deletion.
11	OE.Malware	FAM_SCN_EXP.1-2	Anti-Malware scanning	FAM_SCN_EXP.1-2 requires the scanning engine which is in the IT Environment to scan the client computer for malware.
12	OE.Manage	FMT_MTD.1-2	Management of TSF data	FMT_MTD.1-2 requires the Operating System to provide the root user on Unix and the Windows Administrator on Windows Operating Systems to be able to manage the TOE.
13	OE.PartialSelfProtection	FPT_RVM.1	Non-Bypassability of the TSP	FPT_RVM_EXP.1-1 requires the Operating System's security policy enforcement functions are invoked and succeed before a security-relevant function is allowed to proceed.
		FPT_SEP_EXP.1-2	TSF domain separation	FPT_SEP_EXP.1-1 requires the Operating System to maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface. The IT environment must enforce separation between security domains of subjects in the Operating System's Scope of Control.
14	OE.RemoteSecureComms	FTP_ITC.1	Inter-TSF trusted channel	FTP_ITC.1 ensures that secure communication between the ITM Server and remote trusted IT products will be available to the TOE.
15	OE.SecureComms	FPT_ITT.1	Basic Internal TSF Data Transfer Protection	FPT_ITT.1 ensures that secure communication between the ITM Server and the workstations will be available to the TOE.
16	OE.TimeStamps	FPT_STM.1	Reliable time stamps	FPT_STM.1 requires that time stamps be provided by the IT environment.

Item	Objective	Env SFR ID	SFR Title	Rationale
17	OE.TOEAccess	FIA_UAU_EXP.2-2	User authentication before any action	FIA_UAU.2 requires that a user be authenticated by the TOE before accessing the TOE.
		FIA_UID_EXP.2-2	User identification before any action	FIA_UID.2 requires that a user be identified to the TOE in order to access to the TOE.

Table 8-11 Reverse Mapping of Environment SFRs to Environment Security Objectives

Note: This table has been provided for completeness to show that all security functional requirements for the IT Environment map to at least one Security Objective for the IT Environment.

Item	Environment SFR ID	Environment Security Objectives
17	FAM_SCN_EXP.1-2	OE.Malware
18	FAU_STG_EXP.1-2	OE.AuditStorage
19	FIA_UAU_EXP.2 -2	OE.TOEAccess
20	FIA_UID_EXP.2 -2	OE.TOEAccess
21	FMT_MTD.1-2	OE.Manage
22	FPT_ITT.1	OE.SecureComms
23	FPT_RVM.1	OE.PartialSelfProtection
24	FPT_SEP_EXP.1-2	OE.PartialSelfProtection
25	FPT_STM.1	OE.TimeStamps
26	FTP_ITC.1	OE.RemoteSecureComms

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-12 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-12 Mapping of Functional Requirements to TOE Summary Specification

Item	SFR ID	SFR Title	Requirement is met by:	
			Security Function Ref. No	Rationale
1	FAU_GEN.1	Audit data generation	SA-1	Specifies the types of events to be audited, and the information to be recorded in an audit record.
2	FAU_SAR_EXP.1	Audit review	SA-2	Specifies that the review of the audit logs on the ITM Client is restricted to the authorized administrator and workstation user.

Item	SFR ID	SFR Title	Requirement is met by:	
			Security Function Ref. No	Rationale
3	FAU_STG_EXP.1-1	Protected audit trail storage	SA-3	Specifies that the TOE protects the stored audit records from unauthorized deletion and modification via the ITM console.
4	FAM_SDC_EXP.1	Discovery data collection	AM-1	Specifies the TSF is able to collect system data from the devices on the target network.
5	FAM_SCN_EXP.1-1	Anti-Malware scanning	AM-2	Speciifes the anti-malware scans that the ITM Client is able to invoke.
6	FAM_ACT_EXP.1	Anti-Malware actions	AM-3	Specifies the actions the ITM Client will take based on the detection of a malware.
7	FAM_ALR_EXP.1	Anti-Malware alerts	AM-4	Specifies the alerts that are sent when a malware is detected.
8	FAM_DRS_EXP.1	Data reporting	AM-5	Specifies the reports that can be generated by the TSF.
9	FIA_ATD.1*	User attribute definition	IA-1	Specifies the security attributes maintained for each user.
10	FIA_UAU_EXP.2 -1	User authentication before any action	IA-2	Specifies that each user must be successfully authenticated with a password before being allowed any other actions.
11	FIA_UID_EXP.2 -1	User identification before any action	IA-2	Specifies that each user must identify himself/herself before being allowed to perform any other actions.
12a	FMT_MOF.1 -1	Management of Security Functions Behaviour	SM-1	Specifies the management of functions that are restricted by the TOE to the authorized administrator
12b	FMT_MOF.1 -2	Management of Security Functions Behaviour	SM-2	Specifies the management of functions that are restricted by the TOE to the authorized workstation user.
13	FMT_MTD.1-1	Management of TSF data	SM-3	Specifies that the ITM Server restricts the ability to access TSF data to the authorized administrator. The Workstation User has limited access to manage TSF data on the ITM Client workstation.
14	FMT_SMF.1	Specification of management functions	SM-4	Specifies the security management functions provided by the ITM Server and client.
15	FMT_SMR.1	Security roles	SM-5	Specifies the roles maintained in the ITM Server and client.
16	FPT_SEP_EXP.1-1	TSF domain separation	TP-1	Specifies that the ITM Server and client maintains a security domain for its own execution and enforces separation between security domains of users.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.

8.5 Explicitly Stated Requirements Rationale

FAM_SDC_EXP.1, FAM_SCN_EXP.1*, FAM_ACT_EXP.1, FAM_ALR_EXP.1, and FAM_DRS_EXP.1 had to be explicitly stated because there are no SFRs in the CC that describe the anti-malware security functionality covering the collection of system data, invoking the scanning for malware, taking action when a malware is detected, sending alerts, and providing reports of system data.

FIA_UAU_EXP.2* and FIA_UID_EXP.2* had to be explicitly stated because these SFRs span both the TOE SFRs and IT Environment SFRs. Although the TOE has its own identification and authentication, it also relies on the IT Environment (Operating System) identification and authentication mechanisms.

According to CC Part 1 v2.3 section A.2.6, paragraph 211 states the following: "Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. "

FPT_SEP_EXP.1* had to be explicitly stated because it provides partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection. Since the iteration of FPT_SEP_EXP.1 spans both the TOE requirements and IT Environment, it must be explicitly stated.

FAU_SAR_EXP.1 had to be explicitly stated because it narrows the scope of the original SFR, by stating "on the workstation being used".

FAU_STG_EXP.1* had to be explicitly stated because it narrows the scope of the original SFR by stating "via the TSFI". The above CCIMB RI#19 also applies to FAU_STG_EXP.1. The protection of the audit records relies on the OS and hardware platforms for full protection.