National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

CA

Integrated Threat Management™ r8.0

Report Number:	CCEVS-VR-07-0038
Dated:	June 10, 2007
Version	1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899
20755-6740

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD

ACKNOWLEDGEMENTS

Validation Team

Bradford O'Neill, Jim Brosey

Common Criteria Testing Laboratory

Clifton Morgan

CygnaCom Solutions (an Entrust Company)
McLean, VA

Table of Contents

1 EXECUTIVE SUMMARY

The evaluation of the CA, Inc. product **Integrated Threat Management™ r8.0** was performed by CygnaCom Solutions (an Entrust Company) in the United States and was completed on 28 February 2007. The evaluation was conducted in accordance with the requirements of the Common Criteria, version 2.3, Part 2 and Part 3, Evaluation Assurance Level (EAL 3), and the Common Methodology for IT Security Evaluation (CEM), Version 2.3.

CygnaCom Solutions is certified by the NIAP validation body for laboratory accreditation. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced. The CygnaCom Security Evaluation Laboratory team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL3) have been met. This Validation Report is not an endorsement of the CA, Inc product by any agency of the U.S. Government and no warranty of the product is either expressed or implied. The technical information included in this report was obtained from the Evaluation Technical Report (ETR) produced by CygnaCom Solutions.

The Target of Evaluation (TOE) is the CA product **Integrated Threat Management™ r8.0** software product. There is no difference between the TOE and the CA ITM product. The TOE consists of the following software components:

- ITM Server r8 which includes the java based interfaces (ITM Console, Alert Manager)
- *eTrust* Pest Patrol r8
- *eTrust* AntiVirus r8

The Integrated Threat Management product components not in the TOE are:

- *e*Trust Pest Patrol Scan Engine
- VET Engine
- InoculateIT Engine
- Underlying operating system (OS) software and hardware
- SSL implementation (not tested).

Integrated Threat Management provides:

- Anti-virus protection for devices on enterprise networks (*e*AV*).*
- Detection and elimination of both file and memory based viruses such as worms and Trojan horses on enterprise based networks (*e*AV).

- Detection and elimination of Trojan horses, keyloggers, distributed denial-of-service attack agents, adware, spyware and hijacker tools on Windows based networks. (*e*PP).
- Provides centralized management capabilities for both *e*AV and *e*PP through the ITM console.

The TOE relies on the IT environment to provide:

- Anti-Malware scanning
- Protected audit trail storage
- User authentication before any action
- User identification before any action
- Management of TSF data
- Basic internal TSF data transfer protection
- Non-Bypassability of the TSP
- TSF domain separation
- Reliable time stamps
- Inter-TSF trusted channel

1.1 EVALUATION DETAILS

Evaluated Product: Integrated Threat Management™ r8.0

Developer: CA, Inc., One Computer Associates Plaza, Islandia, NY 11749

CCTL: CygnaCom Solutions, 7925 Jones Branch Dr., Suite 5200 West, McLean, VA 22102-3321.

Validation Team: Bradford O'Neill, Jim Brosey

EAL: EAL3

Completion Date: 28 February 2007.

1.2 INTERPRETATIONS

The evaluation team performed an analysis of the international and national (NIAP) interpretations regarding the CC and the CEM and determined that none were applicable to this evaluation:

1.3 THREATS TO SECURITY

The Security Target identified the following threats that the evaluated product addresses:

T.AdminError	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
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.
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.
T.MaliciousTSFCompromise	A malicious user or process may cause TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).
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.
T.RemoteTransmit	TSF data may be disclosed or modified by an attacker while being transmitted between the TOE and remote trusted IT products.
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.
T.UnidentifiedActions	Failure of the authorized administrator to identify and act upon unauthorized actions may occur.

2 IDENTIFICATION

2.1 SECURITY TARGET AND TOE IDENTIFICATION

Security Target – *CA Integrated Threat Management ™ r8.0.*

TOE Identification – *CA Integrated Threat Management ™ r8.0.*

The Evaluated Configuration of the TOE is software only and includes the following Software Components of *Integrated Threat Management ™ r8.0:*

- ITM Server r8 which includes the java based interfaces (ITM Console, Alert Manager)
- *eTrust* Pest Patrol r8
- *eTrust Anti Virus r8*

The *e*Trust Pest Patrol Scan Engine, VET Engine, and InoculateIT Engine are part of the ITM product but are not evaluated as part of the TOE.

CC Identification – *Common Criteria for Information Technology Security Evaluatio*n, Version 2.3, August 2005.

CEM Identification – *Common Evaluation Methodology for Information Technology Securit*y, Version 2.3, August 2005.

Assurance Level - This ST is Common Criteria Version 2.3, Part 2 extended and Part 3 conformant, at Evaluation Assurance Level 3

Keywords – Anti-virus, Threat Management, Security Target, Security Management, Spyware.

2.2 IT SECURITY 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.

The TOE relies on the environment to provide:

- Anti-Malware scanning
- Protected audit trail storage
- User authentication before any action
- User identification before any action
- Management of TSF data
- Basic internal TSF data transfer protection
- Non-Bypassability of the TSP
- TSF domain separation
- Reliable time stamps
- Inter-TSF trusted channel

2.3 OPERATING SYSTEM

The TOE was evaluated with:

- ITM Server: Windows 2003 Server

- ITM Agent: Windows XP Professional

2.4 HARDWARE PLATFORM

The hardware platform is described in Section 8.

3 SECURITY POLICY

The Integrated Threat Management TOE provides these security services:

- Security Audit
- Anti-Malware
- Identification & Authentication (I&A)
- Security Management
- Partial protection of the TSF

Potential users of this product should confirm that functionality implemented is suitable to meet the user's requirements.

3.1 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

3.2 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

3.3 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.

3.4 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.

3.5 PARTIAL PROTECTION OF THE TSF

The ITM Server and client provide partial protection of TSF data. The TOE presents limited access to end users. It maintains and controls individual sessions for Administrators.

A summary of the SFRs for the TOE and IT environment are included in the tables below.

TOE Security Functional Requirements

Class FAU: Audit Generation	
FAU_ GEN.1	Audit data generation
FAU_SAR_EXP.1	Audit review
FAU_STG_EXP.1	Protected audit trail storage
Class FAM: Anti-Malware	
FAM_SDC_EXP.1	Discovery data collection
FAM_SCN_EXP.1	Anti-Malware scanning
FAM_ACT_EXP.1	Anti-Malware actions
FAM_ALR_EXP.1	Anti-Malware alerts
FAM_DRS_EXP.1	Data reporting
Class FIA: Identification & Authentication	
FIA_ATD.1*	User attribute definition
FIA_UAU_EXP.2 -1	User authentication before any action
FIA_UID_EXP.2 -1	User identification before any action
Class FMT: Security Management	
FMT_MOF.1*	Management of security functions behaviour
FMT_MTD.1-1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
Class FPT: Protection of TSF	
FPT_SEP_EXP.1	TSF domain separation

IT Environment Security Functional Requirements

Class FAM: Anti-Malware	
FAM_SCN_EXP.1-2	Anti-Malware scanning
Class FAU: Audit Generation	
FAU_STG_EXP.1-2	Protected Audit Trail Storage
Class FIA: Identification and Authentication	
FIA_UAU_EXP.2-2	User authentication before any action
FIA_UID_EXP.2-2	User identification before any action
Class FMT: Security Management	
FMT_MTD.1-2	Management of TSF data
Class FPT: Protection of TSF	
FPT_ITT.1	Basic Internal TSF Data Transfer Protection
FPT_RVM.1	Non-Bypassability of the TSP
FPT_SEP_EXP.1-2	TSF domain separation
FPT_STM.1	Reliable time stamps
Class FTP: Trusted Path/Channels	
FTP_ITC.1	Inter-TSF trusted channel

There is no means available for (untrusted) users to install/run executable files, nor to make use of network services.

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE

4.1 USAGE ASSUMPTIONS

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

4.2 ENVIRONMENTAL OBJECTIVES FOR THE IT ENVIRONMENT

OE.AuditStorage	The IT environment will provide a means for secure storage of the TOE audit log files.
OE.Malware	The IT environment will detect and take action against known malware introduced to the workstation via network traffic or removable media.
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.
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.
OE.RemoteSecureComms	The IT environment will provide a secure line of communications between the TOE and remote trusted IT

	products.
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.
OE.TimeStamps	The underlying operating system will provide reliable time stamps.
OE.TOEAccess	The IT Environment will provide mechanisms that control a user's logical access to the TOE.

4.3 ENVIRONMENTAL OBJECTIVES FOR THE NON-IT ENVIRONMENT

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.
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.
ON.NoUntrusted	Those responsible for the TOE must ensure that there are no untrusted users and no untrusted software on the ITM Server host.
ON.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
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.
ON.ProtectAuth	Users must ensure that their authentication data is held securely and not disclosed to unauthorized persons.
ON.SecureUpdates	Those responsible for the TOE will implement secure mechanisms for receiving and validating updated signature files from the Anti-Malware vendors.

4.4 CLARIFICATION OF SCOPE

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL3 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.

3. As with all EAL3 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” (as this term is defined in the CC and CEM) or “vulnerabilities” to objectives not claimed in the ST.
4. Integrated Threat Management depends on the IT environment to provide reliable time stamps, non-bypassability, and TSF domain separation. All cryptographic functions are part of the IT environment, not part of the TOE.
5. The TOE requires scan engines and signature files detect malware. To facilitate protection against ever changing virus and spyware threats, the scan engines and signature files must be updated regularly. However, updating TOE components is contrary to CC certification. Consequently, the scan engines and signature files are considered part of the IT Environment for this evaluation.

The ST provides additional information on the assumptions made and the threats countered.

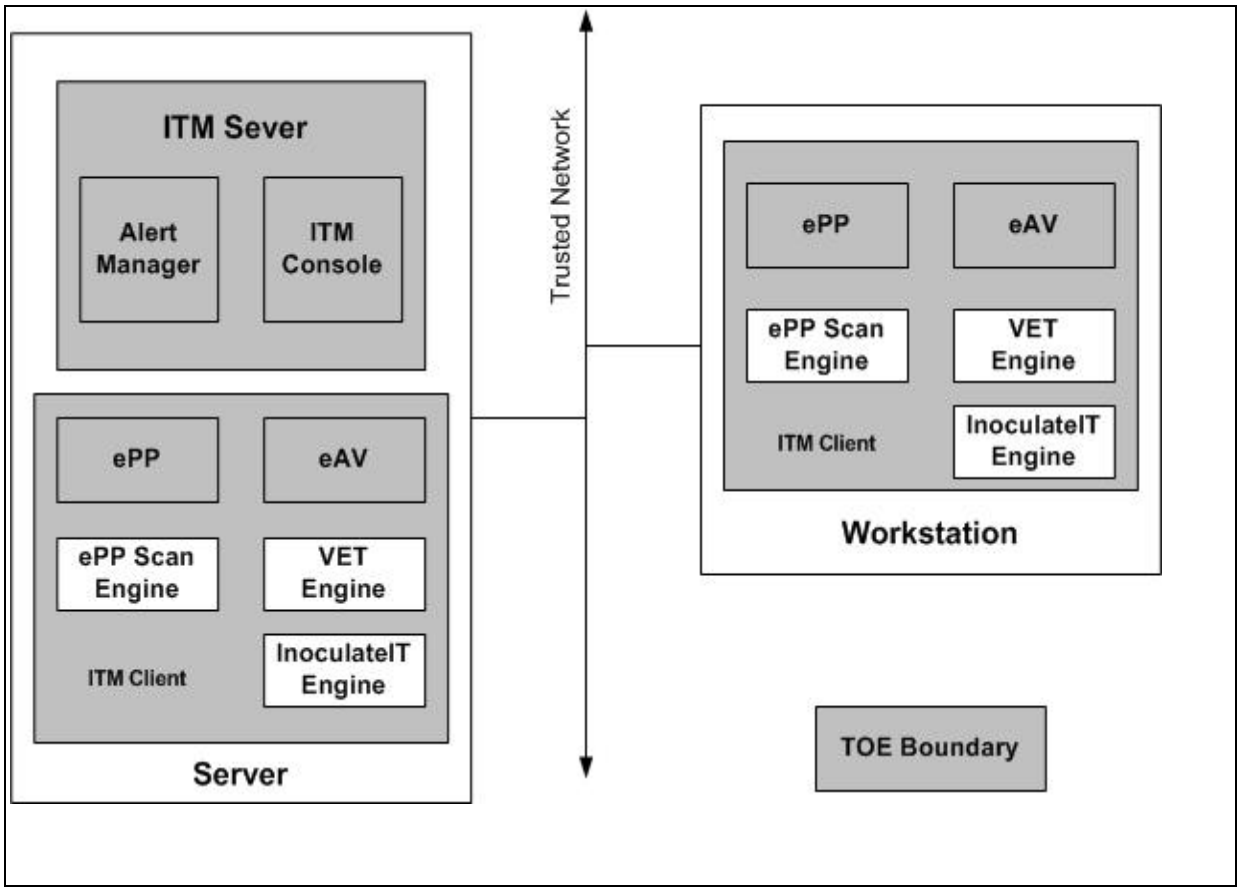
5 ARCHITECTURAL INFORMATION

CA Integrated Threat Management (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.

5.1 PRODUCT 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.

Figure 1: TOE Boundary



5.1.1 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.

5.1.1.1 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

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.

5.1.1.2 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.

5.1.2 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.

5.1.2.1 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. 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

5.1.2.2 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. 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. The Real time Monitor automatically starts up on reboot of the workstation.
- **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.
- **Heuristic Scanner** is a scanning method that uses heuristic analysis, an artificial intelligence technique used to scan files for viruses whose signatures have not yet been isolated and documented. Rather than use a fixed algorithm to scan for specific virus signatures, heuristic analysis uses alternative methods to detect virus-like patterns of behavior.
- **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.

5.2 TOE INTERFACE TO SCAN ENGINES

Malware scanning is performed by the following IT Environment components:

- Pest Patrol Engine
- Vet Engine
- InoculateIT Engine
- Archive Library

Each of these components is DLL files that contain both executable code and malware signature data. The operating system maps the DLL files into ITM's address space whenever ITM is started. The features of these components are exposed to the TOE using in-process COM interfaces in the case of the Pest Patrol Engine and C functions in the other three cases.

In-process COM servers are implemented as DLLs. These DLLs are loaded into the process space of the calling process, and therefore run in the context of the calling process.

For the 3 components that use C functions interface, TOE need to load the corresponding DLL and call the C functions directly provided by the component to perform desired functions.

The realtime protection is provided by the realtime driver in conjunction with the realtime service that utilizes the four components described above. The driver intercepts calls to operating system drivers and use device I/O control calls to communicate with the realtime service.

6 DOCUMENTATION

The following is a list of the end-user documentation that was used to support this evaluation:

- *eTrust™ Antivirus Administrator Guide r8;*
- *eTrust™ Antivirus Implementation Guide r8;*
- *eTrust™ PestPatrol Guide r8;*
- *eTrust™ PestPatrol Implementation Guide r8;* and
- *CA Integrated Threat Management r8.0 Security Target V1.8*

The applicable guidance in these documents must be followed in order to operate *Integrated Threat Management* in its evaluated configuration.

7 IT PRODUCT TESTING

This section describes the testing efforts of the Vendor and the evaluation team.

The purpose of the Testing activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST. This section describes the testing efforts of the developer and the evaluation team.

All of the testing was conducted in at:

CygnaCom Solutions, Inc.
7925 Jones Branch Drive, Suite 5200
McLean, VA 22102-3321

The testing was performed in four parts over five business days. Installation Testing was performed the first day. Developer testing was performed on all five days. Independent and penetration testing was performed on the fifth day of testing.

The test plan and results, as well as the evaluation team's review of the testing in the Evaluation Technical Report, were well written and complete.

Apache Tomcat Application Server Version 5.5 and Java 1.5 Update 4 are bundled with the TOE release media. It is noted that these IT Environment applications were not tested during the evaluation and may have vulnerabilities which require patches.

The TOE relies on the IT Environment to calculate the message digest to verify the integrity of the signature files obtained during a content update action. This verification process was not part of the TOE evaluation and it is not known how or if this integrity verification is performed.

7.1 INSTALLATION TESTING

The installation was performed by the evaluation team. The Target of Evaluation was installed following the procedures defined in the following documents:

- Common Criteria Supplement to the Computer Associates Integrated Threat Management Administration Guide V1.0

- Computer Associates *eTrust ™ Integrated Threat Management Implementation Guide* r8.0

The test installation resulted in a successful installation of the TOE in the evaluated configuration. All of the TOE components were installed correctly for the evaluated configuration by following the procedures documented in the Common Criteria Supplement to the Administration Guide and the Integrated Threat Management Implementation Guide r8.0.

After installation, the evaluated configuration of the TOE was tested without having to change any of the configuration parameters or rerun any of the installation steps.

7.2 DEVELOPER TESTING

The set of developer tests consists of 32 test procedures. The evaluation team performed 22 of the tests provided by the developer. All of the test cases included a test description, security functions tested, rationale, purpose for the test, explicit test steps, and an expected result. The testing was either performed by evaluator while being observed and recorded by the evaluation team or performed by the evaluation team with assistance from the CA personnel.

For all of the tests performed, the technical contact and evaluation team took sample screenshots, which were saved in separate files on the computers used for testing. The evaluation team also took notes during the testing, which are stored in both hard copy and electronic form at CygnaCom SEL as testing evidence for this evaluation.

No hardware test tools or software scripts were used during the developer functional testing.

All of the sample developer tests were executed successfully by the evaluation team.

7.3 EVALUATION TEAM INDEPENDENT TESTING

The evaluation team devised a test subset for independent testing. The test subset consisted of additional test functions to enhance what was tested by the developer. All of the test cases included a purpose, explicit test steps, and an expected result. The evaluation team produced test documentation for the test subset that was sufficiently detailed to enable the tests to be reproducible. This time the testing was performed by the evaluation team, with the CA personnel present. The Validator relied on the independent and penetration test report in *CA eTrust Integrated Threat Management™ r8.0 Test Plan and Report V1.0*.

The test cases defined by the evaluation team were executed after the TOE was installed in the evaluated configuration consistent with the Security Target. The evaluation team selected independent tests to supplement and enhance the functional testing performed on Developer's Functional test suite.

Each test was intended to explicitly exercise the Security Audit, Anti-Malware, Security Management, Identification & Authentication (I&A) and implicitly tested Partial Protection of the TSF by all test cases and the team defined penetration tests.

The environment and configuration for the Team-Defined testing was the same as that for the Developer Functional testing. No hardware test tools were used during the testing. No general test setup procedures were performed prior to the Team-Defined testing. Setup steps and pre-requisites specific to individual tests are described in the individual test case documents.

The validation team relied on the evaluation team's independent testing effort and concluded that the testing was successful.

7.4 EVALUATION TEAM PENETRATION TESTING

For its penetration tests, the evaluation team evaluated the developer's vulnerability analysis document, the independent test plan, the guidance documentation and the TOE design to identify potential penetration test cases. Penetration tests were selected based on the evaluation team's experience with evaluating the developer's design, guidance, test, and vulnerability assessment documentation.

The evaluation team created a penetration test plan. All of the test cases included a purpose, explicit test steps, and an expected result. The evaluation team performed five penetration tests.

- Login Error Messages Credential Enumeration
- Negative URL value
- Format String Vulnerability
- Inadequate Account Lockout
- Message Queuing

In addition to these manual penetration tests the evaluation team conducted a port scan using Nessus Vulnerability Scanner. No vulnerabilities were found using Nessus.

The testing was performed by the evaluation team. The Validator relied on the independent and penetration test report.

8 EVALUATED CONFIGURATION

8.1 TEST SOFTWARE AND HARDWARE

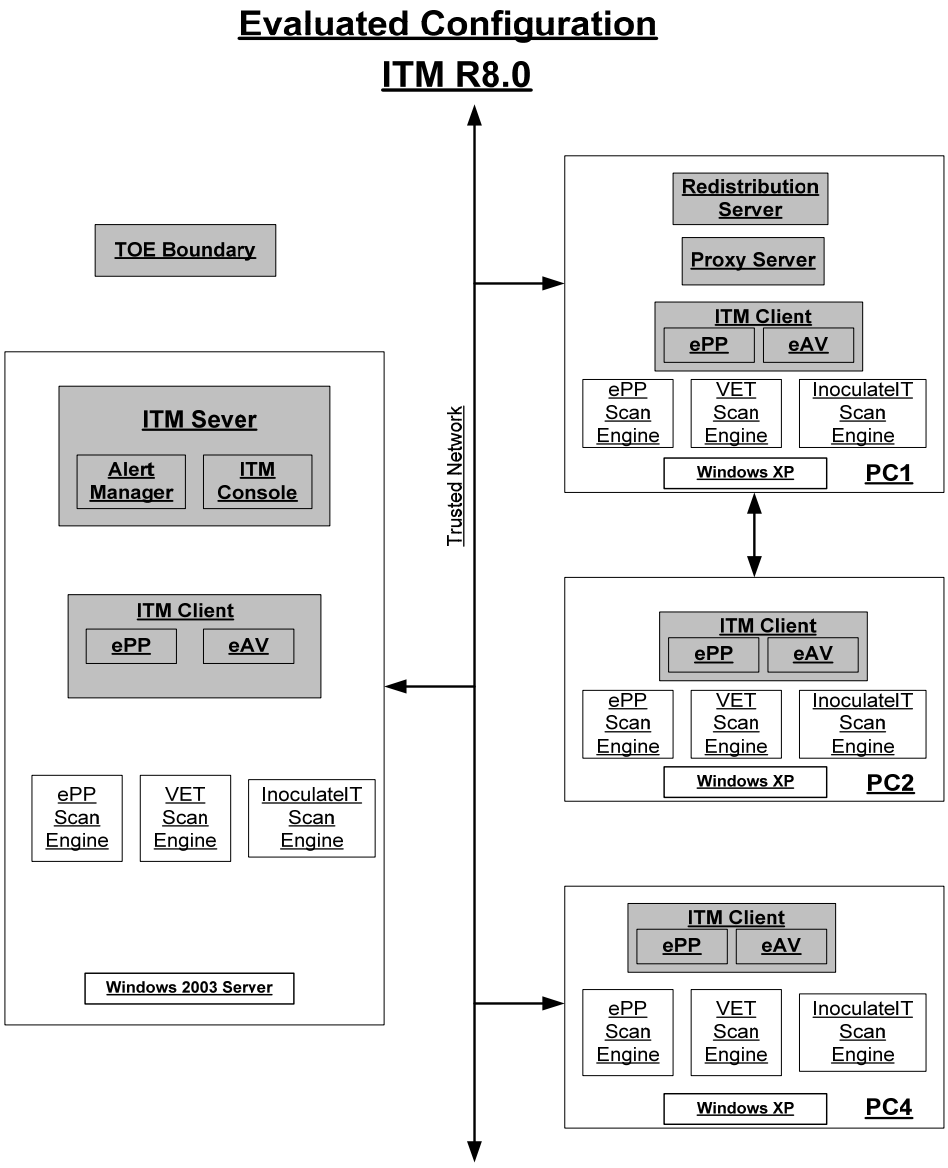


Figure 2: Evaluated Configuration

Server

- Software:
  - Windows 2003 Server
  - ITM Server r8.0
    - Alert Manager
    - ITM Console
  - ITM Agent
    - eTrust Antivirus r8.0
    - eTrust PestPatrol r8.0
- Hardware:
  - Pentium 3 GHz processor
  - 2 GB RAM
  - 80 GB Hard Drive

PC1:

- Software
  - Windows XP Pro
  - ITM Agent
    - Redistribution Server
    - eTrust Antivirus r8.0
    - eTrust PestPatrol r8.
- Hardware:
  - Pentium 2 GHz processor
  - 512B RAM
  - 40 GB Hard Drive

PC2:

- Software
  - Windows XP Pro
  - ITM Agent
    - eTrust Antivirus r8.0
    - eTrust PestPatrol r8.
- Hardware:
  - Pentium 2 GHz processor
  - 512B RAM
  - 40 GB Hard Drive

PC4

- Software
  - Windows XP Pro
  - ITM Agent
    - eTrust Antivirus r8.0
    - eTrust PestPatrol r8.
- Hardware:

- Pentium 2 GHz processor
- 512B RAM
- 40 GB Hard Drive

8.2 TEST TOOLS AND SCRIPTS

The following hardware test tools were used for the independent and penetration testing.

- Nessus Vulnerability Scanner and nmap port scanner.

9 RESULTS OF THE EVALUATION

The evaluation team conducted the evaluation in accordance with the CC and the CEM

The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL3 assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence. In the Final ETR, all Fail or Inconclusive work unit verdicts have been resolved by the developer and the evaluation team.

In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the following documents:

- *Evaluation Technical Report for a Target of Evaluation,, CA eTrust Integrated Threat Management™ r8.0, ETR Version1.0, Security Target Version 1.7, dated January 16, 2007.*

The evaluation team determined the TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 3) requirements. The rationale supporting each CEM work unit verdict is recorded in the ETR.

Therefore, when configured according to the guidance documentation enumerated in section 5.2 of this report, the TOE Integrated Threat Management is CC compliant and satisfies the *CA Integrated Threat Management™ r8.0.*

The ITM r8.0 will detect any attempt to install or run an executable (including a .dll) which matches a known malware signature, regardless of the source of the file (from a remote source or from the local file structure). With proper configuration, ITM r8.0 scans all files prior to any file transfer occurring as dictated by Operating System file traffic. Consequently, any attempt to inject a harmful .dll into a running process will be detected and prevented. However, if ITM's Realtime Scanning is disabled, a harmful .dll thread could possibly be injected into a running process. Under this circumstance, an injected .dll thread would go undetected. Note that disabling the Realtime Scanner is not consistent with the evaluated configuration and is not recommended.

10 VALIDATION COMMENTS/RECOMMENDATIONS

10.1 VALIDATION COMMENTS

The TOE is distributed, but there is no TOE security functional requirement to protect TOE data between machines. Since there are no requirements to protect the TOE data between distributed components of the TOE, the evaluation team did not check whether the network traffic between TOE machines could be intercepted, modified, manipulated, or otherwise interfered with. The customer can have no confidence, based on this evaluation, that the *e*Trust Audit product is capable of protecting itself from any type of threat that could have access to the communication paths between components. The TOE is installed with SSL encryption in the IT environment. The consumer is left to determine whether the SSL encryption is functional and adequate strength to protect the TSF data from disclosure and modification when it is transmitted between separate parts of the TOE as required by FPT_ITT.1.1.

Apache Tomcat Application Server Version 5.5 and Java 1.5 Update 4 are bundled with the TOE release media. It is noted that these IT Environment applications were not tested during the evaluation and may have vulnerabilities which require patches.

The TOE relies on the IT Environment to calculate the message digest to verify the integrity of the signature files obtained during a content update action. This verification process was not part of the TOE evaluation and it is not known how or if this integrity verification is performed.

As noted in Section 4.4 item 5 of this report, The TOE requires scan engines and signature files to detect malware. To facilitate protection against ever changing virus and spyware threats, the scan engines and signature files must be updated regularly. However, updating TOE components is contrary to CC certification. Consequently, the scan engines and signature files are considered part of the IT Environment for this evaluation. Since Auto Update (Content Updates) apply to both TOE and engines, Auto Updates (Content updates) are disabled during installation. Content Updates are configured as part of the installation procedures documented in the CC Supplement to the User Guidance.

The evaluated version of the TOE ITM r8.0.445 was obtained from a Computer Associates FTP site made available to those consumers who want the CC certified version of ITM. As part of the installation process, patches are installed to counter the two known vulnerabilities:

- CVE 2006-3223- Format string vulnerability: The CVE 2006-3223 has been resolved with patch ITM r8.0.432 from Computer Associates. The patch is included as part of the TOE build 445 which is the certified version of the TOE.
- Vulnerability exists if the iGateway component is older than version 4.0.051230. The iGateway vulnerability is resolved at installation time. The Common Criteria Supplement to the Computer Associates Integrated Threat Management Administration Guide V1.0 describes the procedures required to upgrade iGateway version to 4.0.60220.0.

As noted in Figure 2, the evaluated configuration consisted of four PCs using Windows XP and one server using Windows 2003 Server. All critical Windows Updates were installed on each machine in the test environment prior to testing.

Since the ITM CONSOLE does not limit the number of false login requests, it is necessary for the admin to limit the number of "false OS login requests" to achieve the designated TOE SOF.

10.2 SIGNIFICANT FINDINGS DURING EVALUATION

None

10.3 VALIDATION RECOMMENDATIONS

The Validation team observed that the evaluation and all its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validation team agrees that the CCTL presented appropriate rationales to support the evaluation results presented in Section 4 of the ETR and the conclusions presented in Section 5 of the ETR. The Validation team therefore concludes that the evaluation and PASS result for this TOE are complete and correct for CA Integrated Threat Management r8.0.build 445.

11 LIST OF ACRONYMS

Acronym	Description
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
ID	Identifier
IT	Information Technology
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

12 BIBLIOGRAPHY

The validation team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluatio*n, version 2.3, August 2005, Part 1.
- *Common Criteria for Information Technology Security Evaluatio*n, version 2.3, August 2005, Part 2.
- *Common Criteria for Information Technology Security Evaluatio*n, version 2.3, August 2005, Part 3.
- *Common Evaluation Methodology for Information Technology Security, version 2.3,* August 2005.
- *CA Integrated Threat Management ™ r.8.0 Security Target Version 1.8, dated 1 May 2007.*
- *Evaluation Technical Report for a Target of Evaluation,, CA eTrust Integrated Threat Management ™ r8.0.445, ETR Version1.0, Security Target Version 1.8, dated May 1, 2007.*
- *CA eTrust Integrated Threat Management ™ r8.0, Test Report V1.0, dated December 20, 2006.*
- *Common Criteria Supplement to the Computer Associates Integrated Threat Management Administrator Guide V1.2, dated 10 May 2007*