National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Cimcor® CimTrak Integrity Suite Version 2.0.6.0 F

Report Number: CCEVS-VR-VID10303-2010
Dated: 26 July 2010
Version: 1.2

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Mike Allen (Lead Validator)
Jerome Myers (Senior Validator)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Kenji Yoshino
Ryan Day
Stephen Wilson

InfoGard Laboratories, Inc.
709 Fiero Lane
Suite 25
San Luis Obispo, CA 93401

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Validator Comments in Section 10.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cimcor® CimTrak Integrity Suite, the Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the Cimcor® CimTrak Integrity Suite product was performed by InfoGard Laboratories, Inc., in San Luis Obispo, CA in the United States and was completed in January 2010 and updated in June 2010.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by InfoGard Laboratories. The ETR and test report used in developing this validation report were also written by InfoGard Laboratories. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, version 3.1, dated September 2007 at Evaluation Assurance Level 4 (EAL 4) augmented with ALC_FLR.2 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, dated September 2007. The product, when configured as specified in the installation, user and CC supplemental guides, satisfies all of the security functional requirements stated in the Cimcor® CimTrak Integrity Suite Security Target. The evaluation team determined the product to be Part 2 and Part 3 conformant, and meets the assurance requirements of EAL 4 with ALC_FLR.2. The product is not conformant to any Protection Profile.

1.1 TOE Summary

The Cimcor® CimTrak Integrity Suite is composed of CimTrak for Servers and CimTrak for Network Devices. CimTrak for Servers and CimTrak for Network devices allow administrative users to “lock” files and configuration data respectively. CimTrak provides an additional layer of protection for networks by providing logging and/or remediation of any changes to “locked” objects. The Integrity Suite consists of the CimTrak Master Repository, CimTrak Management Console, CimTrak File System Agent (CimTrak for Servers), and CimTrak Network Device Agent.

The CimTrak Master Repository is a centralized server which maintains a centralized store of protected objects and change history. It maintains an encrypted copy of files and configurations that allows for restoration and/or notification in the event of unauthorized change. The Master

Repository also stores a configurable number of previous versions of a file. An administrative user can use these previous versions to rollback a protected file to one of the versions stored in the Master Repository.

The CimTrak File System Agent monitors files or directories on the servers. It can be configured to allow a change and log the event, update the master file stored within the Master Repository, immediately overwrite the change with the copy from the Master Repository, or prompt the administrative user to allow or disallow the change.

The CimTrak Network Device Agent provides the same logging, remediation, and notification features for network device configurations; however, it must be installed on a host platform and communicate with network devices via SSH to detect and remediate changes.

The Master Repository and Agents are headless applications, so the CimTrak Management Console is a GUI that enables the administrative users to manage these components.

The TOE required software components and supported network devices are shown in Table 1 below.

1.2 Validation Summary

During this evaluation, the Validators monitored the activities of the InfoGard evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test reports. The Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validators conclude that the InfoGard findings are accurate, the conclusions justified, and the conformance claims correct.

Table 1: Operational Environment

Component	Description
Master Repository Operating System	Windows 2000 SP4, XP (SP3), 2003, Vista, or 2008
Agent server Operating System	Windows 2000 SP4, XP (SP3), 2003, Vista, or 2008 Linux Kernel 2.6 (Ubuntu, Redhat, CentOS, SuSE)
Management Console Operating System	Windows 2000 SP4, XP (SP3), 2003, Vista, or 2008
Firewall/Router/Switch (Network devices with remote configuration capabilities)	Network Architecture item(s) As required based on network topology Provided scripts support: Cisco and Juniper network devices running the following Operating Systems (OS): Juniper- JunOS version 6.0 and above* Cisco- IOS version 11.2 and above* Cisco- FOS version 6.0 and above* Cisco-ASA version 7.0 and above* *must support SSHv2

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) products, desiring a security evaluation, enter into a contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant, if any; and
- The organizations and individuals participating in the evaluation.

Table 2: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	CimTrak Integrity Suite which consists of: - CimTrak Master Repository 2.0.6.0 F - CimTrak File System Agent 2.0.6.0 F - CimTrak Management Console 2.0.6.0 F - CimTrak Network Device Agent 2.0.6.0 F
Protection Profile	None.
Security Target	Cimcor® CimTrak® Integrity Suite 2.0.6.0 F Security Target EAL 4 augmented ALC_FLR.2 Version 1.2 June 9, 2010
Dates of evaluation	February 2008 through February 2010
Evaluation Technical Report	Evaluation Technical Report Cimcor® CimTrak Integrity Suite 2.0.6.0 F VID 10303 09-1501-R-0048 document version 1.2, released July 26, 2010.
Conformance Result	Part 2 and Part 3 conformant, EAL 4 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1, September 2007 and all applicable NIAP and International Interpretations effective on February 7, 2008
Common Evaluation Methodology (CEM) version	CEM version 3.1R2 dated September 2007and all applicable NIAP and International Interpretations effective on February 7, 2008
Sponsor	Cimcor, Inc., 8252 Virginia Street, Suite C, Merrillville, IN 46410
Developer	Cimcor, Inc., 8252 Virginia Street, Suite C, Merrillville, IN 46410
Common Criteria Testing Lab	InfoGard Laboratories, Inc.
Evaluators	Kenji Yoshino, Ryan Day
Validation Team	Jerome Myers and Mike Allen of The Aerospace Corporation

3 Security Policy

The TOE enforces the following security policies:

3.1 Security Audit

The Security Audit security function within the CimTrak application generates audit logs for application configuration, change detection, remediation, and administrative access to TSF/User Data. Audit logs are stored within the Master Repository and viewed using the Management Console. The Administrator may disable certain types of audit records; however, logging of intrusion and remediation events is always active.

3.2 Access Control

The Access Control security function requires all administrative users and all Agents to authenticate to the Master Repository before any further communication is allowed. The TOE maintains the roles of Administrator, Standard User, and Auditor for human users of the TOE. There is not a user role that represents users on the Agent machines, because the Agents do not support a human user interface.

The Administrator has full access to all management and configuration options. Standard Users can configure Agents and "locked" objects to which they have been assigned permissions. Auditors have read only access.

In addition to the use roles, a "private key" can be assigned to Agents or "locked" objects. The "private key" is a password that is converted to a symmetric key and used to provide an additional layer of encryption for data stored in the Master Repository. Any user attempting to access data protected by a "private key" must provide the "private key."

3.3 Cryptographic Operations

The TOE uses cryptography to secure communications between distributed components of the TOE, secure communications with network devices, and encrypt files stored within the Master Repository. The TOE uses the Cimcor Cryptographic Module, which has been FIPS 140-2 Level 2 validated to perform all cryptographic operations.

3.4 Change Management

The Change Management security function provides the ability for the Agents to detect changes made to files or configuration data set as "locked." CimTrak can be configured to take one of the following actions when such changes are identified:

Log Only – allow the change and log the change

Prompt – prompt the authorized user if the change should be allowed or denied

Update Baseline – allow the change and upload the changed object to the Master Repository

Restore – deny the change by overwriting the changed file with a copy from the Master Repository

Custom – enables the administrative user to create a custom combination of logging, notification, and remediation actions.

4 Assumptions and Clarification of Scope

4.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

A.ADMIN	The Administrators are appropriately trained, not careless, not willfully negligent, non-hostile and follow and abide by the instructions provided in the guidance documentation; however, they are capable of error.
A.PHYSEC	The Master Repository, Network Hosts (Network Agents) and Servers (File System Agents) are housed in a physically secure server room environment.
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and non-TOE related storage repository capabilities on the Network Hosts or the Master Repository machine.
A.PUBLIC	The TOE does not host public data.
A.REMACC	Authorized Administrators may access the TOE remotely from the internal and external networks.
A. TIME_STAMP	The Operational Environment shall provide an accurate time source for use in time stamps.

4.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

T. ADMIN_ERROR	An Administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, thus allowing an attacker to escape detection.
T.CHANGE	A user or IT entity may make unauthorized changes to files/configuration data on resources within the TSC.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources

T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEM	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being discovered thereby causing potential security vulnerabilities.
T.MEDIATE	A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized [Administrator] and the TOE.
T.TSF_COMP	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.UNIDENT_ACTION	Failure of the authorized Administrator to identify and act upon unauthorized actions may occur.

4.3 Organizational Security Policies

The TOE enforces the following OSPs:

P.ACCOUNT	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P. BANNER	The management console component of the TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.
P.CRYPTO	Only NIST FIPS 140-2 validated cryptography (methods and implementations) are acceptable for key management.
P.ROLES	The TOE shall provide an authorized Administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

4.4 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 the following features and parts of the typical CimTrak product were not included in the evaluation and use of these features will remove the product from the evaluated configuration and negate the finding:

- Use of Telnet for Network Agent to Device communication*
- Use of Master Repository FTP Interface
- Compliance Templates ("Compliances") (PCI, SOX, FISMA)
- CimTrak Industrial Agent (Agent intended for Industrial applications i.e.: PLC vs. IT Resources) – This Agent Component is not included in the Common Criteria release of the product. The Industrial Agent is for Industrial applications (manufacturing machinery) and has no use in an Operational Environment.
- Command Line Interface (CLI) – the Security Management security function is only supported through the Graphical User Interface (GUI) for the Common Criteria Evaluated configuration.
- Configuration Support Interface – executed from the Command Line
- Use of the CimTrak Communications protocol for session encryption
- All Fedora-Linux operating systems are excluded.
- All Apple-Macintosh operating systems are excluded.
- All Sun Solaris operating systems are excluded.
- All Hewlett Packard-HPUX operating systems are excluded.

*Telnet is supported by the product but is excluded from the CC Evaluated Configuration as it does not support encryption.

5 Architectural Information

The CimTrak Integrity Suite 2.0.6.0 F is composed of the following components:

- Master Repository 2.0.6.0 F
- Management Console 2.0.6.0 F
- File System Agent 2.0.6.0 F
- Network Device Agent 2.0.6.0 F

The TOE is composed entirely of software components. Figure 1 depicts an example deployment of the TOE on a network and shows the TOE/Operational Environment Boundary. The Server and Database Agents in the figure represent the File System Agent when installed on a server.

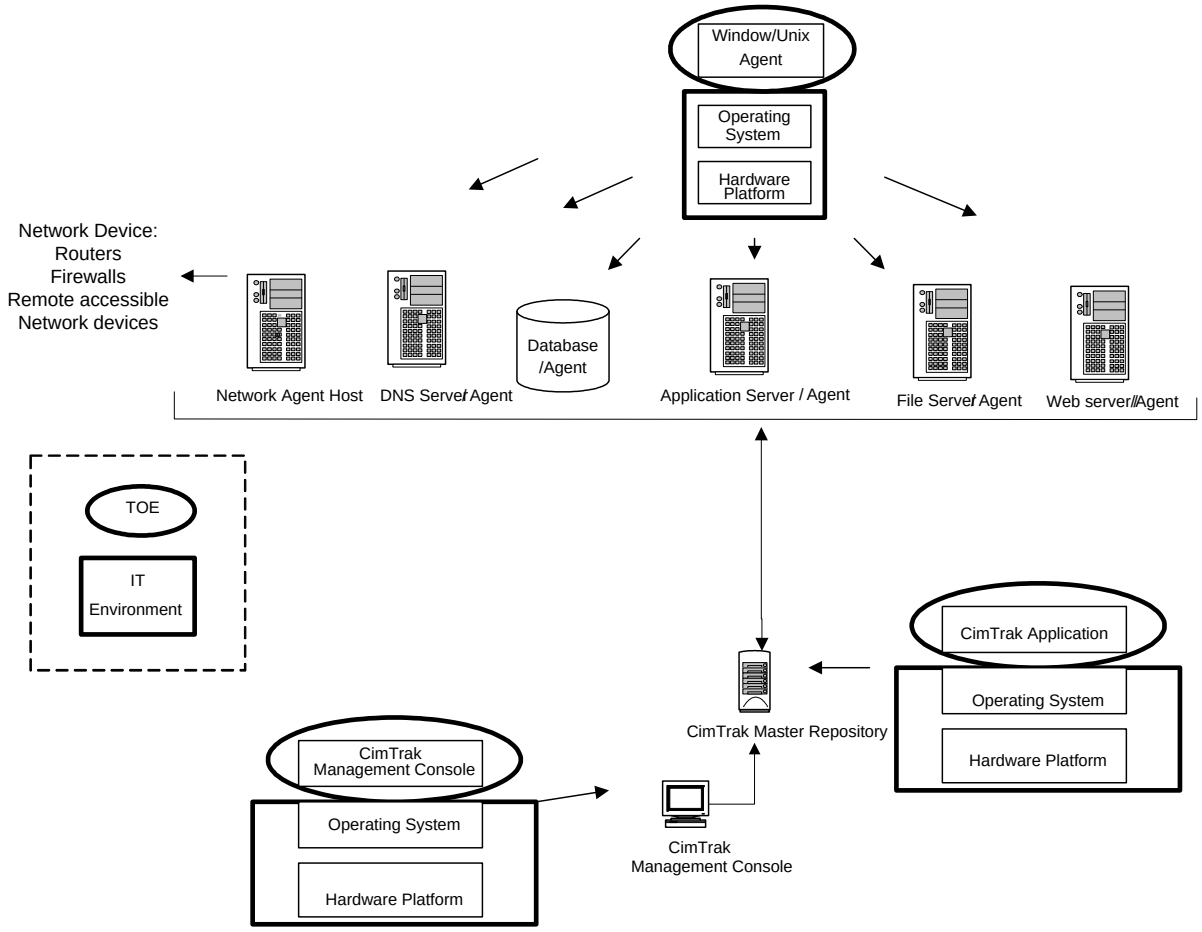

Figure 1 Network Diagram

5.1 Master Repository

The Master Repository is a centralized server which maintains a centralized store of protected objects and change history. The Master Repository implements a proprietary database for storing copies of "locked" files or configuration data. The "locked" objects are stored in encrypted form. These copies allow for restoration and/or notification in the event a change is detected by an Agent. The Master Repository can be configured to store multiple copies of a "locked" object, so administrative users can compare different versions of the object.

The Master Repository includes a PostgreSQL database for all other types of data (e.g., audit logs, user accounts, configuration parameters).

The Master Repository does not have a user interface and can only be configured though the Management Console.

5.2 Management Console

The Management Console is the GUI that allows administrative users to configure the Master Repository, Agent settings, and "lock" state of objects. The Management Console also allows the administrative users to view audit logs and files that are stored on the Master Repository.

Communication between the Management Console and the Master Repository is secured using a TLS session. Management of Agents is performed by updating settings on the Master Repository which are sent to the Agent when the Agent connects to the Master Repository.

5.3 File System Agent

The File System Agent is installed on pre-existing servers and monitors files or directories on those servers. It can be configured to allow a change and log the event, update the master file stored within the Master Repository, immediately overwrite a change with the copy from the Master Repository, or prompt the administrative user to allow or disallow a change.

When the File System Agent starts, it connects to the Master Repository to obtain configuration data and locked files. The File System Agent periodically sends a heartbeat to the Master Repository which alerts the Management Console that the Agent is active and responding.

The Linux File System Agent can be configured to detect changes by periodically polling the last modified dates and using a SHA-1 hash to determine if a file has changed by checking the file at an interval configured by the Administrator.

The Windows File System Agent can be configured to detect changes by two different means. It can use the poll-based method described above, or it can detect changes by registering with the operating system to be notified when a file is updated.

The File System Agents periodically send performance statistics (i.e. CPU utilization, RAM utilization, HD space used, and network utilization statistics) to the Master Repository.

5.4 Network Device Agent

The CimTrak Network Device Agent is installed on a host machine. It uses SSH to connect to network devices so it can monitor the configuration of the network devices. It provides the same logging, remediation, and notification features as the File System Agent; however, it only supports poll based change detection.

6 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the CimTrak Integrity Suite. In these tables, the following conventions are used:

Documentation that is delivered to the customer is shown with **bold** titles.

Documentation that was used as evidence but is not delivered to a customer is shown in a normal typeface.

The TOE is physically delivered to the End-User. The guidance is part of the TOE and is delivered in printed form and as PDFs files on the installation media.

6.1 Design Documentation

Document	Revision	Date
EAL 4 Security Architecture Description – Cimcor CimTrak Integrity Suite	0.6	January 22, 2010
EAL 4 Target of Evaluation (TOE) Design and Functional Specification Cimcor CimTrak Integrity Suite	0.9	January 22, 2010

6.2 Guidance Documentation

Document	Revision	Date
CimTrak Installation Guide Version 2.0.6.0 CimTrak Server / Repository CimTrak Agent CimTrak Management Console CimTrak Network Device Agent	N/A	February 10, 2010
CimTrak User Guide Version 2.0.6.0 CimTrak Server / Repository CimTrak Agent CimTrak Management Console CimTrak Network Device Agent	N/A	February 10, 2010
CimTrak Common Criteria Supplement Version 2.0.6.0 F CimTrak Server/Repository CimTrak Agent CimTrak Management Console CimTrak Network Agent Device	.16	February 10, 2010

6.3 Configuration Management and Lifecycle

Document	Revision	Date
ALC_CMC.4 Life-Cycle Support Documentation: Configuration Management Capabilities Cimcor CimTrak Integrity Suite, Version 0.10, December 1, 2009	0.10	December 1, 2009
ALC_CMS.4 Life-Cycle Support Documentation: Configuration Management Scope Cimcor CimTrak Integrity Suite Version 1.0	.17	August 5, 2010
ALC_DEL.1 Life-Cycle Support Documentation: Delivery Cimcor CimTrak Integrity Suite	0.6	December 1, 2009
ALC_DVS.1 Life-Cycle Support Documentation: Development Security Cimcor CimTrak Integrity Suite	0.7	June 10, 2008
Cimcor Security Flaw Form	3.0	November 7, 2008
ALC_LCD.1 Life-Cycle Support Documentation: Life Cycle Development Cimcor CimTrak Integrity Suite	0.7	March 2, 2009

6.4 Test Documentation

Document	Revision	Date
EAL 4 (+ ALC_FLR): Tests Activity ATE: Cimcor CimTrak Integrity Suite Windows Server 2003 SP2/Red Hat 5.1/Windows XP SP3	0.7	June 14, 2010
EAL 4 (+ ALC_FLR) Tests Activity ATE Cimcor CimTrak Integrity Suite Windows 2000 SP4/Windows Server 2008	0.1	June 14, 2010
EAL 4 (+ ALC_FLR) Tests Activity ATE Cimcor CimTrak Integrity Suite Windows Server 2008/Windows 2000 SP4	0.1	June 14, 2010
EAL 4 (+ ALC_FLR) Tests Activity ATE Cimcor CimTrak Integrity Suite Windows Vista/Windows Server 2003 SP2	0.1	June 14, 2010

Document	Revision	Date
EAL 4 (+ ALC_FLR) Tests Activity ATE Cimcor CimTrak Integrity Suite Windows XP SP3/Windows Vista	0.1	June 14, 2010
Independent and Penetration Test Plan	1.0	January 18-20, 2010
Independent and Penetration Test Plan Part Two	1.0	June 17, 2010

6.5 Vulnerability Assessment Documentation

Document	Revision	Date
Cimcor CimTrak Integrity Suite Version 2.0.6.0 F: Common Criteria Vulnerability Analysis AVA_VAN.3 EAL4	1.0	December 5, 2009

6.6 Security Target

Document	Revision	Date
CIMCOR® CimTrak® Integrity Suite Security Target EAL 4 augmented ALC_FLR.2, June 9, 2010, Version 1.2	1.2	June 9, 2010

6.7 Site Audit

Document	Revision	Date
Cimcor Site Audit Master Checklist	1.0	October 30, 2009

7 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

7.1 Test Configuration

The following diagram and text demonstrates the test setup and placement of the TOE in the test environment in accordance with the Common Criteria Evaluated Configuration as described in the applicable Security Target. Each of the Windows VMs System was tested with all of the supported Windows Operating Systems. The configuration of the VMs lists the Operating Systems that were tested on that VM. Refer to the test documentation listed in section 6.4 for the information on which OSs were tested together.

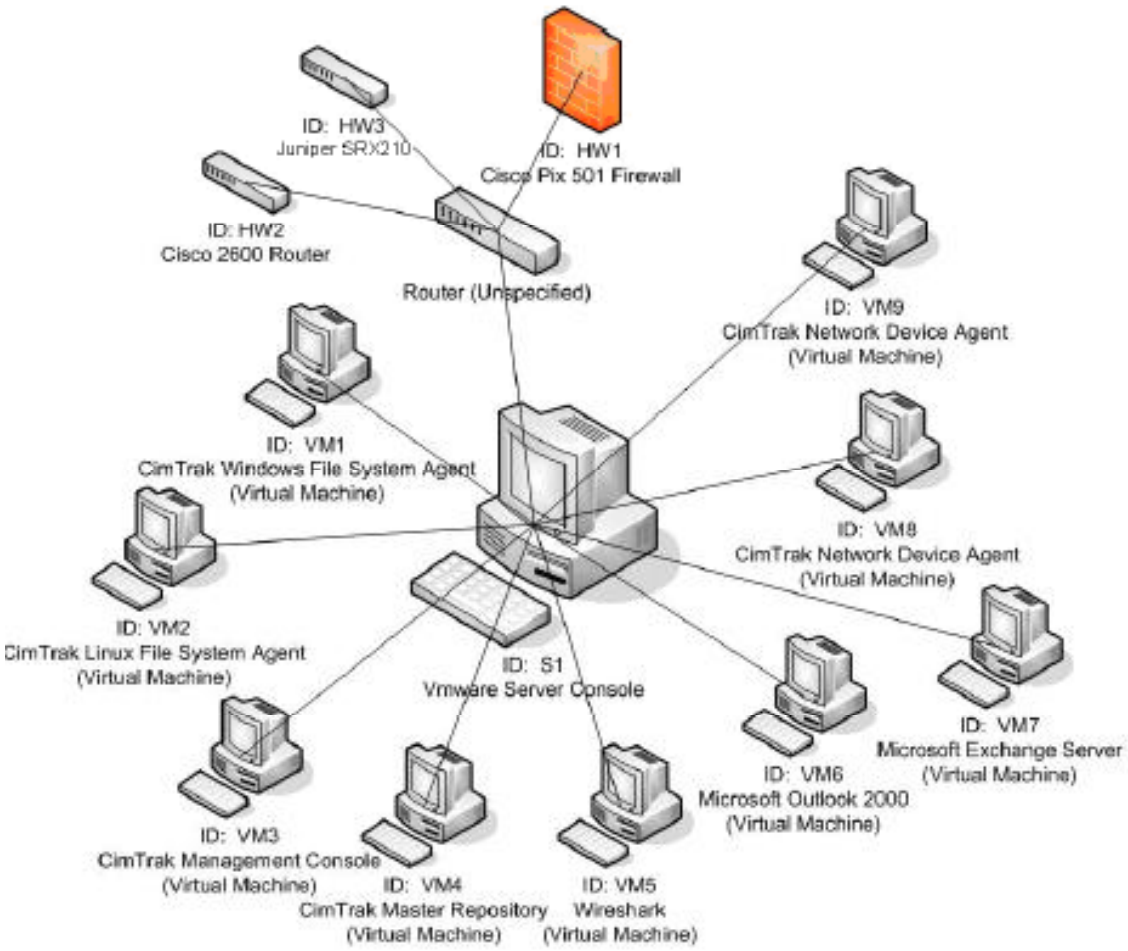

Figure 7-1: TOE Physical Test Setup Configuration

7.1.1 Virtual Machine Server (ID: S1) Configuration Specifics

System S1 is the VMware Server Console implemented on a Dell Optiplex GX745 containing 4

GB of RAM and an Intel Core2 Duo 2.4 GHz processor. All of the TOE component and testing virtual machines will be installed on this system. To avoid disk space constraints, a 250GB hard drive is recommended. Each Virtual Machine configuration will use the default resources and configurations as allocated by VMware Server Console. The default configurations are required since, potentially, all Virtual Machines may be functioning concurrently resulting in the depletion of system resources on System S1. The network interface card should be configured with the following IP Address assignment: 192.168.1.100.

7.1.1.1 Installed Components

• Microsoft Windows Server 2003 SP2 Enterprise Edition
• VMware Server Console Version 1.0.7 build-108231

7.1.2 CimTrak Windows File System Agent (ID: VM1) Configuration Specifics

System VM1 is installed on a Virtual Machine located on System S1. The network interface card should be configured with the following IP Address assignment: 192.168.1.101.

7.1.2.1 Installed Components

OSs:
• Microsoft Windows Server 2003 SP2 Enterprise Edition
• Microsoft Windows 2000 SP4
• Microsoft Windows Server 2008
• Microsoft Windows Vista
• Microsoft Windows XP SP3

Software:
• CimTrak® for Servers Version 2.0.6.0 F Windows File System Agent

7.1.3 CimTrak Linux File System Agent (ID: VM2) Configuration Specifics

System VM2 is installed on a Virtual Machine located on System S1. The network interface card should be configured with the following IP Address assignment: 192.168.1.102.

7.1.3.1 Installed Components

OS:
• Red Hat Enterprise Linux Version 5.1

Software:
• CimTrak® for Servers Version 2.0.6.0 F Linux File System Agent

7.1.4 CimTrak Management Console (ID: VM3) Configuration Specifics

System VM3 is installed on a Virtual Machine located on System S1. The network interface card should be configured with the following IP Address assignment: 192.168.1.103.

7.1.4.1 Installed Components

OSs
• Microsoft Windows Server 2003 SP2 Enterprise Edition
• Microsoft Windows 2000 SP4
• Microsoft Windows Server 2008
• Microsoft Windows Vista
• Microsoft Windows XP SP3

Software:
• CimTrak® for Servers Version 2.0.6.0 F Management Console

7.1.5 CimTrak Master Repository (ID: VM4) Configuration Specifics

System VM4 is installed on a Virtual Machine located on System S1. The network interface card should be configured with the following IP Address assignment: 192.168.1.104.

7.1.5.1 Installed Components

OSs:
• Microsoft Windows XP SP3
• Microsoft Windows Server 2008
• Microsoft Windows 2000 SP4
• Microsoft Windows Server 2003 SP2
• Microsoft Windows Vista

Software:
• CimTrak® for Servers Version 2.0.6.0 F Master Repository
• PSPad Version 4.5.3 (2298)

7.1.6 Wireshark (ID: VM5) Configuration Specifics

System VM5 is installed on a Virtual Machine located on System S1. The network interface card should be configured with the following IP Address assignment: 192.168.1.105.

7.1.6.1 Installed Components

OSs:
• Microsoft Windows Server 2003 SP2 Enterprise Edition

• Microsoft Windows 2000 SP4
• Microsoft Windows Server 2008
• Microsoft Windows Vista
• Microsoft Windows XP SP3

Software:
• Wireshark Version 1.0.6

7.1.7 Microsoft Outlook 2000 (ID: VM6) Configuration Specifics

System VM6 is installed on a Virtual Machine located on System S1. The network interface card should be configured with the following IP Address assignment: 192.168.1.106.

7.1.7.1 Installed Components

OSs:
• Microsoft Windows Server 2003 SP2 Enterprise Edition
• Microsoft Windows 2000 SP4
• Microsoft Windows Server 2008
• Microsoft Windows Vista
• Microsoft Windows XP SP3

Software:
• Microsoft Outlook 2000

7.1.8 Microsoft Exchange Server (ID: VM7) Configuration Specifics

System VM7 is installed on a Virtual Machine located on System S1. The network interface card should be configured with the following IP Address assignment: 192.168.1.107.

7.1.8.1 Installed Components

OSs:
• Microsoft Windows Server 2003 SP2 Enterprise Edition
• Microsoft Windows 2000 SP4
• Microsoft Windows Server 2008
• Microsoft Windows Vista
• Microsoft Windows XP SP3

Software:
• Microsoft Exchange Server Version 5.0.2195.6713

7.1.9 CimTrak Network Device Agent (ID: VM8) Configuration Specifics

System VM8 is installed on a Virtual Machine located on System S1. The network interface card should be configured with the following IP Address assignment: 192.168.1.108.

7.1.9.1 Installed Components

OSs:
• Microsoft Windows Server 2003 SP2 Enterprise Edition
• Microsoft Windows 2000 SP4
• Microsoft Windows Server 2008
• Microsoft Windows Vista
• Microsoft Windows XP SP3

Software:
• CimTrak® for Servers Version 2.0.6.0 F Network Device Agent

7.1.10 CimTrak Network Device Agent (ID: VM9) Configuration Specifics

System VM9 is installed on a Virtual Machine located on System S1. The network interface card should be configured with the following IP Address assignment: 192.168.1.109.

7.1.10.1 Installed Components

OS:
• Red Hat Enterprise Linux Version 5.1

Software:
• CimTrak® for Servers Version 2.0.6.0 F Network Device Agent

7.1.11 Cisco Pix 501 Firewall Version 6.1(4) (ID: HW1) Configuration Specifics

Hardware HW1 is a physical hardware firewall attached to System S1 by an intermediary router. The firewall should be configured with the following IP Address assignment: 192.168.1.110.

7.1.11.1 Installed Components

• Cisco PIX Device Manager Version 1.1(2)
• Hardware: PIX-501, 16 MB RAM, CPU Am5x86 133 MHz
• Flash E28F640J3 @ 0x3000000, 8MB
• BIOS Flash E28F640J3 @ 0xfffd8000, 128KB
• Cisco- FOS version 6.0 or greater

7.1.12 Cisco 2612 (MPC860) processor (revision 0x00) (ID: HW2) Configuration Specifics

Hardware HW2 is a physical hardware router attached to System S1 by an intermediary router. The firewall should be configured with the following IP Address assignment: 192.168.1.111.

7.1.12.1 Installed Components

• Cisco 2612 (MPC860) processor (revision 0x00) with 61440K/4096K bytes of memory.
• Processor board ID JAD06300D65 (1605804976)
• M860 processor: part number 0, mask 49
• Bridging software.
• X.25 software, Version 3.0.0.
• Basic Rate ISDN software, Version 1.1.
• Cisco- IOS version 11.2 or greater

7.1.13 Juniper SRX210 (ID: HW3) Configuration Specifics

Hardware HW3 is a physical hardware router attached to System S1 by an intermediary router. The firewall should be configured with the following IP Address assignment: 192.168.1.112.

7.1.13.1 Installed Components

• Model: SRX210
• JUNOS Base OS boot [9.6R1.13]
• JUNOS Base OS Software Suite [9.6R1.13]
• JUNOS Kernel Software Suite [9.6R1.13]
• JUNOS Packet Forwarding Engine Support [9.6R1.13]
• JUNOS Routing Software Suite [9.6R1.13]
• JUNOS Online Documentation [9.6R1.13]
• JUNOS Crypto Software Suite [9.6R1.13]
• KERNEL 9.6R1.13 #0 built by builder on 2009-08-01 09:23:09 UTC

7.2 Developer Testing

The test procedures were written by the Developer and designed to be conducted using manual interaction with the TOE interfaces.

The Developer tested the TOE consistent with the Common Criteria evaluated configuration identified in the ST. The Developer's approach to testing is defined in the TOE Test Plan. The expected and actual test results (ATRs) are also included in the TOE Test Plan. The Developer testing effort thoroughly tested the available interfaces to the TSF. Each SFR has its own test, so many interfaces and security functions are repeatedly tested in the process and many actions exercise multiple SFRs. This results in SFRs and interfaces being tested more extensively than if a single test was written for each interface.

The evaluation team verified that the Developer's testing tested every aspect of every SFR defined in the ST. This analysis ensures adequate coverage for EAL 4. The evaluation team determined that the Developer's actual test results matched the Developer's expected test results.

7.3 Evaluation Team Independent Testing

The evaluation team conducted independent testing at Cimcor. The evaluation team installed the TOE according to vendor installation instructions and the evaluated configuration as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE while performing work unit ATE_IND.2-2. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Developer's Test Plan as a basis for creating the Independent Test Plan. The evaluation team analyzed the Developer's test procedures to determine their relevance and adequacy to test the security function under test. The following items represent a subset of the factors considered in selecting the functional tests to be conducted:

- Security functions that implement critical security features
- Security functions critical to the TOE's security objectives
- Security functions with open parameters (e.g. text fields, unbounded number fields)

The evaluation team reran 10 of the Developer's test cases and specified 8 additional tests. The additional test coverage was determined based on the analysis of the Developer test coverage and the ST.

Each TOE Security Function was exercised at least once and the evaluation team verified that each test passed.

7.4 Vulnerability Analysis

The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis and penetration tests.

The evaluators performed a vulnerability analysis of the TOE to identify any obvious vulnerabilities in the product and to determine if they are exploitable in the intended environment for the TOE operation. In addition, the evaluation team performed a public domain search for potential vulnerabilities. The public domain search did not identify any known vulnerabilities in the TOE as a whole or any components of the TOE.

Based on the results of the evaluation team's vulnerability analysis, the evaluation team devised penetration testing to confirm that the TOE was resistant to penetration attacks performed by an attacker with Enhanced-Basic attack potential. The evaluation team conducted testing using the

same test configuration that was used for the independent testing. In addition to the documentation review used in the independent testing, the team used the knowledge gained during independent testing and the design activity to devise the penetration tests. The penetration tests attempted to misuse components of the TOE (e.g., directly access the PostgreSQL database) and put the TOE in undefined states (e.g., unexpected storage space restrictions). This resulted in a set of five penetration tests all of which failed to circumvent the product security policies.

7.5 Follow-up Testing

After determining the vendors desire to include other windows operating systems in the evaluated configuration, the evaluation team developed another set of test procedures titled "Part Two". These procedures followed the same plan as above but with the following additional setup:

1. Install Microsoft Windows Vista on VM1 (File System Agent)
2. Install Microsoft Windows Vista on VM3 (Management Console)
3. Install Microsoft Windows Server 2008 on VM4 (Master Repository)
4. Install Microsoft Windows Vista on VM5 (Wireshark)
5. Do not follow the setup instructions for VM2, VM6, VM7, VM8, VM9, or network devices.

Once the steps in Section 6 of the vendor's test procedures have been completed, perform the following additional setup:

1. Install Cygwin on VM1.
2. Install the Management Console on VM3.

All tests were completed successfully on the additional operating systems.

8 Evaluated Configuration

The evaluated configuration consists of a Master Repository, a Management Console, File System Agents, and Network Device Agents. The Master Repository and Management console run on Windows 2000, XP SP3, 2003, Vista, or 2008. The File System Agents and Network Device Agents run on Windows 2000, Windows XP SP3, Windows 2003, Windows Vista, Windows 2008, or Linux Kernel 2.6 (Ubuntu, Redhat, CentOS, SuSE). The Network Device Agents can monitor Juniper - JunOS version 6.0 and above, Cisco - IOS version 11.2 and above, Cisco - FOS version 6.0 and above, and Cisco - ASA version 7.0 and above. The only additional hardware required is the network infrastructure that enables all of the components of the TOE to communicate.

The administrative user who installs the TOE must follow the installation and operational guidance provided in the "CimTrak Common Criteria Supplement Version 2.0.6.0 F, CimTrak Server / Repository, CimTrak Agent, CimTrak Management Console, CimTrak Network Device Agent" to achieve and remain in the Evaluated Configuration. The guidance requires the Administrator to configure repository encryption, session encryption, the password policy, and ensure the usage assumptions are achieved.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1R2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R2.

The Validators followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validators observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validators therefore conclude that the evaluation team's results that the TOE meets the security criteria in the Security Target, which specifies an assurance level of EAL 4 + ALC_FLR.2 are correct and complete.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the CIMCOR® CimTrak® Integrity Suite 2.0.6.0 F product meets the claims stated in the Security Target. The validation team also wishes to add the following notations about the use of the product. The following optional features of the product were not examined as part of this evaluation and their use will remove the product from the evaluated configuration:

- The Telnet protocol for Network Agent to Device communication
- The Master Repository FTP Interface
- Compliance Templates ("Compliances") (PCI, SOX, FISMA)
- The CimTrak Industrial Agent
- The Command Line Interface (CLI) for Security Management
- The Configuration Support Interface
- Agents used on the following operating systems:
    - Fedora-Linux
    - Apple-Macintosh
    - Sun Solaris
    - Hewlett Packard-HPUX

11 Security Target

The Security Target is identified as the CIMCOR® CimTrak® Integrity Suite 2.0.6.0 F Security Target EAL 4 augmented ALC_FLR.2, Version 1.2, June 9, 2010.

12 Glossary

The following abbreviations and terms are used throughout this document:

Administrators	Refers in a general sense to a CimTrak application user and therefore a user holding at least one of three available roles: Administrator, Standard user, Auditor.
Administrator	Refers to the Administrator role specifically, as contrasted with the Administrators designation above.
AES	Advanced Encryption Standard
Agent	Refers to both Filesystem Agent and Network Agent components installed as part of the CimTrak application. Where "Filesystem" or "Network" does not precede an agent description, it denotes that the content relates to both Agent types.
Agent Server	Refers to the server platform upon which a Filesystem Agent is installed.
ASA	(Cisco) Adaptive Security Appliance
Authoritative Copy	Refers to a saved copy of "locked" User data stored in the Master Repository for the purpose of restoring files to the last known approved state.
Client	As referenced in the Management Console subsystem, Client Core subsystem, the client in this instance refers to the management console machine.
DLL	Dynamic Link Library
External Entities	Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.
Intrusion	Refers to an event in which there was an unexpected or unauthorized change to a file/object group, monitored by the CimTrak application.
Filesystem Agent	Refers to the component of the CimTrak application which is installed on servers within the network to allow the CimTrak application to monitor selected (locked) files, implement corrective action based on detected changes and collect local audit data on behalf of the Master Repository where audit data is stored.
FIPS	Federal Information Processing Standard
FOS	(Cisco) Firewall Operating System

GUI	Graphic User Interface
Heartbeat	Refers to an acknowledgement message sent by the CimTrak Agent to the CimTrak Master Repository at established intervals to assure that the Agent is present and operational.
HMAC	Hashed Message Authenticated SHA1 hash
IOS	(Cisco) Internetwork Operating System
JUNOS	Juniper Operating System
Locked Files	Refers to files that are protected on Agent server/Network Host server machines by the CimTrak application. This also connotes that changes to these files are detected by the TOE and that remediation measures, including replacement with an authoritative copy, may be taken as configured by the Administrator.
Monitoring Parameters	Refers to the CimTrak feature which allows the monitoring of CPU, Memory and Disk usage of Agent Machines and the triggering of an Alarm if a configured threshold is reached.
Master Repository	Refers to the main CimTrak application which includes server functionality used to communicate with Agent components, security management components for application configuration and databases used for storage of TSF and User Data.
Management Console	Refers to the component of the CimTrak application that is installed on an [Administrator] Workstation to provide access to the Master Repository for the purpose of configuring the application and reviewing detected security events and remediation taken by the TOE application.
NDIM	Network Device Interaction Module
Network Agent	Refers to the component of the CimTrak application which is installed on dedicated Host Servers within the network to allow the CimTrak application to monitor selected (locked) configuration data from Network Devices, implement corrective action based on detected changes and collect local audit data on behalf of the Master Repository where audit data is stored.
Network Agent Server	Refers to the dedicated Network Host platform upon which the Network Agent is installed.
ODBC	Open DataBase Connectivity

"Private Key" feature	The "Private Key" feature allows an Administrator to apply a secondary encryption key to specific Agents or Database Object, thus requiring a passphrase be entered prior to granted access to the Agent data or object. This secures data from other [Administrators] who do not know the passphrase required to view or access the data. This is either applied at Installation time (Agent based) or during Management Console sessions (Object based).
Polling monitor	Refers to the detection mechanism employed by CimTrak network agents to detect changes made to network devices.
RNG	Random Number Generator
SQL	Structured Query Language
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functionality
User Data	Refers to data stored on Agent server machines within the Operational Environment which is protected by the TOE's security functionality and, when so configured, is stored as an authoritative copy within the TOE Master Repository.
VB	Visual Basic

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1.) Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2006, version 3.1, revision 1.

2.) Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2007, version 3.1, revision 2.

3.) Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2007, version 3.1, revision 2.

4.) Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2007, version 3.1, revision 2.

5.) CIMCOR® CimTrak® Integrity Suite 2.0.6.0 F Security Target EAL 4 augmented ALC_FLR.2, Version 1.2, June 9, 2010.

6.) Evaluation Technical Report for CIMCOR® CimTrak® Integrity Suite 2.0.6.0 F. 09-1501-R-0084 V1.2, July 26, 2010.