National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Tripwire Enterprise, version 5.2

Report Number: **CCEVS-VR-VID10123-2009**

Dated: **3 April 2009**

Version: **1.0**

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

Mr. Daniel P. Faigin
Mr. Kenneth Elliott III
The Aerospace Corporation
El Segundo, California and Columbia, Maryland

Common Criteria Testing Laboratory

SAIC, Inc.
Columbia, Maryland

Table of Contents

1 EXECUTIVE SUMMARY

The evaluation of **Tripwire Enterprise, version 5.2** was performed by SAIC in the United States and was completed in March 2009. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Tripwire TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3 and International Interpretations effective on 30 September 2006. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3

Science Applications International Corporation (SAIC) determined that the evaluation assurance level (EAL) for the product is EAL 3 family of assurance requirements augmented with ALC_FLR.2. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Tripwire, Inc. Tripwire Enterprise Security Target.

This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided. This Validation Report is not an endorsement of the Tripwire product by any agency of the US 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 for Tripwire Enterprise, version 5.2 (ETR) Parts 1 and 2 produced by SAIC.

1.1 Evaluation Details

Evaluated Product:	Tripwire Enterprise, version 5.2
Security Target:	Tripwire, Inc. Tripwire Enterprise Security Target, Version 1.0, April 2, 2009
Sponsor & Developer:	Tripwire, Inc 326 SW Broadway, 3rd Floor Portland, OR 97205
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Completion Date:	April 3, 2009
CC:	Common Criteria for Information Technology Security

	Evaluation, Version 2.3
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation, Version 2.3
Evaluation Class:	EAL 3 augmented with ALC_FLR.2
Description	The TOE is a change audit assessment product that can assure the integrity of critical data on a wide variety of servers and network devices (e.g., routers, switches, firewalls, and load balancers) called nodes. It does this by monitoring system status, configuration settings, file content, and file metadata on the nodes and checking it against previously stored node data to detect modifications. The TOE consists of a server application component (Tripwire Enterprise Server), a client application component (Tripwire Enterprise Agent), and a client administrative console application component (Tripwire CLI application). The evaluated configuration of the TOE is a specific configuration that was used in conducting the Common Criteria evaluation of the TOE. The evaluated configuration consists of Tripwire Enterprise Server, and Tripwire Firebird Database (part of the IT environment) running on the same machine. The evaluated configuration also includes one or more Tripwire Enterprise Agents running on separate platforms (either machines or devices) in the IT environment.
Disclaimer	The information contained in this Validation Report is not an endorsement of the Tripwire product by any agency of the U.S. Government and no warranty of the Gatekeeper product is either expressed or implied.
PP:	None
Evaluation Personnel	Shukrat Abbas Quang Trinh
Validation Team:	Daniel P. Faigin Kenneth Elliott III

1.2 Interpretations

The Evaluation Team determined that there were no NIAP Interpretations applicable to this evaluation.

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

- An authorized user may incorrectly change TOE data or functions they are authorized to modify.
- An attacker may be able to inappropriately change attribute information for targeted objects.
- An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
- An attacker may be able to gain unauthorized access to data collected from targeted objects.

2 IDENTIFICATION

The product being evaluated is Tripwire Enterprise, version 5.2.

3 SECURITY POLICY

3.1 Change Audit Assessment

The Tripwire Enterprise Agent component of the TOE can collect object attribute information for files, directories, registry keys and registry key values. By comparing collected information against saved values, the agent monitors these resources to detect changes. Once detected, the agent reports the detected change to the Tripwire Enterprise Server to allow administrator specified actions to occur.

For Agentless nodes, the Tripwire Enterprise Server component collects attribute information, compares the information to baselines and initiates administrator specified actions. The Tripwire Enterprise Server can monitor files on Agentless nodes, command output from agentless nodes, and network availability using interfaces that each node provides.

The Tripwire Enterprise Server component can perform actions in response to object attribute comparisons, specifically: displaying integrity check results to the console, sending integrity check results to administrators using email, sending integrity check results to administrators using SNMP, sending a log message to a Syslog server, executing a command on the Tripwire Enterprise Server host operating system, executing a command on the Tripwire Enterprise Agent host operating system, and promoting new element versions to be a baseline. For some Agentless node types, Tripwire Enterprise Server can also restore a changed element to its baseline state on the Agentless node.

3.2 Security Audit

The TOE provides its own audit mechanism, with its own audit trail, that can generate audit records containing integrity check results and TOE management actions. The TOE refers to audit records as ‘log messages” and to the audit trail as the “message log”. These terms are interchangeable. The TOE stores the “message log” in the Firebird Database.

The TOE provides administrators the ability to manage the Tripwire Enterprise Server audit trail using administrator console interfaces. Administrators can read, search and sort log messages in the audit trail based on date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

3.3 User Data Protection

The TOE implements three security objects: user sessions, nodes, and node groups. The user session is the only object that is also a subject. Nodes and node groups are definitions of network entities upon which some integrity check operation is to be performed. Examples of the information the Tripwire Enterprise Server retains about a node or node group are a name, the type of node(s), a description, the number of elements being checked, and last check date/time.

Access to subjects and objects is controlled by the Discretionary Access Control (DAC) policy for all available operations on nodes and node groups (and their contents). Node objects have ACLs that can specify user, user group, and role access permissions. These attributes are compared against user identities and roles of subjects in order to determine whether requested operations should be allowed. If the access checks fail, access will be refused. Only the administrator role can access the user session subject.

3.4 Identification and Authentication

The TOE defines user identities, authentication data, user groups, and role information. The TOE offers no TSF-mediated functions until the user is authenticated. The TOE offers no TSF-mediated functions until the user is identified.

3.5 Security Management

Tripwire Enterprise Server offers a graphical user interface (GUI), and a command line interface (CLI). The TOE restricts the ability to execute commands by restricting access to these user interfaces, by enforcing user permissions, and by assigning roles to users.

A user permission is a system authorization that enables a user with that permission to view, add, change, or delete data in Tripwire Enterprise. Common types of user permissions load permissions (which provide read-only access to a class of Tripwire Enterprise objects and groups), create permissions (permitting creation of objects and groups), delete permissions, update permissions, and manage permissions.

Tripwire Enterprise includes five default user roles, all of which are considered to be trusted accounts. A user role is a collection of user permissions that may be assigned to a user. The default user roles are Administrator, Power User, Regular User, Monitor User, and User Administrator. Four of these are organized hierarchically: Administrator > Power User > Regular User > Monitor User). The User Administrator role is orthogonal to the other roles and has permissions to manipulate user accounts.

3.6 TSF protection

Users of Tripwire Enterprise can access commands only through one of the two administration interfaces provided. The TOE only accepts commands through these interfaces, ensuring that command are processed only within the TE Server (and thus, the TOE's enforcement of access control cannot be bypassed). The TOE uses the SSL protocol provided by the IT environment to protect the communication between the agent and the server.

The TOE relies on the underlying operating system to provide the abstraction of a process. The TOE uses one process for the execution of the Tripwire Enterprise Server. The Firebird database (in the IT environment) operates in its own process. Additional subordinate processes may be created by the Tripwire Enterprise Server to perform independent tasks; however, this process structure is not related to Tripwire Enterprise Server enforcement of internal user roles. The Firebird Database in the IT environment is relied upon to store, retrieve and protect data which it handles such that only the Tripwire Enterprise Server can access TOE data in the database.

The Tripwire Enterprise Server is a Java program that runs on its own JVM. The JVM is provided as part of the TOE installation process, as a distinct product, but is not part of the TOE. The TOE itself distinguishes actions of TOE users within the TOE by associating users with threads running within the JVM. The TOE does not provide a general programming interface to TOE users. The JVM also provides the actual implementation of SSL (i.e., TLSv1). References to the TOE using SSL mean that the TOE is using the JVM SSL implementation.

Agentless nodes provide an interface conformant with their security model for external access to the data objects that the TOE monitors. The TOE complies with that security model in accessing the objects (e.g., by providing login credentials required by the agentless nodes using supported network protocols such as SSH or telnet). For agentless nodes that do not support SSH based protocols for login, it is expected that those responsible for managing the agentless nodes have taken steps to secure the communication pathways between the TOE and the agentless nodes per their security environment. The TOE does not rely upon the security of these communication pathways to agentless nodes for TOE's self protection.

The Tripwire Enterprise Server and Tripwire Enterprise Agent components of the TOE configure and use the SSL provided to them by the JVM upon which they are running. Both the server and agent configure their JVM to require a mutually authenticated SSL connection be established for all communications between the server and agent. This allows these components of the TOE to use the RMI protocol to exchange services.

The TOE also uses the JVM provided SSL to protect the confidentiality and integrity of its communication with the users of the GUI and CLI. This protects the data, including TOE user names and passwords, from manipulation and observation.

4 ASSUMPTIONS

The following assumptions have been made about the use of the TOE.

4.1 Intended Usage Assumptions

- The TOE has access to all of the IT Systems (nodes) and data within those IT Systems that it is configured to monitor.
- The TOE is appropriately scalable1 to the IT Systems it is configured to monitor.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT Systems the TOE monitors.
- The host on which the TE server component of the TOE resides does not provide a general purpose computing environment to untrusted users.

4.2 Physical Assumptions

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.
- Those responsible for managing the agentless nodes have taken steps to secure the communication pathways between the TOE and the agentless nodes per their security environment.

4.3 Personnel Assumptions

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

[1] Appropriately scalable refers to the TOE being able to handle the volume of processing or traffic flow for systems which it is monitoring.

- Only authorized users can access the TOE.

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; and meets them with only a certain level of assurance (EAL 3 augmented with ALC_FLR.2 in this case).
2. As with all EAL 3 evaluations, this evaluation did not specifically search for vulnerabilities that were not "obvious" (as this term is defined in the CC and CEM); seriously attempt to find counters to them; nor find vulnerabilities related to objectives not claimed in the ST.
3. The use of AAA monitoring tool and the external authentication server are excluded in the evaluated configuration.
4. It is important to note that the Firebird Database and the Java Virtual Machine were not covered by this evaluation.

5 ARCHITECTURAL INFORMATION

The TOE is a change audit assessment product that can monitor the integrity of critical data on a wide variety of servers and network devices (e.g., routers, switches, firewalls, and load balancers) called nodes. It does this by gathering system status, configuration settings, file content, and file metadata on the nodes and checking gathered node data against previously stored node data to detect modifications.

The TOE consists of a server application component (Tripwire Enterprise Server), a client application component (Tripwire Enterprise Agent), and a client administrative console application component (Tripwire CLI). The product is also bundled with a database application (Firebird Database) to support the product's storage needs. The Firebird Database is considered part of the IT environment. While the product supports using the Firebird Database and the Tripwire Enterprise Server (TE Server) on different machines, they must run on the same machine in an evaluated configuration. The other TOE components can run on different machines in various combinations. The Tripwire Enterprise Server is the only product installed and active on the machine in which it is running.

There are two classes of nodes that the TOE can monitor, those with built-in external administration interfaces and those without. Examples of the kind of node with built-in administration interfaces are firewalls, routers, switches, load balancers, etc.. Some of these external interfaces use web servers and allow administration via a remote web browser, and others provide command line interfaces or other custom protocols. These nodes are referred to as agentless nodes.   Examples of nodes without built-in administration interfaces are Microsoft Windows systems and UNIX systems (Solaris, AIX, HP-UX, etc.)   These nodes are referred to as agent nodes, and host an installation of Tripwire Enterprise Agent.

The Tripwire Enterprise Agent provides an interface for Tripwire Enterprise Server where none otherwise exists or to provide a more fully featured interface than an existing one. Tripwire Enterprise Agents are installed on nodes that run server-type operating system.

The TOE may also be used to monitor the configuration of its nodes, thereby identifying changes made by users or other applications, such as software-provisioning and patch-management tools that run independently of Tripwire Enterprise.

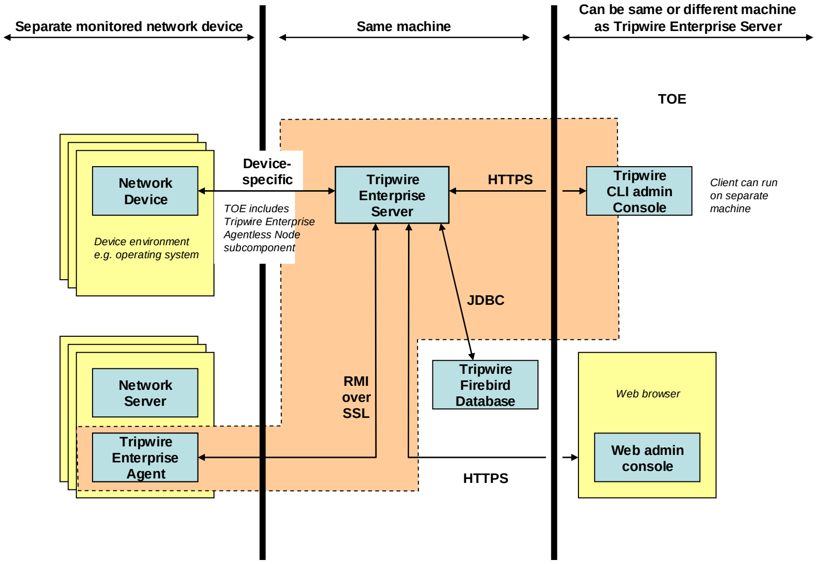
Separate monitored network device
Same machine
Can be same or different machine as Tripwire Enterprise Server
TOE
Network Device
Device environment e.g. operating system
Device-specific
TOE includes Tripwire Enterprise Agentless Node subcomponent
Tripwire Enterprise Server
HTTPS
Tripwire CLI admin Console
Client can run on separate machine
JDBC
Network Server
Tripwire Enterprise Agent
RMI over SSL
Tripwire Firebird Database
Web browser
Web admin console
HTTPS

Figure 1: TOE boundary

The Tripwire Enterprise Server component delegates work to Tripwire Enterprise Agents, interacts with agentless nodes, analyzes information, and provides a web-based user interface (or a network interface that provides limited functionality using the Tripwire CLI application component as an alternative to a web browser) for managing the TOE installation. The Tripwire Enterprise Server component is composed of five main subcomponents:

1. User Interface (UI)
2. Downloadable Agent Code
3. Database Mapping Layer
4. Remote Method Invocation (RMI) Layer
5. Agentless Node device-specific interface

The User Interface (UI) subcomponent provides two interfaces for other programs that provide access to the administrators of the system; a graphical user interface (GUI) called the Tripwire Enterprise Web Admin Console and a command line interface (CLI) called the Tripwire CLI. They will be referred to in this document as the GUI and CLI, respectively.

The UI's GUI is a web server running in the TOE for use by an external web browser. The web browser is not part of the TOE. The connection between the web browser and the GUI uses HTTPS to protect the integrity of the connection. The GUI provides an administrator the ability to perform such functions as add users, configure and schedule integrity checks, manage nodes, and view reports. User identification and authentication is handled through the GUI.

The UI's CLI provides an interface for scripts to perform a limited number of operations on the TOE. Its functionality is a subset of the GUI's and is insufficient to fully administer the TOE. For example, there are no CLI commands for adding or deleting users or changing passwords. The CLI provides administrator access to the Tripwire Enterprise Server. Like the GUI interface, the CLI connects to the Tripwire Enterprise Server using HTTPS[2].

The Tripwire Enterprise Server utilizes the SSL mechanism provided by the JVM in the IT environment as part of the HTTPS communication with the GUI and the CLI.

The TOE also uses RMI (Remote Method Invocation) over mutually authenticated SSL network connections to protect intra-TOE communication between Tripwire Enterprise Server and the Tripwire Enterprise Agents over an untrusted network.

The Evaluated Configuration includes components running in the TOE boundary and components running outside the TOE boundary. Inside the TOE boundary are Tripwire Enterprise Server, and the Tripwire CLI running on a single computer, and one or more Tripwire Enterprise Agents running on remote servers.

The TOE relies upon the IT environment for the following:

- **Host Operating System**. The operating system provides process-related (e.g., time) and network-related (e.g., name resolution) services for the JVM. One of the following:
  - Windows 2000, XP Professional, 2003
  - Solaris 7, 8, or 9
  - Red Hat Enterprise Linux 3 & 4
- **Firebird Database**. Stores data for Tripwire Enterprise Server.
  - Version 1.0.3 for Windows and Red Hat Enterprise Linux
  - Version 1.0.0 for Solaris
- **Java Virtual Machine**. Provides a runtime environment for the TOE.
  - Sun Microsystems JVM 1.4.2_08

[2] The Tripwire Enterprise Server uses the SSL provided by the IT Environment for HTTPS communications.

- **SMTP Server**. An email server is used to facilitate delivery of integrity check results to administrators when the TOE is so configured.
- **SNMP recipient**. A network management device is used to facilitate delivery of integrity check results to administrators when the TOE is so configured.
- **Syslog Server**. A destination for the collection of log messages sent by the TOE.
- **Servers supporting Tripwire Enterprise Agents**:
    - Windows 2000, XP Professional, 2003
    - Solaris 8, 9, 10
    - Red Hat Enterprise Linux 3 & 4, SUSE Enterprise Server 9
    - HP-UX 11.0, 11i v1, 11i v2
    - AIX 5.1, 5.2, 5.3
- **Agentless Nodes:**
    - Alcatel OmniSwitch
    - Cisco Catalyst Routers & Switches
    - Cisco IOS Routers & Switches
    - Cisco PIX Firewall
    - Cisco VPN Concentrator
    - Extreme
    - F5 BigIP
    - Foundry
    - HP ProCurve M & XL
    - Juniper M/T Series
    - Marconi ASX
    - NetScreen
    - Nokia IPSO Firewall
    - Nortel Passport & Alteon
    - POSIX compliant UNIX systems

6 DOCUMENTATION

The following documentation was used as evidence for the evaluation of the TOE. Documents that are publically available are shown in **boldface**.

6.1 Design documentation

Document	Revision	Date
Tripwire Enterprise v5.2 Design Document (HLD, FSP, and RCR)	3.7	2009-03-24
Tripwire Enterprise 5.2 User Guide, TW1031-11	-	-
Tripwire Enterprise 5.2 Reference Guide, TW1092-02	-	-

6.2 Guidance documentation

Document	Revision	Date
Tripwire Enterprise 5.2 User Guide, TW1031-11	-	-
Tripwire Enterprise 5.2 Reference Guide, TW1092-02	-	-
Tripwire Enterprise Installation Guide 5.2, TW1032-12	-	-
Tripwire Enterprise 5.2 Release Notes Addendum		March 2009

6.3 Configuration Management and Lifecycle documentation

Document	Revision	Date
Tripwire, Inc. Tripwire Enterprise 5.2, Tripwire for Servers 4.6, Tripwire Manager 4.6 Configuration Management Plan, TW-ACM1-03	0.3	2007-09-21
Tripwire, Inc. Tripwire Enterprise 5.2, Tripwire for Servers 4.6, Tripwire Manager 4.6 Lifecycle, TW-ALC1-03	0.3b	2007-09-21

6.4 Delivery and Operation documentation

Document	Revision	Date
Tripwire Manager and Tripwire for Servers Delivery Procedures Delivery Procedures, TW-TFSADO1-08	0.8	2007-09-25
Tripwire Enterprise Installation Guide 5.2, TW1032-12	-	-
Tripwire Enterprise 5.2 Release Notes Addendum		March 2009

6.5 Test documentation

Document	Revision	Date
Tripwire Inc. Tripwire Enterprise 5.2 Common Criteria Test Plan, TW-TETP1-01	1.1	2008-01-09
TW-TETP1-01 10-8-07 TE_5 2_common_criteria_test cases.xls	-	2007-08-07
Test case zip (The table in ATE_COV.2-1 identifies the test cases that evaluation team found applicable.)	-	-

6.6 Vulnerability Assessment documentation

Document	Revision	Date

Tripwire Enterprise version 5.2 Vulnerabilities Assessment, TW-TEAVA1-01	0.1	2007-10-25
Tripwire, Inc. Tripwire Enterprise Strength of Function Analysis, TW-TFSSOF1-01	0.1	2008-04-09

6.7 Security Target

Document	Revision	Date
Tripwire, Inc. Tripwire Enterprise Version 5.2 Security Target	1.0	2009-04-02

7 IT PRODUCT TESTING

The evaluation team applied each EAL 3 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the functional specification and as stated in the TOE security functional requirements.

First the evaluation team analyzed the vendor-provided test plan and test procedures. While a number of tests were directed at the server, there were also tests developed specifically for each of the identified devices in order to test the full range monitoring capabilities available for that device. Through analysis the evaluation team confirmed that the claimed security functions were fully addressed via the available test plan and procedures.

The vendor ran the entire test suite using both Unix and Windows[3] hosts, in accordance with the test plan, for the server and targeting each of the applicable agents and also agentless network devices as follows:

- Windows
- Solaris
- Red Hat Enterprise Linux
- SUSE Linux
- HP-UX
- AIX
- Alcatel OmniSwitch
- Cisco Catalyst Routers & Switches
- Cisco IOS Routers & Switches

[3] Note that while the server can be installed on multiple Unix-type platforms, on Red Hat Enterprise Linux was used since the server is a Java application and each of the applicable operating systems utilize the same version of the supporting JVM.

- Cisco PIX Firewall
- Cisco VPN Concentrator
- Extreme
- F5 BigIP
- Foundry
- HP ProCurve M
- HP ProCurve XL
- Juniper M/T Series
- Marconi ASX
- NetScreen
- Nokia IPSO Firewall
- Nortel Passport
- Nortel Alteon
- POSIX compliant UNIX systems

The vendor delivered the actual test results (for each of the applicable devices along with test results of non-device specific functions of the server) for both the Unix and Windows hosted server instances to the evaluation team for analysis.

Subsequently, the evaluators developed their own test plan including plans to repeat some developer tests, develop some independent test cases, and to perform vulnerability analysis and penetration testing commensurate with EAL3.

Ultimately, the evaluation team repeated about 45% of the developer test procedures, including tests procedures directed at a little over 30% of the applicable devices including 2 agents and 6 agentless devices. The evaluators achieved results consistent with expectations based on their analysis.

The evaluators then developed some additional independent tests, based on the evaluation and also on some vulnerability analysis (including a public search for potential vulnerabilities). Independent functional tests were devices for each security function and yielded expected results. No vulnerabilities in the TOE were found during a search of vulnerability databases and tests devised from postulated vulnerabilities in the I&A mechanism.

8 RESULTS OF THE EVALUATION

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

9 VALIDATOR COMMENTS/RECOMMENDATIONS

1. The TOE does not provide an interface for individual users to change password. Password are changed by the administrator with the appropriate permissions to modify the user accounts.
2. While the TOE includes the capabilities to generate and review audit records, it provides no mechanisms (e.g., an alert) to handle exceptions that might occur when the available audit storage space becomes exhausted. The available space is based that available to the associated database. Once that database runs out of available storage space it can no longer accept audit records (including monitored events) and the TOE will essentially fail due to its inability to successfully record any new events.
3. The TOE requires the use of passwords and while there is guidance provided regarding the selection of suitably strong passwords, the TOE provides no mechanisms to actually restrict (e.g., length, complexity) the set of allowable passwords.
4. The TOE makes use of a Firebird Database in order to store audit and other collected data. The Firebird Database is an open source product that is installed during TOE installation.
5. For this evaluation, it was appropriate for the Security Target to claim compliance with the external standards for MD5 and SHA-1 for the definition of the encryption algorithm. There are many ways of determining compliance with a standard. Tripwire has chosen to make a developer claim of compliance. This means that there has been no independent verification (by either the evaluators or a third party standards body, such as a FIPS laboratory) that the implementation of the cryptographic algorithms actually meets the claimed standards. Potential users of this product should confirm that the cryptographic capabilities are suitable to meet the user's requirements.

10 ANNEXES

Not applicable.

11 SECURITY TARGET

The security target for this product’s evaluation is **Tripwire, Inc. Tripwire Enterprise Version 5.2 Security Target**, version 1.0, April 2, 2009.

12 GLOSSARY

There were no definitions used other than those used in the CC or CEM.

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 August 2005, Version 2.3.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, Version 2.3.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 2005, version 2.3.

[7] Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R

[8] Evaluation Technical Report for Tripwire Enterprise version 5.2 Part II, version 1.0, April 2, 2009

[9] Tripwire, Inc. Tripwire Enterprise Security Target, version 1.0, April 2, 2009.

[10] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001