National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Tripwire Enterprise, Version 8.1 with the 8.1.2.5 patch

Report Number: CCEVS-VR-10462-2012
Dated: August 31, 2012
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin
The Aerospace Corporation

Jean Hung
The MITRE Corporation

Common Criteria Testing Laboratory

James Arnold
Julie Cowan
Neal Haley
Quang Trinh
SAIC, Inc.
Columbia, MD

Table of Contents

List of Figures

List of Tables

1 EXECUTIVE SUMMARY

The evaluation of **Tripwire Enterprise, Version 8.1 with the 8.1.2.5 patch** was performed by Science Applications International Corporation (SAIC) in the United States and was completed in June 2012. 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 Target of Evaluation (TOE) was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3 and the Intrusion Detection System System Protection Profile (IDSSYPP), Version 1.7, July 25, 2007. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.

SAIC determined that the evaluation assurance level (EAL) for the product is EAL2 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 Version 8.1 Security Target, Version 1.1, July 13, 2012.

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 National Information Assurance Partnership (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, Inc. Tripwire Enterprise Version 8.1 (ETR) Parts 1 and 2 produced by SAIC.

The Tripwire Enterprise, Version 8.1 with the 8.1.2.5 patch TOE is an intrusion detection system consisting of a sensor, scanner, and analyzer to monitor IT systems for activity that may indicate inappropriate activity on the IT system. The TOE is an attribute change assessment product that also reconciles the changes against existing management systems and policies. The TOE provides three main capabilities: File Integrity Monitor, Compliance Policy Manager, Remediation Manager and is composed of Server and Agent components and utilizes or otherwise accesses numerous components in its operating environment.

The Tripwire Enterprise Server can be installed on the following platforms which are in the operating environment: Windows Server 2003 (SP1, SP2) & R2 (32-bit & 64-bit); Windows Server 2008 (SP1) & Server Core (32-bit & 64-bit); Windows Server 2008 R2 (64-bit); Solaris 10 Global & Non-Global Zone (SPARC); Red Hat Enterprise Linux 5.2, 5.3, 5.4, 5.5, 5.6, and 6.0 (x86 and x64); and, SUSE Linux Enterprise Server 10.2 and 11.1 (x86 and x64).

Tripwire Enterprise installs the following Java Virtual Machine (JVM) for use by the TOE on these platforms (this JVM is in the operating environment): Sun Microsystems JVM v1.5.0 for AIX and HP-UX agents and v1.6.0.u24 for all other platforms.

Tripwire Enterprise (TE) supports the following backend DBs which are in the operating environment: MySQL v5.1.49 (Bundled with TE); Structured Query Language (SQL) Server 2005 SP2; SQL Server 2008, 2008 R2; and, Oracle 10g, 11gR1, 11gR2.

The Tripwire Enterprise Web Admin Console supports Firefox 3 or later browsers.

Tripwire Enterprise Agents are installed on file servers and desktops. These nodes are the supported systems/platforms that can be monitored by the TOE. The Tripwire Enterprise Agents can be installed on the following file servers which are in the operating environment: Windows Server 2003 (Service Pack 2) (x86 and x64); Windows Server 2008 (x86 and x64); Windows Server 2008 Core (x86 and x64); Windows Server 2008 R2 (x64); Solaris 9 (UltraSPARC ii); Solaris 10 Global & Non-Global Zone (UltraSPARC ii, x86 and x64); Red Hat Enterprise Linux 4 update 7 (x86 and x64 Editions); Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 6 (x86 and x64 Editions); Red Hat Enterprise Linux 5.2, 5.3, 5.4, 5.5 (PAE kernel); SUSE Linux Enterprise Server 9.2, 10.2, 11.0, 11.1 (x86 and x64 Editions); Cent OS 5.2, 5.4, 5.5 (x86 and 64 Editions); Fedora Core 10; HP-UX 11iv1, v2, v3 (PA-RISC); HP-UX 11iv2, v3 (Itanium); AIX 5.2, 5.3 & 6.0 (64-bit); and, AIX 5.3 (32-bit).

The Tripwire Enterprise Agents can be installed on all versions of the following operating systems which are in the operating environment: Windows 2000 Professional (Service Pack 4, update 1); Windows XP Professional (Service Pack 3) (x86); Windows Vista (Service Pack 1) (x86 and x64); and, Windows 7 (x86 and x64).

The TOE is dependent on the correct operation of the operating environment, including the components identified above, none of which are included within the scope of the evaluation.

The TOE, when configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in the Tripwire, Inc. Tripwire Enterprise Version 8.1 Security Target.

2 IDENTIFICATION

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a National Security Agency (NSA) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by 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 granted by the National Institute of Standards and Technology (NIST).

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation 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 (PP) to which the product is conformant (if any);

- The organizations and individuals participating in the evaluation.

Table 1. Evaluation Details

Evaluated Product:	Tripwire Enterprise, Version 8.1 with the 8.1.2.5 patch
Sponsor:	Tripwire, Inc. 101 SW Main Street, Suite 1500 Portland, OR 97204
Developer:	Tripwire, Inc. 101 SW Main Street, Suite 1500 Portland, OR 97204
CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	12 July 2011
Completion Date:	July 2012
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 3
Evaluation Class:	EAL 2 augmented with ALC_FLR.2
Description:	The TOE is an intrusion detection system consisting of a sensor, scanner, and analyzer to monitor Information Technology (IT) systems for activity that may indicate inappropriate activity on the IT system. The TOE is an attribute change assessment product that also reconciles the changes against existing management systems and policies. The TOE provides three main capabilities: File Integrity Monitor, Compliance Policy Manager, Remediation Manager.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Tripwire Enterprise, Version 8.1 with the 8.1.2.5 patch by any agency of the U.S. Government and no warranty of the Tripwire Enterprise, Version 8.1 with the 8.1.2.5 patch is either expressed or implied.
PP:	Intrusion Detection System System Protection Profile (IDSSYPP), Version 1.7, July 25, 2007

Evaluation Personnel: Science Applications International Corporation:

James Arnold
Julie Cowan
Neal Haley
Quang Trinh

Validation Body: National Information Assurance Partnership CCEVS

2.1 Interpretations

Not applicable.

3 SCOPE OF EVALUTION

3.1 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter.

- An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
- An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
- An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
- An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
- An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
- An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
- An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
- Unauthorized attempts to access TOE data or security functions may go undetected.
- Improper security configuration settings may exist in the IT System the TOE monitors.
- Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
- Vulnerabilities may exist in the IT System the TOE monitors.
- The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

- The TOE may fail to recognize vulnerabilities or inappropriate activity based on Intrusion Detection System (IDS) data received from each data source.
- The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
- Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
- Inadvertent activity and access may occur on an IT System the TOE monitors.
- Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.2 Organizational Security Policies

The ST identifies the following organizational security policy that the TOE and its operating environment are intended to fulfill:

- Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

  This policy effectively supports the implementation of a system monitoring policy, as specified by NIST SP 800-53 Revision 3 control SI-4.
- Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
- The TOE shall only be managed by authorized users.

  This policy effectively supports both account management (AC-2) and access control (AC-3) controls in NIST SP 800-53 Revision 3. It does this by enforcing the requirements that external authorization is required to perform management functions, and that the system restricts use of those management functions to only authorized individuals
- All data collected and produced by the TOE shall only be used for authorized purposes.
- Users of the TOE shall be accountable for their actions within the IDS.

  This policy effectively support the implementation of an audit and accountability policy, as specified by NIST SP 800-53 Revision 3 controls AU-1 and AU-2.
- Data collected and produced by the TOE shall be protected from modification.
- The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

3.3 Physical Scope

The evaluated product is **Tripwire Enterprise Server, Version 8.1 with the 8.1.2.5 patch**.

The TOE is a software only TOE. All hardware used to deploy the TOE is in the operational environment.

This table identifies software components and indicates whether or not each component is in the TOE.

TOE or Environment	Component	Description
TOE	Tripwire Enterprise Server, Version 8.1 with the 8.1.2.5 patch	Analyzes collected information from Tripwire Enterprise nodes
TOE	Tripwire Enterprise Agent, Version 8.1	Collects information from monitored servers for the Tripwire Enterprise Server
TOE	Event Generator	An auditing utility that can be installed with Tripwire Enterprise (TE) Agent on some Windows and UNIX file servers.
TOE	Tripwire Command Line Interface (CLI) Admin Console	A utility that allows TE functions to be executed using a command line, without using the TE Graphical User Interface (GUI).
TOE	Change-Audit License	A license certificate that activates the TE change auditing for a single monitored system of a specific type.
TOE	Configuration-Assessment License	A license certificate that enables TE to run policy tests on a single node. To generate policy test results for a node, the node must have valid Change-Audit & Configuration-Assessment licenses.
TOE	Automated-Remediation License	A license certificate that enables TE to remediate policy tests on a single file server node. To automatically remediate failed policy tests for a node, the node must have valid Change-Audit, Configuration-Assessment, and Automated-Remediation licenses.
Environment	JVM Version 1.6.0	The Java Virtual Machine provides a Transport Layer Security (TLS) v1 implementation for communications between the TOE and remote trusted IT entities.
Environment	TE Server OS (See below for additional details)	The operating system on which the TE Server is installed
Environment	Backend DB (See below for additional details)	The database used by TE server to store all data.

TOE or Environment	Component	Description
Environment	TE Node (See below for additional details)	A server or network device being monitored.
Environment	Lightweight Direct Access Protocol (LDAP) or Active Directory Server	An authentication server that is required only if the LDAP/Active Directory System login method is selected.

3.3.1 Required non-TOE hardware/software/firmware

The TOE depends upon the required platforms identified below that are in the TOE environment.

The TOE relies upon the following software in the local[1] operational environment of the Tripwire Enterprise Server or the Tripwire Enterprise Agent.

- Java Virtual Machine – provides a runtime environment for the TOE.

The TOE assumes the following network IT entities are in the operating network environment.

- Simple Mail Transfer Protocol (SMTP) Server – An email server is used to facilitate delivery of integrity check results to administrators when the TOE is so configured.
- Simple Network Management Protocol (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.
- Workstation providing a web browser for access to the GUI
- TE Nodes
- LDAP/Active Directory server – An authentication server used to authenticate TE users when the System Login Method is set to LDAP/Active Directory.

Notification mechanisms such as email, SNMP, and syslog server are outside of the TOE boundary. The TOE implements only the client-side of these protocols. The TOE utilizes external (non-TOE) mechanisms for delivery of notifications, thus the TOE cannot guarantee delivery of notifications. Web browsers used with the web-based GUI are not part of the TOE.

3.3.1.1 Tripwire Enterprise System Requirements

The Tripwire Enterprise Server can be installed on the following platforms which are in the operating environment:

- Windows Server 2003 (SP1, SP2) & R2 (32-bit & 64-bit)
- Windows Server 2008 (SP1) & Server Core (32-bit & 64-bit)
- Windows Server 2008 R2 (64-bit)
- Solaris 10 Global & Non-Global Zone (SPARC)

[1] Local operational environment refers to software running on the same host as either the server or agent components of the TOE.

- Red Hat Enterprise Linux 5.2, 5.3, 5.4, 5.5, 5.6, and 6.0 (x86 and x64)
- SUSE Linux Enterprise Server 10.2 and 11.1 (x86 and x64)

Tripwire Enterprise installs the following JVM for use by the TOE on these platforms. This JVM is in the operating environment.

- Sun Microsystems JVM v1.5.0 for AIX and HP-UX agents and v1.6.0.u24 for all other platforms

The TE administrators need to ensure that current and patched JVMs are used during operation of the TE in order to support the security functionality provided. Tripwire makes Java Runtime Environment (JRE) update packages available for download at the same time as Tripwire provides patch release and major updates. Note: JRE updates are not available for AIX and HPUX Agent JVMs.

TE supports the following backend DBs which are in the operating environment:

- MySQL v5.1.49 (Bundled with TE)
- SQL Server 2005 SP2
- SQL Server 2008, 2008 R2
- Oracle 10g, 11gR1, 11gR2

TE Web Admin Console supports the following web browsers which are in the operating environment:

- Firefox 3 latest or later

While the TOE supports Firefox 3 and higher, it has only been tested with Firefox version 3 and 12.

3.3.1.2 Tripwire Enterprise Agent Requirements

TE Agents are installed on file servers and desktops. These nodes are the supported systems/platforms that can be monitored by the TOE.

The Tripwire Enterprise Agents can be installed on the following file servers which are in the operating environment:

- Windows Server 2003 (Service Pack 2) (x86 and x64)
- Windows Server 2008 (x86 and x64)
- Windows Server 2008 Core (x86 and x64)
- Windows Server 2008 R2 (x64)
- Solaris 9 (UltraSPARC ii)
- Solaris 10 Global & Non-Global Zone (UltraSPARC ii, x86 and x64)
- Red Hat Enterprise Linux 4 update 7 (x86 and x64 Editions)
- Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 6 (x86 and x64 Editions)
- Red Hat Enterprise Linux 5.2, 5.3, 5.4, 5.5 (PAE kernel)
- SUSE Linux Enterprise Server 9.2, 10.2, 11.0, 11.1 (x86 and x64 Editions)

- Cent OS 5.2, 5.4, 5.5 (x86 and 64 Editions)
- Fedora Core 10
- HP-UX 11iv1, v2, v3 (PA-RISC)
- HP-UX 11iv2, v3 (Itanium)
- AIX 5.2, 5.3 & 6.0 (64-bit)
- AIX 5.3 (32-bit)

The Tripwire Enterprise Agents can be installed on all versions of the following operating systems which are in the operating environment:

- Windows 2000 Professional (Service Pack 4, update 1)
- Windows XP Professional (Service Pack 3) (x86)
- Windows Vista (Service Pack 1) (x86 and x64)
- Windows 7 (x86 and x64)

All current patches and security fixes must be installed upon these operating systems before installing the Tripwire Enterprise Agents.

The following platforms listed in the Tripwire Enterprise v8.1 Patch README were not subject to testing during this evaluation:

- Red Hat Enterprise Linux 5.7, 6.1, 6.2 (all platforms)

3.3.1.3 Tripwire Enterprise Node Requirements

In addition to desktops and file servers, TE can operate on the following types of nodes which are in the operating environment: databases, virtual environments, directory services, network devices. These nodes are the supported systems that can be monitored by the TOE.

The Tripwire Enterprise configuration can target the following databases:

- IBM DB2 Enterprise Edition version 8.2 – AIX 5.x, Windows 2003, HPUX 11i
- IBM DB2 Enterprise Edition version 9.5 – AIX 5.x, Windows 2003, HPUX 11i
- SQL Server 2000 SP4
- SQL Server 2005 SP2
- SQL Server 2008 SP1, R2
- Oracle 9i, 10g, 11gR1
- Sybase ASE 15.5

The Tripwire Enterprise configuration can target the following virtual environments:

- VMware ESX 3.0x, 3.5x, 4.0, 4.1
- VMware ESXi 3i
- VirtualCenter 2.5

- vCenter Server 4.0, 4.1, or 5.0[2]

The Tripwire Enterprise configuration can target the following directory services:

- Microsoft Active Directory (Windows 2000, 2003/2003 R2, 2008, 2008 R2)
- Sun Directory Server (iPlanet/Sun ONE Directory Server 5.1 SP4, Solaris 9, Sun Java System Directory Server 5 2005Q4 (5.2 P4))
- Novell eDirectory (eDirectory 8.7.3(IR3 and IR5), eDirectory 8.8)

The Tripwire Enterprise configuration can target all versions the following network devices:

- Alcatel OmniSwitch 6xxx/7xxx/8xxx series
- Cisco Catalyst 1900/2820 Switch
- Cisco CatOS, IOS, PIX OS and ASA
- Cisco VPN 3000 Series Concentrator
- Extremeware Switches
- F5 BigIP
- Foundry FastIron Switch
- Foundry ServerIron Switch
- HP ProCurve Series – firmware C and E
- HP ProCurve XL
- Juniper M/T Series, Netscreen, Screen OS
- Ericsson/Marconi ForeThought
- Nokia IPSO Firewall
- Nortel Alteon and Passport Switches – Alteon OS and WebOS
- POSIX compliant UNIX systems (UDK)

All current patches and security fixes must be installed upon these network devices before allowing a Tripwire Enterprise Server to target the network device.

The following platforms listed in the Tripwire Enterprise v8.1 Patch README were not subject to testing during this evaluation:

- VMwareESX 4.2, ESXi 4.2, ESXi 5.

3.4 Logical Scope

The description of the security features of the product are described in further details in Section 0. In summary, these functions are:

- Intrusion Detection System (IDS)
- Security Audit

[2] In the Tripwire Enterprise v8.1 Patch README, VMware vSphere 5 refers to VCenter Server 5.0.

- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

3.5 Excluded Features

The Evaluated Configuration of the TOE does not include the Remedy AR System tickets Plug-in, the HP Openview Plug-in, or the AAA Monitoring Tool. The Remedy AR System tickets Plug-in and the HP Openview Plug-in are extra tools available from Tripwire. The guidance documentation instructs that these tools not be installed. The AAA Monitoring Tool is included within the TOE delivery.

The ability to transfer logs is excluded from the evaluated configuration. This capability requires the use of the Tripwire Log Center. The guidance documentation instructs that this capability not be configured.

In addition, the ability to use the set command to specify the default userid and password during a CLI session is excluded from the evaluated configuration via providing guidance instructing administrators to not use the set command.

The Tripwire Configuration Datamart (AKA Arena) is licensed separately and is excluded from the TOE.

When in its evaluated configuration which requires Federal Information Processing Standard (FIPS)-mode of operation, Internet Explorer browsers are unable to connect to the TOE and as such are not usable with the evaluated configuration. Firefox has been tested and should be used.

4 SECURITY POLICY

The TOE enforces the following security policies as described in the ST.

4.1 Intrusion Detection System

The Tripwire Enterprise (TE) 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 TE Agent reports the detected change to the Tripwire Enterprise Server to allow administrator specified actions to occur. The TE Agent also checks the current monitored system/state for policy compliance. If an Event Generator is installed on an Agent system, TE can monitor the system for changes made in real-time. With real-time monitoring, the Event Generator continuously reports any detected changes to TE.

For nodes without a TE Agent, 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, command output, and network availability using interfaces that each node provides. TE Agent uses OpenSSL 0.98k, which is not FIPS validated, to create hashes of monitored files. OpenSSL is not used for the protection of any sensitive information.

The Tripwire Enterprise Server component can perform actions in response to object attribute comparisons, specifically: display integrity check results to the console, send integrity check results to administrators using email, send integrity check results to administrators using SNMP,

send a log message to a Syslog server, execute a command on the Tripwire Enterprise Server host operating system, execute a command on the Tripwire Enterprise Agent host operating system, and promote new element versions to be a baseline. For some TE nodes, Tripwire Enterprise Server can also restore a changed element to its baseline state on. TE also uses baselining and restoration to process software installation package data.

The syslog server, SMTP server, and recipient of SNMP messages are all external IT entities residing in the environment. It is the responsibility of these IT entities to complete the delivery of such communications. The TOE provides the functionality to send communications to these IT entities in the environment. The TOE does not rely upon these external IT entities to provide security for the TOE.

To test for policy compliance, the administrator downloads & installs TE policies from the Tripwire web site or creates a new TE policy in the Policy Manager. Policy compliance tests can be run on selected nodes and the results viewed in the Policy Manager. TE automatically runs the policy tests whenever a version check results in the creation of change versions for elements of the effective scope of the policy test. Running a policy test involves comparing each change version with the pass/fail criteria defined by the policy test, generating a policy test result for each change version, and updating the compliance statistics for each node in the policy test's effective scope. (This evaluation did not assess the suitability of a given policy files to assess the system's compliance against the external policy or guideline, but rather assessed whether the policy checks specified worked correctly.)

Remediation is the process of resolving failures generated by a policy test. There are two types of remediation: automated and manual. With automated remediation, the TE Agent on the node for which the policy test failed runs a script or performs other actions to bring the node into compliance with the policy test. With manual remediation, a user manually performs the actions to bring the node into compliance with the policy test. In the evaluated configuration, the TOE will be configured to send an alarm when a policy test fails. [3]

The TOE provides a mechanism for authorized users to read the System data. In addition, the TOE protects the collected System data from unauthorized deletion and modification at its own interfaces. It also maintains a defined amount of System data in the event of a failure. When the System data storage capacity is reached, the TOE will shutdown and send an alarm. The TOE depends upon the DB to protect the data stored in it from unauthorized access via the DB interfaces.

For the automated Remediation actions, an administrator configures the TOE to execute a administrator-supplied command or script on the Agent node.

4.2 Security Audit

The TOE provides its own security audit log mechanism, with its own security audit log trail, that can generate records containing TOE management actions and security-related events. These records are referred to as Security Audit Log (SAL) messages. In addition, the TOE generates TE log messages which record a variety of events or activities in a message log. The message log is not considered security-relevant.

The security audit function implements the SAL. The TOE stores the SAL (and message log) in the Database. The term audit data in this ST refers to the SAL messages.

[3] All third party commands, such remediation commands, issued on a device/system in the operational environment are not assured by this evaluation, other than the issuance of the command by TE.

The TOE provides administrators the ability to manage the Tripwire Enterprise Server SAL using administrator console interfaces. Administrators can select which security-relevant events will result in the generation of an audit record. Administrators can read and sort SAL 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.

The TOE protects the SAL messages from unauthorized deletion and prevents modifications at its own interfaces. When the SAL log storage capacity is reached, the TOE maintains all stored audit log messages, shuts down and sends an alarm. The TOE depends upon the DB to protect the data stored in it from unauthorized access via the DB interfaces.

The security audit function relies on the TOE's environment to supply a reliable date and time stamp which the TOE includes in each SAL message. The security audit function also relies upon the TOE's environment to store and protect audit data contained in a SAL message.

4.3 User Data Protection

The TOE implements access controls on eleven TE objects: nodes, and node groups, rules and rule groups, actions and action groups, tasks and task groups, TE policies, policy tests, and policy test groups. Nodes and node groups are definitions of network entities upon which some integrity check and policy compliance assessment operations are 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 objects is controlled by the Discretionary Access Control (DAC) policy for all available operations on these objects (and their contents). Node objects have access controls that can specify the user role assigned to a user or user group to define the user permissions granted to the user. These attributes are compared against user identities and groups of subjects in order to determine whether the user is granted the user role and therefore whether the requested operations should be allowed. If the access checks fail, access will be refused.

4.4 Identification and Authentication

The TOE offers a few non security-relevant mediated functions (i.e., Simple Object Access Protocol (SOAP) locale management commands and the twtool licurl, set, version, and help functions) before the user is identified and authenticated. All security-relevant mediated functions require the user to be authenticated. The TOE provides two different login methods:

Password Method	The TOE itself identifies and authenticates the username and password supplied. Always used for identifying and authenticating the built-in "administrator" account.
LDAP/Active Directory Method	The TOE is configured to request authentication services from a LDAP or Active Directory server for all user accounts except the built-in "administrator" account. In this case, TE depends upon the LDAP or AD server to be securely installed and administered.

TE always authenticates Administrator accounts with the Password login method, regardless of the selected login method. The TOE maintains the following security attributes for each user account using the Password Method: user identity, authentication data, user groups, role information, and authorizations. The TOE requires passwords to be between six and twenty-four characters in length. Guidance provides recommendations to the users for creating strong passwords. In addition, the TOE is able to lockout user accounts if the number of consecutive unsuccessful authentication failures exceeds a threshold configured by an administrator.

4.5 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. TE Server provides management tools for:

- Modifying the behavior of system data collection, analysis, and reaction
- Enabling/disabling integrity check rules
- Enabling/disabling integrity check actions
- Managing the object and user security attributes used by the discretionary access control policy
- Query and add system and audit data
- Query and modify TOE data

The TOE also protects the collected System data from unauthorized deletion and modification at the TOE interfaces.

A user permission is a system authorization which enables a user with that permission to view, add, change, or delete data in Tripwire Enterprise. The following list defines a sample of the common types of user permissions.

- **Load permissions** provide read-only access to a class of Tripwire Enterprise objects and groups. For instance, the load rules permission grants access to the Rule Manager. In the Rule Manager, users can review all rules and rule groups.
- **Create permissions** authorize users to create a class of Tripwire Enterprise objects and groups. For example, the create nodes permission authorizes users to create nodes and node groups.
- **Delete permissions** authorize users to permanently remove objects or groups from the system. For instance, with the delete nodes permission, users can delete both nodes and node groups.
- **Update permissions** enable users to modify the properties of a class of Tripwire Enterprise objects and groups. For example, users can change the properties of nodes and node groups with the update nodes permission.
- **Manage permissions** authorize users to modify Tripwire Enterprise settings or parameters.

Tripwire Enterprise includes nine (9) 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 account or an access control entry. The default user roles are: Administrator, Monitor User, Policy Manager, Policy User, Power User, Regular User, Rule Manager, Rule User, and User Administrator. Four of these default user roles (Administrator, Power User, Regular User, and Monitor User) are organized hierarchically from most capabilities to least capabilities being Administrator, Power User, Regular User and Monitor User. The User Administrator role is orthogonal to the other roles and has permissions to manipulate user accounts. The Policy Manager, Policy User, Rule Manager, and Rule User default roles are used in access controls applied to pre-configured TE objects. To preserve the intended purpose of these roles, administrators are instructed in guidance to avoid assigning them directly to user accounts.

TE also provides a tool called FastTrack which automatically runs only the first time that the administrator logs into the Console. This tool provides limited capabilities required to setup TE.

4.6 Protection of the TSF

The TOE ensures that the audit data and System data is available by protecting it from modification and deletion and by maintaining all of the stored data when storage exhaustion occurs.

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 database (in the operational 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. It is expected that the operational environment provides protections such that the communications between the Tripwire Enterprise Server and the database cannot be spoofed. It is also expected that the database be protected such that only the TOE can access the database. This is accomplished by requiring the communications with the database to be encrypted and requiring users to login to access the database. The database 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 user community of the TOE has no relationship to the users of the underlying operating system. The JVM also provides the actual implementation of TLS v1 used for communications between the TOE and remote IT products. The JVM is configured to use TLS for these communications.

TE 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 nodes using supported network protocols such as Secure Shell (SSH) or telnet). For nodes that do not support SSH based protocols for login, it is expected that those responsible for managing the nodes have taken steps to secure the communication pathways between the TOE and the nodes per their security environment. The TOE does not rely upon the security of these communication pathways to nodes for TOE's self protection.

There are two different cryptographic implementations used by the TOE. The TOE includes the FIPS certified Tripwire Cryptographic Module (TCM) which is used to implement TLS to protect communications between the TE server and TE Agents. The TOE uses the JVM TLS implementation in the operational environment to protect communications between the TOE and the remote IT entities.

The Tripwire Enterprise Server and Tripwire Enterprise Agent components of the TOE use the TLS v1 provided by the TCM to communicate with each other. The server to agent connection is established with a mutually authenticated TLS connection. This allows these components of the TOE to use the RMI protocol to exchange services.

The TOE protects the TSF data transmitted from the TSF to a remote trusted IT product using TLS/SSH from unauthorized disclosure and modification. If modifications are detected, the TOE

provides the ability to verify the integrity of the TSF data transmitted information. Communication between the server portion of the TOE and a remote DB are protected via TLS provided by the JVM or by the private, secure network on which the DB resides.

The TOE also uses the JVM provided TLS 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.

5 CLARIFICATION OF SCOPE

5.1 Assumptions

The ST identifies the following assumptions about the use of the product:

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- There will be one or more competent individuals assigned to manage the TOE and its environment 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 and that of its environment.
- The TOE can only be accessed by authorized users.
- The TOE has access to all the IT System data it needs to perform its functions.
- The TOE is appropriately scalable to the IT System the TOE monitors.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

5.2 Limitations and Exclusions

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 (EAL 2 augmented with ALC_FLR.2 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 EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
4. The evaluation did not assess the suitability of given policy files to assess the system’s compliance against the external policy or guideline, but rather assessed whether the policy checks specified worked correctly.

5. The TOE relies on the operational environment in which it operates for the following security and other functionality:
   - Protect the TOE's stored executable image and its execution environment.
   - Protect TOE stored data, including audit records and scan results.
   - Provide a means to audit attempts to access the TOE stored executable image and stored data from the operational environment (i.e., not through the TOE's own interfaces).
   - Provide a reliable time stamp for use in audit records and scan results.
   - Identify and authenticate authorized administrators and restrict the ability to manage and operate the TOE to authorized administrative users.
   - Provide a means for authorized administrators to review and sort the audit records in the audit trail.
   - Provide encryption services used to encrypt communication channels between TOE Console and web browsers used to access it as well as between the TOE and other operational environment components.
   - Additionally, the TOE relies on its host to facilitate communication with scan targets (e.g., directory servers, agents, network devices, and databases) for the purposes of scanning and auditing.
6. The Evaluated Configuration of the TOE does not include the Remedy AR System tickets Plug-in, the HP Openview Plug-in, or the AAA Monitoring Tool. The AAA Monitoring Tool is included within the TOE delivery. The Remedy AR System tickets Plug-in and the HP Openview Plug-in are extra tools available from Tripwire. The guidance documentation instructs that these tools not be installed.
7. The product capabilities described in Section were not included within the scope of the evaluation and no claims are made regarding them.

6 ARCHITECTURAL INFORMATION

The Target of Evaluation (TOE) is Tripwire Enterprise, Version 8.1 with the 8.1.2.5 patch. The TOE is an intrusion detection system consisting of a sensor, scanner, and analyzer to monitor IT systems for activity that may indicate inappropriate activity on the IT system. The TOE is an attribute change assessment product that also reconciles the changes against existing management systems and policies. The TOE provides three main capabilities: File Integrity Monitor, Compliance Policy Manager, Remediation Manager.

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 databases, directory servers, 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. 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 (or file server 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. If an Event Generator is installed on an Agent system, the system can be monitored for changes made in real-time.

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.

A node is represented in the TOE by its network address (hostname or IP address).

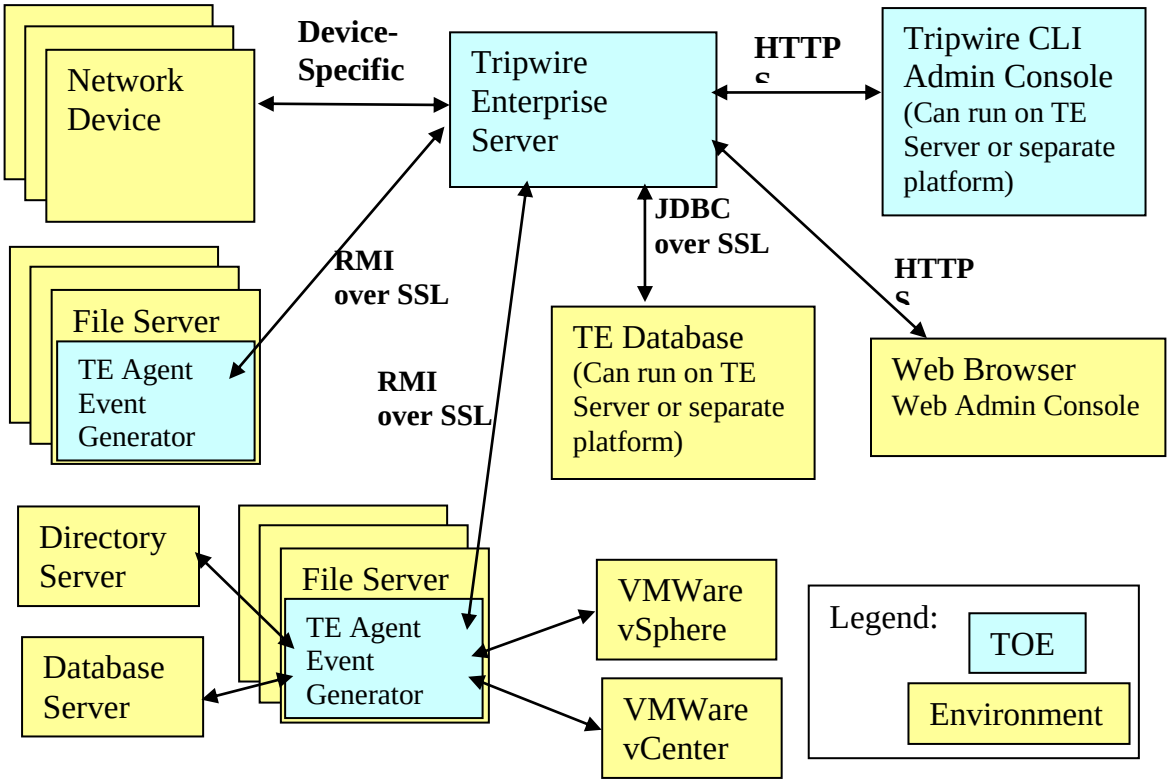

Figure 1: TOE boundary

The Tripwire Enterprise (TE) Server component delegates work to Tripwire Enterprise Agents, interacts with TE nodes, analyzes information, assesses policy compliance, repairs configuration errors, 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:

- User Interface (UI)
- Downloadable Agent Code

- Database Mapping Layer
- Remote Method Invocation (RMI) Layer
- TE 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 Admin Console. 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 Hypertext Transport Protocol Secure (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[4], configure and schedule policy compliance tests, configure remediation actions, 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[5].

Commands available through the CLI include the following:

baseline	Baselines sets of monitored elements (node groups, a single node, or elements within a node).
check	Checks monitored elements for change. (Also known as an integrity check)
delete	Deletes specified TE objects
export	Exports specified nodes or rules to an XML node file.
help	Provides assistance in using the CLI.
import	Imports an XML node file or an XML rule file into the Tripwire Enterprise configuration.
licurl	Generates a Launch-in-Context URL.
promote	Promotes the latest version of an element to the baseline.
promoteRefNode	Copies the current baselines from one node to one or more other nodes.
report	Generates Tripwire Enterprise reports, by specific nodes or rules.
runaction	Runs one or more TE actions. (An action is a TE object that initiates a response to detected changes.)

[4] The more general term 'integrity check' is used in the Security Target, but is intended to have the same meaning as the term 'version check' which is used in Tripwire guidance documentation.
[5] The Tripwire Enterprise Server uses the SSL provided by the operational environment for HTTPS communications.

runtask	Runs a TE task
set	Sets default arguments for common options for other CLI commands.
setcustomproperty	Assigns custom-property values to specified nodes, elements, or element versions.
variable	Defines or updates a Tripwire Enterprise variable.
version	Reports the current version of the CLI.

TE Server user identification and authentication credentials must be included as arguments to the **baseline**, **check**, **delete, export, import**, **promote**, **promoteRefNode, report, runaction, runtask, setcustomproperty** and **variable** commands every time they are invoked.[6] The other commands (**licurl**, **set**, **version**, and **help**) as well as SOAP local management commands are processed locally by the CLI and are not passed to the TE Server so no identification or authentication is performed. The **set** command can be used to specify the default userid and password during a CLI session, after which arguments with the default userid and password will be automatically added to each of the commands sent to the Tripwire Enterprise Server. Tripwire Enterprise v8.1 Supplemental Common Criteria Guidance advises the administrator to not use this feature in the CC evaluated configuration. Including user identification and authentication credentials as arguments to each command allows the Tripwire Enterprise Server to process commands from multiple users without having to maintain separate user sessions. Every command sent to Tripwire Enterprise Server stands alone and executes without a session context.

The Downloadable Agent Code is the portion of the Tripwire Enterprise Server that provides instructions to the Tripwire Enterprise Agent component about what types of operations to perform on a particular agent's host machine. This code is a Java object that is executed by the Tripwire Enterprise Agent by means of Remote Method Invocation (RMI). This code can contain instructions to perform any of the following activities:

- Create a baseline (a known good state)
- Run an integrity check
- Execute an action

The Database Mapping Layer provides a JDBC interface to a SQL database. If the configuration uses a remote SQL server, the TE Server must be configured to encrypt all communications between itself and the database. For local or remote MySQL DB installations a single account is automatically created in the database during TE Server installation. If the MySQL DB is used, MySQL can either be installed on the same system as the TE server or installed on a system located on a private physical network that is not globally routable and is protected from attacks and from unauthorized physical access. If the Oracle DB is used, it must be installed on a system located on a private physical network that is not globally routable and is protected from attacks and from unauthorized physical access.

For remote installations using SQL server and Oracle DBs, the administrator is instructed to create the single database account. This account is used by the Tripwire Enterprise Server when

[6] If authentication credentials (i.e., userids and passwords) are saved in scripts on the machine being used as an administrative workstation, protection of these scripts is outside the scope of the TOE. The storage of plaintext passwords in scripts will make some 800-53 controls/enhancements non-compliant.

storing and accessing configuration information about monitored objects[7], log messages and report data in the database. The database is relied upon to store, retrieve and protect data that it handles such that only the Tripwire Enterprise Server can access its own data.

The Remote Method Invocation (RMI) Layer allows Tripwire Enterprise Server to execute Java byte code on Tripwire Enterprise Agents. RMI runs over a mutually authenticated TLS connection. Since the protocol transporting the RMI protocol is authenticated, RMI need not perform additional security checks. However, as a precaution, RMI messages are executed using downloaded byte code encapsulated in Java Archive (JAR) files which are signed by another certificate. These JAR files are signed by a certificate, in which the private signing half is only held in-house at Tripwire headquarters. Any communications based on unsigned or improperly signed JARs are rejected at the start of the RMI communication.

The TE Node device-specific interface provides a custom interface for obtaining configuration parameters and other management data from a specific list of supported devices (nodes). The device-specific interfaces utilize protocols such as SSH, telnet, and File Transfer Protocol (FTP).

7 PRODUCT TESTING

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report For Tripwire, Inc. Tripwire Enterprise Version 8.1.

Evaluation team testing on version 8.1 with Patch 8.1.2.5 of the product was conducted at the vendor's development site May 7 through May 11, 2012.

The purpose of this 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 for an EAL2+ evaluation.

7.1 Developer Testing

The vendor approach to testing of the TOE security functions involves a series of manual tests. Test procedure descriptions describe in detail how each test is implemented. The primary function of each test procedure document is to provide a good understanding of the purpose of the test, including a description of the test cases and variations that are tested by the corresponding tests. In addition each test procedure document includes instructions for the repeatable execution of the tests. This includes a description of any requirements for establishing the test environment for each test as well as a description of how to actually execute each test and verify its results against the expected results.

In general, the developer selected a small subset of their overall tests in order to fulfill the test requirements for an EAL2+ evaluation. The selection was chosen to provide representative testing of the security functions related to each of the security requirements in the Security Target. The developer has documented their tests in a test plan, a series of mappings between pre-existing test cases and the Security Functional Requirements (SFRs) for coverage, and their referenced test procedure repository. Results were provided in terms of success, last date of application, and some notes.

[7] This includes user names and passwords used to establish a connection to TE nodes. These passwords are stored within the database in a hashed form.

7.2 Evaluation Team Independent Testing

The evaluators developed a test plan addressing TOE installation, use of developer-provided security functional tests, and independently created security functional and penetration tests. After testing the evaluators produced a test report describing the hand-on, independent testing effort.

The evaluators installed and configured the evaluated TOE version (32- and 64-bit versions) in four representative operational configurations, intended to cover both the TOE server and agent host variations, but also the variations in the target components and environments, using the evaluated guidance documents. The test configurations were used to ensure coverage of the server products hosted on different supported operating systems; agents running on the full range of supported operating systems; supporting backend databases; and targets (directory servers, virtual environments, databases, and network devices). Scanning tools, including nmap and Wireshark, were used to scan the installed TOE components and to observe network traffic among applicable components.

The evaluation team devised a test subset based on coverage of the security functions described in the ST. The evaluators exercised about 50% of the developer tests, without issues of substance, as well as their own tests finding the TOE to operate as claimed. The evaluators performed port scans on each of the component hosts in order to identify and rationalize any open ports. The evaluators collected network sessions for the purpose of verifying that the connections between the TOE server and TOE agents as well as between the TOE server and administrator browsers to confirm they were encrypted as claimed.

Ultimately, the tests exercised by the evaluators touched on every claimed security function as well as some security architecture aspects of the TOE. Given the breadth of tests directly and successfully exercised by the evaluators the testing requirements for EAL2+ are fulfilled.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities. The evaluation team did not identify any findings that indicated vulnerabilities in the TOE. Note that during the course of evaluation, the evaluators extended their search beyond the TOE to directly supporting 3rd party components. In addition, the evaluation team conducted tests confirming that unauthorized users in the operational environment of the TOE could not get unexpected (e.g., insecure) access to the TOE components when configured as instructed. However, it is recommended that all supporting products and browsers be fully patched and use the latest secure versions where applicable.

8 DOCUMENTATION

8.1 Product Guidance

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- Tripwire Enterprise v8.1 Supplemental Common Criteria Guidance, Version 1.1, July 13, 2012, TW1140-00
- TRIPWIRE® ENTERPRISE v8.1 REFERENCE GUIDE, TW1092-12

- TRIPWIRE® ENTERPRISE v8.1 INSTALLATION & MAINTENANCE GUIDE, TW1032-25
- TRIPWIRE® ENTERPRISE v8.1 USER GUIDE, TW1031-21
- Tripwire Enterprise 8.1 Patch README February 24th, 2012

Note that these are the only documents provided with the TOE.

8.2 Evaluation Evidence

The following tables identify the additional documentation submitted as evaluation evidence by the vendor. With the exception of the Security Target, these documents are proprietary and not available to the general public.

Design Documentation	Version	Date
Tripwire Enterprise Version 8.1 Design Document	1.1	13 July 2012

Guidance Documentation	Document ID	Date
Tripwire Enterprise v8.1 Supplemental Common Criteria Guidance, Version 1.1	TW1140-00	13 July 2012
TRIPWIRE® ENTERPRISE v8.1 REFERENCE GUIDE	TW1092-12	
TRIPWIRE® ENTERPRISE v8.1 INSTALLATION & MAINTENANCE GUIDE	TW1032-25	
TRIPWIRE® ENTERPRISE v8.1 USER GUIDE	TW1031-21	
Tripwire Enterprise 8.1 Patch README February 24th, 2012		24 Feb 2012

Life Cycle Documentation	Version	Date
Tripwire, Inc. Tripwire Enterprise Version 8.1, Configuration Management Plan,	1.1	13 July 2012
Tripwire, Inc. Tripwire Enterprise 8.1 Lifecycle Document	1.0	5 June 2012
Tripwire Enterprise v8.1 Delivery Procedures	1.0	6 June 2012

Test Documentation	Version	Date
Tripwire Enterprise Version 8.1 Test Plan and Procedures	1.0	6 June 2012
Tripwire Enterprise Version 8.1 Test Case Mappings	1.1	13 July 2012
docsys-te-patch-8.1.2.5.zip (test procedures)	n/a	n/a

Vulnerability Assessment Documentation	Version	Date
Not applicable	n/a	n/a

Security Target	Version	Date
Tripwire, Inc. Tripwire Enterprise Version 8.1 Security Target	1.1	13 July 2012

9 RESULTS OF THE EVALUATION

The Evaluation Team conducted the evaluation in accordance with the CC, the CEM, and the CCEVS.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2+ 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.

The Evaluation Team accomplished this by providing notes, comments, or vendor actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. 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. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary part of the ETR (see Chapter 15).

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1r3 [1], [2], [3] and CEM version 3.1r3 [4]. The evaluation determined the TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 2) requirements, augmented with ALC_FLR.2. The rationale supporting each CEM work unit verdict is recorded in the "Final Evaluation Technical Report For Tripwire, Inc. Tripwire Enterprise Version 8.1 Part 2" which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

Section 6.1, ST Evaluation: Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the ST is a CC compliant ST.

Section 6.2, TOE Evaluation: The verdicts for each CEM work unit in the ETR sections included in the proprietary part of the ETR (see Chapter 15) are each "PASS". Therefore, the TOE (see below product identification) satisfies the Security Target, when configured according to the following guidance documentation:

- Tripwire Enterprise v8.1 Supplemental Common Criteria Guidance, Version 1.1, July 13, 2012, TW1140-00
- TRIPWIRE® ENTERPRISE v8.1 REFERENCE GUIDE, TW1092-12
- TRIPWIRE® ENTERPRISE v8.1 INSTALLATION & MAINTENANCE GUIDE, TW1032-25
- TRIPWIRE® ENTERPRISE v8.1 USER GUIDE, TW1031-21
- Tripwire Enterprise 8.1 Patch README February 24th, 2012

Additionally, the evaluation team's performance of developer tests, independent tests, and penetration tests further demonstrates the accuracy of the claims in the ST.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL2 augmented with ALC_FLR.2" certificate rating be issued for Tripwire Enterprise, Version 8.1 with the 8.1.2.5 patch.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements are listed in the following table:

Table 2. TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_ARC.1	Security architecture description
ADV_FSP.2	Security-enforcing functional specification
ADV_TDS.1	Basic design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.2	Use of a CM system
ALC_CMS.2	Parts of the TOE CM coverage
ALC_DEL.1	Delivery procedures
ALC_FLR.2	Flaw reporting procedures
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_VAN.2	Vulnerability analysis

10 VALIDATOR COMMENTS/RECOMMENDATIONS

1. There was a question of whether the TOE collects sufficient audit to meet ECAR-1 or AU-2+CNSS 1253, for those events that are applicable to this TOE? Or specifically -- "(a) Successful and unsuccessful attempts to access, modify, or delete security objects, (b) Successful and unsuccessful logon attempts, (c) Privileged activities or other system level access, (d) Starting and ending time for user access to the system, (e) Concurrent logons from different workstations, (f) Successful and unsuccessful accesses to objects, (g) All program initiations, (h) All direct access to the information system.".

   In the context of the evaluated configuration, the evaluators found that the TOE audits the events associated with items a, b, and c. In the case of d, while logins are audited, users can be disconnected without being subject to audit. In the case of e, the TOE does not specifically keep track of whether simultaneous access might be occurring from multiple/different workstations. In the case of f and g, while privileged actions are generally audited the TOE does not specifically audit failed object accesses nor program invocation. In the case of h, the TOE is a software application and as a result it would be largely up to its host operating system to audit direct access to the TOE or its resources.

2. The TOE implements a permissive default access policy for objects created by and used by its users. This was deemed acceptable since all users of the TOE are specifically provided access since they play a role in the intrusion detection and prevention functions implemented by the TOE. As such, all of the applicable users are expected to be trusted in some regards and are further assumed to operate in a relatively cooperative mode such that they would not interfere with each other.

3. The evaluated product supports only a limited number of administrative browsers (i.e., FireFox) due to issues in connecting using FIPS certified ciphers discovered during testing of the TOE.

4. The TOE has been patched to 8.1.2.5 and that patch offers additional support for agents (Red Hat Enterprise Linux 5.7, 6.1, 6.2) and target virtual environment nodes (VMwareESX 4.2, ESXi 4.2, ESXi 5). However, that additional support has not been subject to the evaluation.

11 ANNEXES

Not applicable.

12 SECURITY TARGET

The ST for this product's evaluation is **Tripwire, Inc. Tripwire Enterprise Version 8.1 Security Target, Version 1.1, 07/13/2012**.

13 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 3, July 2009

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 3, July 2009

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009

[5] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008

[6] Intrusion Detection System System Protection Profile (IDSSYPP), Version 1.7, July 25, 2007

[7] Tripwire, Inc. Tripwire Enterprise Version 8.1 Security Target, Version 1.1, July 13, 2012