Security Target

for

Tripwire Manager Version 3.0 with Tripwire for Servers Version 3.0

Tripwire Manager Version 3.0, with Tripwire for Servers Check Point Edition Version 3.0

Release Date:	**February 13, 2003**
Version:	**2.1**
Status:	**Final**

Prepared By:	**Corsec Security, Inc.** 10340 Democracy Lane Suite 201 Fairfax, VA 22030 Phone: 703.267.6050
Prepared For:	**Tripwire, Inc.** 326 SW Broadway, 3rd Floor Portland, OR 97205 Phone: 503.223.0280

Table of Contents

List of Figures

List of Tables

1 ST Introduction

1.1 Security Target Identification

Title:
Security Target for Tripwire Manager Version 3.0, with Tripwire for Servers Version 3.0
Tripwire Manager Version 3.0, with Tripwire for Servers Check Point Edition Version 3.0

Version:	2.1
Status:	Final
Release Date:	February 13, 2003
Prepared By:	Corsec Security, Inc.

Two TOE Identifiers:
Tripwire Manager, Version 3.0, with Tripwire for Servers, Version 3.0.
Tripwire Manager, Version 3.0, with Tripwire for Servers Check Point Edition, Version 3.0.

Assurance level:	EAL1
Common Criteria:	Common Criteria for Information Technology Security Evaluation (CC), Version 2.1, August 1999 (aligned with ISO/IEC 15408).
Interpretations:	National and International interpretations are provided within the Section 9.2 of this ST.
Keywords:	Data Integrity Assessment, Integrity Checking, Tripwire, Check Point

1.2 TOE Reference

The TOE is identified as the following:

Tripwire Manager, Version 3.0, with Tripwire for Servers Version 3.0.
Tripwire Manager, Version 3.0, with Tripwire for Servers Check Point Edition, Version 3.0.

The Operating System (OS) on which the Tripwire software relies, this ST and all the administration and user guides that are listed within the Table **7** (section 8.4.2 of this ST), are part of the TOE as well.

1.3 CC Conformance Claims

This TOE is:

1) CC Version 2.1 Part 2- extended.
   There are four explicitly stated functional requirements in this ST.
2) CC Version 2.1 Part 3-conformant.

1.4 Security Target Overview

This document is the Security Target for Tripwire Manager Version 3.0, with Tripwire for Servers Version 3.0; Tripwire Manager Version 3.0, with Tripwire for Servers Check Point Edition Version 3.0 .

Tripwire is a file systems integrity checker tool designed to aid system administrators and users to monitor file system for unauthorized or unexpected modification. Tripwire can assure the integrity of critical data on the system(s) by detecting corrupted or altered files and reporting the occurrence to the system administrators, so corrective actions can be taken.

This ST contains the following sections:

- **ST Introduction** – Provides an overview of the ST
- **TOE Description** – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE
- **Security Environment** – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.
- **Security Objectives** – Identifies the security objectives that are satisfied by the TOE and the TOE environment.
- **TOE Environment IT Security Requirements** – Presents the Security Functional Requirements (SFRs) met by the TOE Environment
- **TOE IT Security Requirements** – Presents the Security Functional Requirements (SFRs) met by the TOE
- **Assurance Requirements** – Presents the Security Assurance Requirements met by the TOE
- **TOE Summary Specification** – Describes the security functions provided by the TOE to satisfy the security requirements and objectives
- **Protection Profile Claims** – Presents the rationale concerning compliance of the ST with CC Version 2.1.
- **ST Rational** – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- **References** – Presents the lists of the acronyms and interpretations used on this ST.

1.5 Document Conventions

There are several font variations within this ST. The text below provides an explanation of the font conventions used to show operations, as defined in Common Criteria, performed on the requirements.

Assignment:	*Requirement text will appear in Italics and underlined*
Iteration:	Typical CC requirement naming will be followed by a lower case letter for each new iteration. (Ex. FMT_MOF.1a)
Selection:	**Requirement text will appear in bold and underlined**
Refinement:	***Requirement text will appear in bold italics***

2 TOE Description

This section describes the Target of Evaluation (TOE) in terms of the class of product, the provided security functionality, and the TOE boundaries.

2.1 Tripwire Overview

The Tripwire software is a data integrity assessment product that can assure the integrity of critical data on system(s) by monitoring the system files for unauthorized or unexpected modification. The TOE accomplishes this by detecting the corrupted or altered files and reporting the occurrence to the system administrators, so corrective actions can be taken. The following diagram describes in general terms the steps of checking the data integrity using Tripwire software.

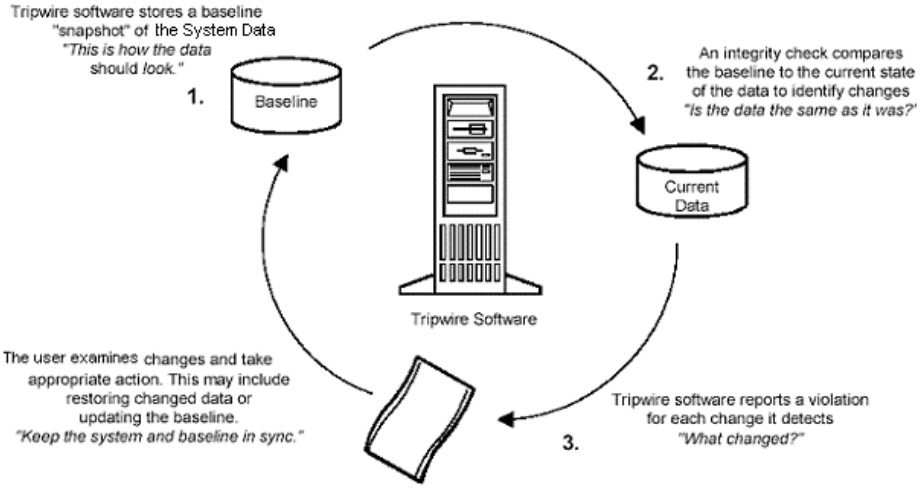

Figure 1. Process of checking the data integrity using Tripwire software

1. Based on the configuration, the Tripwire software creates a baseline snapshot of the system data in a known good state.
2. After the baseline is established, the Tripwire software can regularly check the integrity of the system data. During an integrity check, Tripwire software compares the current state of data to the baseline and reports a violation or any change it detects.
3. The administrator (user) examines report files to evaluate changes to the system data and to take appropriate measures such as:
    a. If the changes are considered to be malicious or unauthorized, then the system administrator may take steps to restore the correct files to the system.
    b. If the changes are acceptable, than the baseline database can be updated to include them so that Tripwire software no longer detects them as violations.

2.1.1 Tripwire for Servers

Tripwire for Servers (TFS) is a self-contained integrity assessment system that can be installed on each machine that needs to be monitored. The TFS automatically verifies data and file integrity against a known good state in the Tripwire database and quickly notifies the administrator of any changes. The Tripwire for Servers software engine conducts subsequent file checks, automatically comparing the state of the system with the baseline database. Any inconsistencies are reported to Tripwire Manager and to the host system's log file. Reports can also be emailed to an administrator. In addition, Tripwire for Servers can execute commands automatically in response to violations, or every time when integrity checks are performed. If a violation is actually an authorized change (such as installing an upgrade or new application), a user can update the database so changes no longer show up as violations.

Tripwire for Servers detects changes to the system data, whether from outside the organization or from within it. Tripwire for Servers software can be used in the same way, whether it is used in conjunction with Tripwire Manager to manage the machines or managed by issuing commands from the command line.

2.1.2 Tripwire for Servers Check Point Edition

Tripwire for Servers, Check Point Edition (TFS CPE) assures the integrity of Check Point firewalls and VPN gateways by detecting and reporting change of the system data. Such data may include: logs, firewall rules, configurations, or allowed VPN connections. TFS CPE establishes a baseline of data in known good state, detects and reports changes to the baseline, and enables rapid discovery and remediation when an undesired change occurs.

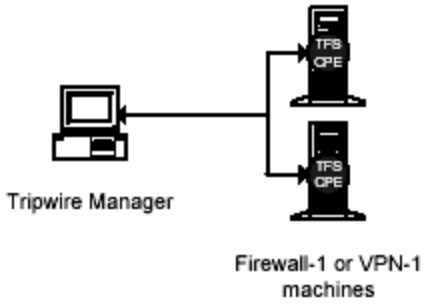

Figure 2. Tripwire for Servers Check Point Edition configuration

Tripwire for Servers CPE provides the capability to use Check Point Log Viewer as a means to review integrity checks run by Tripwire software; however this functionality is excluded from this evaluation. All other functions that the Tripwire of Server uses to review the integrity check reports are also available in Tripwire for Servers CPE.

Considering the above comments, Tripwire for Servers Check Point Edition and Tripwire for Servers provide the same security functions, therefore they have been consider to be the same

for this evaluation. Both TFS and TFS CPE products will be referred as Tripwire for Servers for the remainder of this ST.

2.1.3 Tripwire Manager

Tripwire Manager (TWM) is a Java-based application with a graphical user interface (GUI) that allows the administrator to manage multiple installations of Tripwire for Servers software from a central location. The most basic configuration is a single Manager that controls all Tripwire for Servers machines:

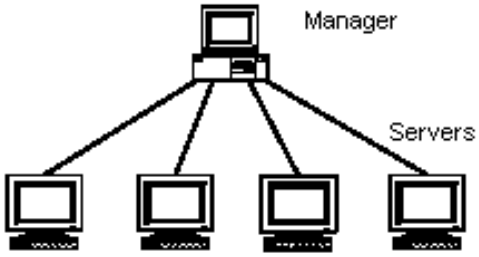

Figure 3.Tripwire configuration with one Manager

Multiple Managers can connect to the same Tripwire for Servers machine. However, only one Manager can issue commands to a Tripwire for Servers machine at a time.

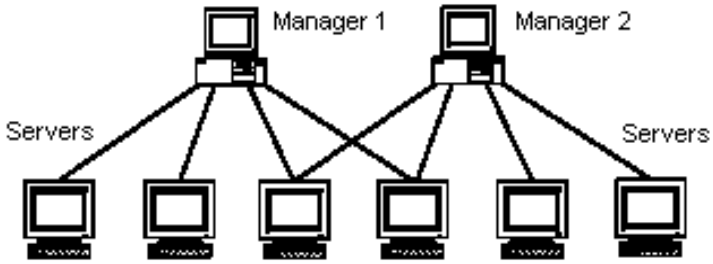

Figure 4. Tripwire configuration with multiple Managers

Tripwire Manager can manage up to 2,500 Tripwire for Servers installations from a central console. From a single console it is possible to view and manage reports from all Tripwire-equipped machines. Secure Sockets Layer (SSL), an industry-standard authentication and data encryption protocol, protects each communication link between the Tripwire Manager Console and network components running Tripwire for Servers software.

2.2 TOE Boundary

The complete TOE consists of (at least) two physically separate machines which consist of the Tripwire for Servers, and the Tripwire Manager products[1]. Both products are software applications that reside on top of the operating system platform. With this in mind, the sole

[1] Tripwire for Servers and Tripwire Manager can be installed on the same machine also.

definition of the TOE includes the Tripwire software application components and the Operating System. All the administration and user guides that are included in Tripwire delivery package are considered to be part of the TOE as well.

The physical computers and network interfaces related to the product are outside the scope of this TOE.

The installation configuration for the two TOE is as the following:

- Tripwire Manager and Tripwire for Servers
- Tripwire Manager and Tripwire for Server Check Point Edition.

This ST refers to both TOE configuration, unless otherwise is specified.

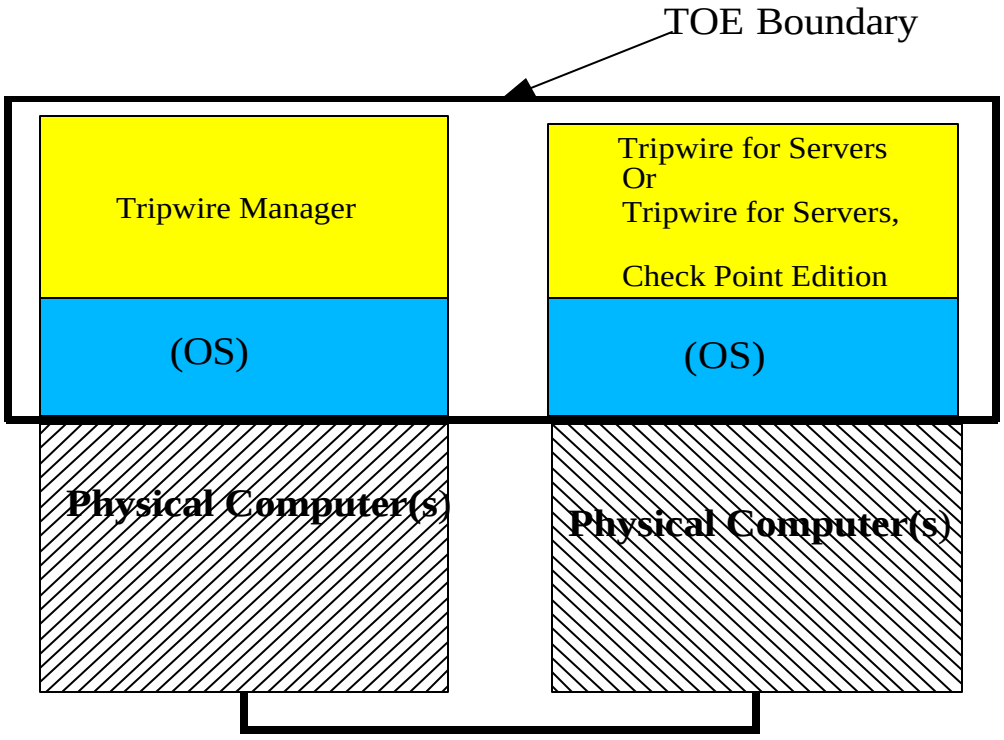

Figure 5. TOE Boundary

2.2.1 Tripwire Manager

2.2.1.1 Hardware Requirements

Hardware components are not considered part of the TOE; however, the Tripwire Manager requires the following minimum hardware requirements to operate:

1. Sun Solaris operating system
   - Ultra SPARC II or higher processor,
   - 115 MB free hard disk space,
   - 256 MB RAM
2. Windows operating systems
   - Intel Pentium III class or higher processor,
   - 60 MB free hard disk space,
   - 256 MB RAM

In addition, all systems require network connectivity to the Tripwire for Servers product.

2.2.1.2 Software Requirements

The following software components are required for Tripwire Manager operation but are not considered to be part of the TOE:

1. Sun Solaris Platforms
   - Sun Solaris 7
   - Sun Solaris 8
2. Windows Platforms
   - Windows NT 4.0 with SP4+ (Workstation, Server, Server Enterprise Edition)
   - Windows 2000 (Professional, Server, Advanced Server)
   - Windows XP Professional

2.2.2 Tripwire for Servers

2.2.2.1 Hardware Requirements

Hardware components are not considered part of the TOE; however, the Tripwire for Servers requires the following minimum hardware requirements to operate:

1. Compaq Tru64 UNIX operating systems
   - Intel Pentium class processor,
   - 25 MB free hard disk space,
   - 128 MB RAM
2. FreeBSD operating system
   - Intel Pentium class processor,
   - 25 MB free hard disk space,
   - 128 MB RAM
3. GNU / Linux operating systems
   - Intel Pentium class processor,
   - 25 MB free hard disk space,
   - 128 MB RAM

4. HP/UX operating systems
   - PA-RISC 1.1 or higher processor
   - 25 MB free hard disk space,
   - 128 MB RAM
5. IBM AIX operating systems
   - RS/6000 processor,
   - 25 MB free hard disk space,
   - 128 MB RAM
6. Sun Solaris operating systems
   - SPARC processor,
   - 30 MB free hard disk space,
   - 128 MB RAM
7. Windows operating systems
   - Intel Pentium class processor,
   - 20 MB free hard disk space,
   - 128 MB RAM

In addition, all systems require network connectivity to the Tripwire Manager product.

2.2.2.2 Software Requirements

The following software components are required for Tripwire for Servers operation but are not considered to be part of the TOE:

1. Compaq Tru64 platforms
   - Compaq Tur64 4.0F
   - Compaq Tur64 4.0G
   - Compaq Tur64 5.0A
   - Compaq Tur64 5.1
   - Compaq Tur64 5.1A
2. FreeBSD Mall platform
   - FreeBSD 4.4
   - FreeBSD 4.5
3. GNU / Linux Platforms
   - Caldera OpenLinux 2.4
   - Debian GNU/Linux 2.2
   - Mandrake Linux 8.1
   - Red Hat Linux 6.2
   - Red Hat Linux 7.0
   - Red Hat Linux 7.1
   - Red Hat Linux 7.2
   - Slackware Linux 8.0
   - SuSE Linux 7.2

- SuSE Linux 7.3
- Turbolinux Linux Workstation 6.1
- Turbolinux Linux Workstation 7.0
- Turbolinux Linux Server 7.0

4. Hewlett Packard HP/UX platforms
   - Hewlett Packard HP/UX 10.20
   - Hewlett Packard HP/UX 11.0
   - Hewlett Packard HP/UX 11i
5. IBM AIX Platforms
   - IBM AIX 4.3
   - IBM AIX 4.3.3
   - IBM AIX 5L V5.1
   - Sun Solaris Platforms
   - Sun Solaris 2.6
   - Sun Solaris 7
   - Sun Solaris 8
6. Windows Platforms
   - Windows NT 4.0 with SP4+ (Workstation, Server, Server Enterprise Edition)
   - Windows 2000 (Professional, Server, Advanced Server)
   - Windows XP Professional

2.2.3 Tripwire for Servers Check Point Edition

2.2.3.1 Hardware Requirements

Hardware components are not considered part of the TOE; however, the Tripwire for Servers CPE requires the following minimum hardware requirements to operate:

1. Sun Solaris operating systems
   - SPARC processor,
   - 30 MB free hard disk space,
   - 128 MB RAM
2. Windows operating systems
   - Intel Pentium class processor,
   - 20 MB free hard disk space,
   - 128 MB RAM

In addition, all systems require network connectivity to the Tripwire Manager product.

2.2.3.2 Software Requirements

The following software components are required for Tripwire for Servers CPE operation but are not considered to be part of the TOE:

1. Sun Solaris Platforms
   - Sun Solaris 7
   - Sun Solaris 8
2. Windows Platforms
   - Windows NT 4.0 with SP4+(Workstation, Server, Server Enterprise Edition)
   - Windows 2000 (Professional, Server, Advanced Server)
   - Windows XP Professional

2.3 TOE Logical Boundaries

Tripwire for Servers is a data integrity checking tool that can monitor stored data within the server's file system for any changes. When violations are identified, audit reports are generated identifying the violations discovered from the integrity check of a Tripwire for Servers machine(s). Tripwire for Servers also generates auditable events for database initializations, integrity checks, database updates, policy file updates, and TFS commands executed. Each auditable event includes the date and time of the event, event type, subject identity, and outcome of the event. All auditable events are stored and time stamped by the Tripwire for Servers underlying operating system.

Tripwire Manager allows the administrator to manage multiple installations of Tripwire for Servers software from a central location. The functions performed include performing integrity checks, updating the database, retrieving an audit report, editing the configuration file, editing the integrity policy file, and editing the policy enforcement schedule file.

As the Tripwire software is used to establish the security of machines throughout the network, it must itself be protected from intruders. The Tripwire Manager system provides internal security by using a combination of techniques, including Secured Sockets Layer technology, cryptographic signatures, and authentication.

All communication between the Tripwire Manager and Tripwire for Servers machines is protected using the Secured Sockets Layer (SSL) protocol to prevent eavesdropping. The Tripwire implementation of SSL uses 168-bit Triple DES encryption.

To prevent tampering and to protect against unauthorized modification, Tripwire files (policy file, database file, (optionally) report files, configuration file, site key file, local key file and agent configuration file) on each Tripwire for Servers machine are stored on disk in a binary-encoded, signed form, using El Gamal asymmetric cryptography with 1024 bit keys. The Tripwire Manager and Tripwire for Servers machines register each other by exchanging public authentication keys to facilitate secure communication. These keys are generated and distributed when each Tripwire for Servers machine is added to the Manager.

Cryptographic techniques do not protect against all attacks, such as the deletion of Tripwire data files. For maximum security, important files should be protected by the operating system or stored on read-only media. The integrity of those files should be checked on regular basis by

verifying their hashes using the Tripwire for Servers comparing utility against a baseline of data in a known good state.

Every communication between the Tripwire Manager and Tripwire for Servers machines is authenticated, allowing each party to verify the identity of the other. Tripwire Manager stores the site and local passphrases for each machine registered to that Manager. The passphrases are stored encrypted using triple DES with 168 bit keys based on a Manager passphrase. Because the Manager passphrase controls access to all the machines on the network, neither the passphrase nor the 168 bit key that it generates is permanently stored on disk. Instead, they are stored encrypted in the buffer for 5 minutes after the Manager passphrase is entered, and it is required to periodically re-enter the passphrase.

3 TOE Security Environment

This section describes the secure usage assumptions, threats, and organization security policies that together define TOE security environment.

3.1 Assumptions

A.No_Evil_Admin: Trustworthy Administrator
The Administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by TOE documentation.

A.HW/SW/FW_Func: Hardware/Software/Firmware function
The computer systems, software, and associated devices function correctly.

A. Phys_Acs: Physical Access
The TOE is located within a controlled access location that prevents unauthorized physical access by outsiders.

A. Peer: Connectivity to other systems
Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

A.Object_Cont: Object Control
It is assumed that only administrator(s) controls the objects (i.e. programs, scripts, etc) that the TOE calls using automated command execution.

3.2 Threats

This section contains threats identified for the TOE and the IT Environment. These threats exist in the environment that the TOE operates in and are countered by the TOE and the TOE environment.

T.Capture: Eavesdropping data communication
An attacker may eavesdrop on, or otherwise capture, data being transferred between Tripwire for Servers and Tripwire Manager.

T.Deletion: TOE data deletion
An attacker may attempt to delete or destroy TOE configuration data.

T.Modification: TOE data modification
An attacker may attempt to modify the TOE configuration data.

T.Integrity: IT System data integrity
The integrity of the IT system data may be compromised as a result of an attacker action or due to software, hardware, or user errors.

3.3 Organizational Security Policies

There are no organization security policies for this TOE.

4 Security Objectives

The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the TOE IT Environment.

4.1 Security Objectives for the TOE

This section identifies and describes the security objectives satisfied by the TOE.

O.Data_Prot: Data Protection
The TOE must protect its functions and data from deletion and/or unauthorized modification.

O.Audit_Data: Audit data generation
Tripwire for Servers must be able to generate audit data. Audit data must include the identity of authenticated operating system user responsible for each auditable event.

O.Audit_Rep_Gen: Audit report generation
The TOE must be able to generate audit reports that summarize any violations identified during an integrity check of system data.

O.Audit_Rep_Rev: Audit report review
The TOE must enable the user to review the audit reports that summarize any violations identified during an integrity check of system data.

O.Secure_Comm: Secure communications channel
The TOE must provide a secure communications channel between the Tripwire for Servers product and the Tripwire Manager product.

O.System_Integrity: System data integrity
The TOE must perform integrity checks on all system objects covered within the integrity policy.

O.System_Action: System action
The TOE must perform assigned actions upon detection of any violations of the integrity policy.

O.Iden_Auth: Identification and authentication
The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

O.TW_Agent: Tripwire agent
The TOE must provide the ability to configure the access rights to the Tripwire for Servers agent service.

O.TW_Config: Tripwire configuration
The TOE must provide the ability to configure access rights to the Tripwire for Servers configuration files.

4.2 Security Objectives for the Environment

The TOE Environment accomplishes the security objectives delineated within this section.

OE.Admin_Trust: Trustworthiness of the Administrator

Any administrator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.

OE. Sys_Assur: Validation of security function
Those responsible for the TOE must ensure that security-relevant software, hardware, and firmware are correctly functioning.

OE. Phys_Prot: Physical protection
Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

OE.Del_Inst: Delivery and Installation
Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

5 IT Security Requirements

This section defines functional and assurance requirements for the TOE, and the Security requirements for the IT environment.

5.1 TOE Security Functional Requirements

The following table represents a summary of the functional requirements defined for this ST.

Table 1: Functional Requirements for the TOE and its Environment

Functional Requirement:	Operations Performed:	CC Stated or Explicit:
FDP_ACC.1a: Subset access control	Assignment, Iteration	CC Part 2
FDP_ACC.1b: Subset access control	Assignment, Iteration	CC Part 2
FDP_ACF.1a: Security attribute based access control	Assignment, Iteration	CC Part 2
FDP_ACF.1b: Security attribute based access control	Assignment, Iteration	CC Part 2
FDP_SDI.2: Stored data integrity	Assignment, Refinement	CC Part 2
FMT_MSA.1a: Management of security attributes	Assignment, Selection, Iteration	CC Part 2
FMT_MSA.1b: Management of security attributes	Assignment, Selection, Iteration	CC Part 2
FMT_MSA.3a: Static attribute initialization	Assignment, Selection, Iteration	CC Part 2
FMT_MSA.3b: Static attribute initialization	Assignment, Selection, Iteration	CC Part 2
FMT_SMR.1: Security roles	Assignment	CC Part 2
FMT_SMF.1: Specification of Management Functions	Assignment	CC Part 2
FIA_UID.1: Timing of identification	Assignment	CC Part 2
FIA_UAU.1: Timing of authentication	Assignment	CC Part 2
FIA_ATD.1a: User attribute definition	Assignment, Iteration, Refinement	CC Part 2
FIA_ATD.1b: User attribute definition	Assignment, Iteration, Refinement	CC Part 2
FAU_SAR.1: Audit review	Assignment	CC Part 2
FAU_STG.1: Protected audit trail storage	Assignment	CC Part 2
FPT_STM.1: Reliable time stamps	None	CC Part 2
FAU_TWG.1: Tripwire Security audit data generation	N/A	Explicitly Stated
FAU_PRG.1: Tripwire Policy audit report generation	N/A	Explicitly Stated
FAU_PRR.1: Tripwire policy audit report review	N/A	Explicitly Stated
FTP_TWI.1: Tripwire Inter-TSF trusted channel	N/A	Explicitly Stated

5.1.1 FDP: User Data Protection

5.1.1.1 FDP_ACC.1a: Subset access control

FDP_ACC.1.1a

The TSF shall enforce the *Agent Configuration Policy* on *the access rights for the system administrator(s) to the authentication key file; schedule file; task file; log file; and/or agent configuration file.*

5.1.1.2 FDP_ACC.1b: Subset access control

FDP_ACC.1.1b

The TSF shall enforce the *Configuration Policy* on *the access rights for the system administrator(s) to the policy file; database file; report file; and/or configuration file.*

5.1.1.3 FDP_ACF.1a: Security attribute based access control

FDP_ACF.1.1a-NIAP-0416

The TSF shall enforce the *Agent Configuration Policy* to objects based on the following: *User Identity, and Tripwire site key.*

FDP_ACF.1.2a

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *after a successful Identification and Authentication to the OS, the system administrator(s) must present the appropriate passphrase associated with the Tripwire site key to gain access to the authentication key file, schedule file, task file, log file, and agent configuration file defined within the Agent Configuration Policy.*

FDP_ACF.1.3a-NIAP-0405-NIAP-0407

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *no additional rules.*

FDP_ACF.1.4a-NIAP-0407

The TSF shall explicitly deny access of subjects to objects based on the following rules: *no additional explicit denial rules.*

5.1.1.4 FDP_ACF.1b: Security attribute based access control

FDP_ACF.1.1b-NIAP-0416

The TSF shall enforce the *Configuration Policy* to objects based on the following: *User Identity, and Tripwire site key or local key*.

FDP_ACF.1.2b

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *after a successful Identification and Authentication to the OS, system administrator(s) must present the appropriate passphrases associated with the Tripwire site key or local key to gain access to the policy file, database file, report file, and configuration file defined within the Configuration Policy.*

FDP_ACF.1.3b-NIAP-0405-NIAP-0407

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *no additional rules.*

FDP_ACF.1.4b-NIAP-0407

The TSF shall explicitly deny access of subjects to objects based on the following rules: *no additional explicit denial rules.*

5.1.1.5 FDP_SDI.2: Stored data integrity

FDP_SDI.2.1

The ***Tripwire for Servers*** TSF shall monitor ***either manually or in accordance with the schedule file the*** user data stored within the TSC for *integrity errors* on all objects, based on the following attributes: *the hashed values of objects stored within the systems most recently updated database.*

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall *generate an audit report; and (based on the parameters of the configuration file), send an email to the system administrator, and/or take the actions identified on using the automated command execution functionality.*

5.1.2 FMT: Security Management

5.1.2.1 FMT_MSA.1a Management of security attributes

FMT_MSA.1.1a-NIAP-0405

The TSF shall enforce the *Agent Configuration Policy* to restrict the ability to **modify** the security attributes *of the access rights to the authentication key file, schedule file task file, log file, and agent configuration file* to *the system administrator(s).*

5.1.2.2 FMT_MSA.1b Management of security attributes

FMT_MSA.1.1b-NIAP-0405

The TSF shall enforce the *Configuration Policy* to restrict the ability to **modify** the security attributes *of the access rights to the policy file, database file, report file, and configuration file* to *the system administrator(s).*

5.1.2.3 FMT_MSA.3a Static attribute initialization

FMT_MSA.3.1a-NIAP-0429

The TSF shall enforce the *Agent Configuration Policy* to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2a-NIAP-0405

The TSF shall allow the *system administrator(s)* to specify alternative initial values to override the default values when an object or information is created.

5.1.2.4 FMT_MSA.3b Static attribute initialization

FMT_MSA.3.1b-NIAP-0429

The TSF shall enforce the *Configuration Policy* to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2b-NIAP-0405

The TSF shall allow the *system administrator(s)* to specify alternative initial values to override the default values when an object or information is created.

5.1.2.5 FMT_SMR.1 Security roles

FMT_SMR.1.1-NIAP-0405

The TSF shall maintain the roles *system administrator*.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

5.1.2.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1-INTERP-065

The TSF shall be capable of performing the following security management functions: *Access control, Authentication, and Integrity check.*

5.1.3 FIA: Identification & Authentication

5.1.3.1 FIA_UID.1: Timing of identification

FIA_UID.1.1

The TSF shall allow *request for help on the login procedure* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.2 FIA_UAU.1: Timing of authentication

FIA_UAU.1.1

The TSF shall allow *request for help on the login procedure* on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

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

5.1.3.3 FIA_ATD.1a: User attribute definition

FIA_ATD.1.1a

The ***Tripwire for Servers*** TSF shall maintain the following list of security attributes belonging to ***the one*** individual user ***for each server***: *Local Key & Passphrase or Site Key & Passphrase*.

5.1.3.4 FIA_ATD.1b: User attribute definition

FIA_ATD.1.1b

The ***Tripwire Manager*** TSF shall maintain the following list of security attributes belonging to ***the one*** individual user ***for each manager***: *Manager Key & Passphrase and the respective Site key or Local key & passphrases of all Tripwire for Servers products that are registered with the Tripwire Manager*.

5.1.4 FAU: Security Audit

5.1.4.1 FAU_SAR.1: Audit review

FAU_SAR.1.1-NIAP-0405

The TSF shall provide *system administrators* with the capability to read *all* from the audit records.

FAU_SAR.1.2

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

5.1.4.2 FAU_STG.1: Protected audit trail storage

FAU_STG.1.1-NIAP-0405-NIAP-0422

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2-NIAP-0423-NIAP-0429

The TSF shall be able to **prevent** unauthorized modifications.

5.1.5 FPT: Protection of TSF

5.1.5.1 FPT_STM.1: Reliable time stamps

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

5.2 Explicitly Stated TOE Functional Requirements

5.2.1 FAU: Tripwire Security Audit

5.2.1.1 FAU_TWG.1: Tripwire Security audit data generation

FAU_TWG.1.1

The Tripwire for Servers TSF shall be able to generate an audit record of the following auditable events:

a) All auditable events for the not specified level of audit; and

b) Database initializations, integrity checks, database updates and policy file updates.

FAU_TWG.1.2

The Tripwire for Servers TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event (informational, warning, or error), and host identity; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, the authenticated OS user performing a TFS action, event ID, and event description.

5.2.1.2 FAU_PRG.1: Tripwire Policy audit report generation

FAU_PRG.1.1

The Tripwire for Servers TSF shall be able to generate an audit report based on the following items listed in the integrity policy file :

a) All objects that were detected to be added, removed, or modified from the existing file system or registry structure.

FAU_PRG.1.2

The Tripwire for Servers TSF shall record within each entry of the audit report at least the following information:

a) Date and time of the creation of the report, TFS host name, TFS host ID, TFS account name responsible for report creation; and

b) For each audit report, based on the auditable definitions of the functional components included in the ST, number of violations identified, maximum severity, total number of integrity errors, total number of objects scanned, location of policy file, location of configuration file, location of database file, location of Tripwire command issued, IP address of TFS, and date & time of last database update.

5.2.1.3 FAU_PRR.1: Tripwire policy audit report review

FAU_PRR.1.1

The TSF shall provide the Tripwire for Servers user and Tripwire Manager user with the capability to read all information from the audit reports.

FAU_PRR.1.2

The TSF shall provide the audit reports in one or a combination of the following formats:

1. Visible to the screen,
2. Stored as Html,
3. Stored as XML, and/or
4. Sent via email.

5.2.2 FTP: Tripwire Trusted Path/Channels

5.2.2.1 FTP_TWI.1: Tripwire Inter-TSF trusted channel

FTP_TWI.1.1

The Tripwire Manager TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides protection of the channel data from modification or disclosure.

FTP_TWI.1.2

The Tripwire Manager TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.

FTP_TWI.1.3

The Tripwire Manager TSF shall initiate communication via the trusted channel for performing integrity checks, updating database, retrieving audit report, editing configuration file, editing integrity policy file, editing policy enforcement schedule file, sending a request to a Tripwire for Servers machine to be registered.

5.3 TOE Security Assurance Requirements

The assurance requirements for this Security Target, taken from Part 3 of the CC, comprise the EAL1 level of assurance. The assurance components are summarized in the following table.

Table 2: Assurance Components (EAL1)

Assurance Class	Assurance Components	
Class ACM: Configuration Management	ACM_CAP.1	Version numbers
Class ADO: Delivery and Operation	ADO_IGS.1	Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_RCR.1	Informal correspondence demonstration
Class AGD: Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Class ATE: Tests	ATE_IND.1	Independent testing - conformance

5.3.1 ACM: Configuration management

5.3.1.1 ACM_CAP.1: Version numbers

The reference for the TOE shall be unique to each version of the TOE.[ACM_CAP.1.1C]
The developer shall provide a reference for the TOE.[ACM_CAP.1.1D]
The TOE shall be labeled with its reference.[ACM_CAP.1.2C]

5.3.2 ADO: Delivery and operation

5.3.2.1 ADO_IGS.1-INTERP-051: Installation, generation, and start-up procedures

The installation, generation and start-up documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.[ADO_IGS.1.1C]
The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.[ADO_IGS.1.1D]

5.3.3 ADV: Development

5.3.3.1 ADV_FSP.1: Informal functional specification

The functional specification shall describe the TSF and its external interfaces using an informal style.[ADV_FSP.1.1C]
The developer shall provide a functional specification.[ADV_FSP.1.1D]
The functional specification shall be internally consistent.[ADV_FSP.1.2C]
The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.[ADV_FSP.1.3C]
The functional specification shall completely represent the TSF.[ADV_FSP.1.4C]

5.3.3.2 ADV_RCR.1: Informal correspondence demonstration

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.[ADV_RCR.1.1C]
The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.[ADV_RCR.1.1D]

5.3.4 AGD: Guidance documents

5.3.4.1 AGD_ADM.1: Administrator guidance

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.[AGD_ADM.1.1C]
The developer shall provide administrator guidance addressed to system administrative personnel.[AGD_ADM.1.1D]
The administrator guidance shall describe how to administer the TOE in a secure manner.[AGD_ADM.1.2C]
The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.[AGD_ADM.1.3C]
The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.[AGD_ADM.1.4C]

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.[AGD_ADM.1.5C]
The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.[AGD_ADM.1.6C]
The administrator guidance shall be consistent with all other documentation supplied for evaluation.[AGD_ADM.1.7C]
The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.[AGD_ADM.1.8C]

5.3.4.2 AGD_USR.1: User guidance

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.[AGD_USR.1.1C]
The developer shall provide user guidance.[AGD_USR.1.1D]
The user guidance shall describe the use of user-accessible security functions provided by the TOE.[AGD_USR.1.2C]
The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.[AGD_USR.1.3C]
The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.[AGD_USR.1.4C]
The user guidance shall be consistent with all other documentation supplied for evaluation.[AGD_USR.1.5C]
The user guidance shall describe all security requirements for the IT environment that are relevant to the user.[AGD_USR.1.6C]

5.3.5 ATE: Tests

5.3.5.1 ATE_IND.1: Independent testing - conformance

The TOE shall be suitable for testing.[ATE_IND.1.1C]
The developer shall provide the TOE for testing.[ATE_IND.1.1D]

5.4 Strength of Function Claim

No strength of security function claim is made for this TOE.

6 TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions implemented by the TOE and its environment to meet the security requirements stated within section 5 of this ST. A mapping of the security functions identified and their related security requirements can be found within Table 6, in section 8.4.1 of this ST.

6.1.1 Access Control

FDP_ACC.1a	FDP_ACC.1b	FDP_ACF.1a
FDP_ACF.1b	FMT_MSA.1a	FMT_MSA.1b
FMT_MSA.3a	FMT_MSA.3b	FMT_SMF.1

Tripwire for Servers uses a number of files to assess system security:

- Policy file (to specify how Tripwire software monitors the system);
- Database file (the center of integrity assessment);
- Report files (records the changes detected during an integrity check that violate the rules in the policy file);
- Configuration file (stores system-specific information that controls Tripwire operation);
- Site Key file and Local Key file (store public and private keys used to sign Tripwire files cryptographically);
- Agent Configuration file (stores information that each machine uses to communicate with the Tripwire Manager);
- Authentication Key file (stores the keys Tripwire Agent uses to authenticate connections with Tripwire Manger);
- Schedule file (stores scheduling information for integrity check);
- Task file (stores information about completed tasks); and
- Log file.

Tripwire for Server implements the Configuration Policy (*tw.cfg*) and the Agent Configuration Policy (*agent.cfg*) to set the access rights to these critical security components. For each file, there is a parameter defined in the Configuration file or Agent Configuration file that can be used to set the TFS file permissions:

tw.cfg

File:	Parameter:	Default File permissions
Policy file	POLICYRIGHT	Write by owner / Read by all
Database file	DBRIGHTS	Write by owner / Read by all
Report files	REPORTRIGHT	Write by owner / Read by all
Configuration file	CFGRIGHTS	Write by owner / Read by all

agent.cfg

File:	Parameter:	Default file permissions
Authentication Key file	AUTHKEYFILERIGHTS	Write by owner / Read by all
Schedule file	SCHEDULEFILERIGHTS	Write by owner / Read by all
Task file	TASKFILERIGHTS	Write by owner / Read by all
Log file	LOGFILERIGHTS	Write by owner / Read by all
Agent Configuration file	AGENTCFGRIGHTS	Write by owner / Read by all

All these files are stored on the Tripwire for Servers machine in binary-encoded and signed form using El Gamal asymmetric cryptography with 1024 bit keys.

Access to the Tripwire files is controlled by the operating systems and additional Tripwire for Servers mechanisms. A user must first authenticate to the host operating system by providing the correct identification and authentication token. Additionally, the user must present the appropriate passphrase associated with the key to edit or modify signed Tripwire files.

TFS uses two sets of keys:

- Site key – used to protect the policy file and configuration files (*tw.cfg*, *agent.cfg)*, which can be used across an entire site.
- Local key – used to protect database and report files, which are specific to a particular system.

Additionally, the site key is used to protect the Authentication key file, Schedule file, Task file, and Log File.

Tripwire Manager stores the site and local passphrases for each machine registered to that Manager in the *console.dat* file. The passphrases are stored encrypted using triple DES with 168 bit keys based on a Manager passphrase.

When a Tripwire Manager sends a command to a Tripwire for Servers machine that requires a site or local passphrase, the Manager prompts the user for the Manager passphrase. This passphrase is used to de-crypt the passphrases in *console.dat,* allowing the Manager to access and send the appropriate passphrase for the Tripwire for Servers machine.

6.1.2 Auditing

FAU_TWG.1 FAU_SAR.1 FPT_STM.1 FAU_STG.1

The auditing function provides the ability to generate auditable events for the TOE. These auditable events will include: database initializations, integrity checks, database updates, policy file updates, and TFS commands executed. Each auditable event logged includes: date and time of the event, type of event, host identity, the authenticated OS user, event ID, and event description.

Audit data will be saved in suitable form for the administrator to interpret the information and will be protected from unauthorized deletion. The file protection is provided by changing the permissions for the Tripwire for Servers directory and files to full control for authorized administrators only in UNIX. In the Windows environment file protection is provide by giving write and execute permissions only to users who are authorized to administer Tripwire software

in Windows (including Tripwire Agent service if it is specified as user). The audit records can be viewed using a proper OS editor.

In addition, the auditing function provides the ability to generate audit reports for violations discovered from the integrity check of a Tripwire for Servers machine. The TOE takes a snapshot of the files in a known good state and stores a hash value associated with each file being monitored in the integrity policy file. Violations are identified by comparing objects listed in the integrity policy file against the objects currently existing on the machine. Any object detected to be added, removed, or modified from the existing file system or registry structure is identified as a violation and is included in the audit report.

The following summary information is provided for each audit report:

- number of violations identified,
- maximum severity,
- total number of integrity errors,
- total number of objects scanned,
- location of policy file,
- location of configuration file,
- location of database file,
- location of Tripwire command issued,
- IP address of TFS, and
- date & time of last database update.

Date and time of the creation of the report, TFS host name, TFS host ID, and TFS account name responsible for report creation will be part of audit report as well.

For each audit report, the TOE also provides the capability to view the audit reports on the screen and to store them in one, or a combination of, the following formats: HTML, XML, and/or sent via email. By default, Tripwire report files are named ($HOSTNAME)-($DATE).twr.

6.1.3 Authentication

FIA_UID.1	FIA_UAU.1	FIA_ATD.1a
FIA_ATD.1b	FMT_SMR.1	FMT_SMF.1

To gain access to the TOE data and functionality, the authorized users must first successfully identify and authenticate themselves via the operating system (UNIX/Windows) login process. To authenticate a user at logon, UNIX uses techniques such as username/password pair, Kerberos V4/V5, and proprietary schemes. After logon, every process a user creates has the same User ID and Group ID and thus the access rights of the user referenced by the User ID. Windows security relies on user credentials and object permissions. A user authenticates by providing a username/password pair. When a user logs on to a Windows-based machine or domain, Windows authenticates the user and identifies the user by using a unique security identifier (SID).

The authentication function provides the definition of the security attributes identified for both the Tripwire Manager and Tripwire for Servers products. Security attributes for the Tripwire for Servers product include the local key and site key along with their associated passphrases.

Security attributes for the Tripwire Manager product are the manager key along with its associated passphrase.

After successful authentication to the OS, in order to perform the TOE functionality, the user must authenticate to the TFS using the local key & passphrase or site key & passphrase authentications. To authenticate to the TWM, the user must present the manager key & passphrase.

TWM stores the site and local passphrases for each machine registered to that Manager in the *console.dat* file. The passphrases are stored encrypted using triple DES with 168 bit keys based on a manager passphrase. The Agent Configuration file stores information that each TFS machine uses to communicate with the TWM. When a TWM sends a command to a TFS machine that requires a site or local passphrase, the Manager prompts the user for the manager passphrase. This passphrase is used to de-crypt the passphrases in *console.dat*, allowing the Manager to access and send the appropriate passphrase for the Tripwire for Servers machine.

6.1.4 Communications

FTP_TWI.1

The communication function provides a secure communication channel between the Tripwire Manager and the Tripwire for Servers products. All communication between the Tripwire Manager and Tripwire for Servers machines is protected using the Secured Sockets Layer (SSL) protocol to prevent eavesdropping. The Tripwire implementation of SSL uses 168 bit Triple DES encryption.

The Tripwire Manager and Tripwire for Servers machines register each other by exchanging public authentication keys to facilitate secure communication. These keys are generated and distributed when each Tripwire for Servers machine is added to the Manager.

Once the Tripwire Manager and the Tripwire for Servers machines have exchanged keys, every time a connection is made between the two, each side authenticates the other by generating a random data packet and requesting that the other side digitally sign it. The signed packet can be verified using the public key of the signer.

Tripwire Manger uses the secure communication channel to perform integrity checks, update the database, retrieve audit report, edit configuration file, edit integrity policy file, edit policy enforcement schedule file, and send a request to a Tripwire for Servers machine to be registered.

6.1.5 Integrity Checking

FAU_PRG.1 FAU_PRR.1 FDP_SDI.2
FMT_SMF.1

The integrity checking function provides the Tripwire for Servers product with the capability of monitoring for any changes in the data stored within the system's file system. This process is provided by comparing the hashed values of objects stored within the system's most recently updated database against the hashed values of the objects currently in the file system. The list of objects to be monitored is determined by the integrity policy file.

When violations are identified, meaning an inconsistency between the two hashed values of any object to be monitored, a report is generated identifying these violations. The TOE will store the report and can also send it to an administrator by email (if configured to do so). In addition, Tripwire for Servers can automatically execute commands defined within the policy file in response to violations, or every time integrity checks are performed. Reviewing the report will help the administrator to determine if the violations are actually authorized changes (such as installing an upgrade or new application) or if the changes are considered to be malicious or unauthorized. Based on that decision, the system administrator can update the database (so changes no longer show up as violations) or take steps to restore the correct files to the system.

6.2 Assurance Measures

The assurance requirements for this TOE are the EAL1 requirements, which stress assurance through Tripwire's actions which are within the bounds of current best-commercial practice. These assurance measures provide, primarily by review of Tripwire-supplied evidence, independent confirmation that these actions have been competently performed. They also include the following independent, third-party analysis:

1. Confirmation of system generation and installation procedures
2. Verification that the system security state is not misrepresented
3. Independent functional testing

A mapping is provided between the Assurance Requirements from Section 5.3 and the Assurance Measures, which are intended to satisfy the Assurance Requirements. As shown in the Table 7, the Assurance Measures are provided in the form of references to the relevant and appropriate document associated with each requirement.

7 PP Claims

There are no protection profile claims for this security target.

8 Rationale

This section demonstrates the completeness and consistency of this ST.

- Traceability: The security objectives for the IT and environment are explained in terms of OSPs, threats countered, and assumptions met. The SFRs are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following:
  a) security objectives to OSPs and/or threats countered
  b) objectives to assumptions met
  c) SFRs to objectives met
- Assurance Level: A justification is provided for selecting an EAL1 level of assurance for this ST.
- Dependencies: A mapping is provided as evidence that all dependencies are met.

8.1 Security Objectives Rationale

This section provides evidence demonstrating coverage of the TOE security environment by the IT security objectives. The security objectives were derived exclusively from statements of OSPs, threats and assumptions. The following table demonstrates the mapping between the assumptions, threats and policies to the security objectives is completed, and the following discussion provides evidence of coverage for each statement of TOE security environment.

Table 3: Security Environment mapped to Security Objectives

	O.Data_Prot	O.Audit_Data	O.Audit_Rep_Gen	O.Audit_Rep_Rev	O.Secure_Comm	O.System_Integrity	O.System_Action	O.Iden_Auth	O.Time_Stamp	O.TW_Agent	O.TW_Config	OE.Admin_Trust	OE. Sys_Assur	OE. Phys_Prot	OE.Del_Inst
A.No_Evil_Admin												X			X
A.HW/SW/FW_Func													X		
A. Phys_Acs														X	
A. Peer												X			X
A.Object_Cont												X		X	X
T.Capture					X										
T.Deletion	X	X						X							
T.Modification	X	X	X	X		X	X	X	X						
T.Integrity		X	X	X		X	X	X	X	X	X				

8.1.1 Assumptions

A.No_Evil_Admin: Trustworthy Administrator
The Administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by TOE documentation.

Coverage Rationale:

The OE.Admin_Trust objective provides that any administrator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.

The OE.Del_Inst objective ensures that the TOE is installed and managed in a manner that is consistent with the administrator and user guides.

A.HW/SW/FW_Func: Hardware/Software/Firmware function
The computer systems, software, and associated devices function correctly.

Coverage Rationale:

The OE.Sys_Assur objective provides that software, hardware, and firmware will function correctly.

A. Phys_Acs: Physical Access
The TOE is located within a controlled access location that prevents unauthorized physical access by outsiders.

Coverage Rationale:

The OE.Phys_Prot objective ensures that those parts of the TOE critical to security policy are protected from any physical attack

A. Peer: Connectivity to other systems
Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

Coverage Rationale:

The OE.Del_Inst objective ensures that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.

The OE.Admin_Trust objective provides that any administrator of the TOE must be trusted.

A.Object_Cont: Object Control
It is assumed that only administrator(s) controls the objects (i.e. programs, scripts, etc) that the TOE calls on automated command execution.

Coverage Rationale:

The OE.Phys_Prot objective ensures that those parts of the TOE critical to security policy are protected from any physical attack.

The OE.Admin_Trust objective provides that any administrator of the TOE will not disclose their authentication credentials to any individual not authorized for access to the TOE.

The OE.Del_Inst objective ensures that the TOE is installed and managed in a manner which is consistent with the administrator and user guides.

8.1.2 Threats

T.Capture: Eavesdropping data communication
An attacker may eavesdrop on, or otherwise capture, data being transferred between Tripwire for Servers and Tripwire Manager.

Coverage Rationale:

The O.Secure_Comm objective provides secure communications channel between the Tripwire for Servers product and the Tripwire Manager product.

T.Deletion: TOE data deletion
An attacker may attempt to delete or destroy TOE configuration data.

Coverage Rationale:

The deleting or destroying of the Tripwire configuration data will compromise the integrity check for the TSF data.

The O.Data_Prot objective addresses this threat by providing the TOE self-protection. The identification and authentication to the OS protects TSF data by allowing only authorized user to gain access to the TOE configuration data (O.Iden_Auth). The O.Audit_Data objective counters this threat by requiring the TOE to audit attempts for data accesses.

T.Modification: TOE data modification
An attacker may attempt to modify the TOE configuration data.

Coverage Rationale:

An attacker may attempt to modify the TOE configuration files in a manner that the potential violations can go undetected during the integrity check, and thus the integrity for the TSF data will be compromised.

The O.Data_Prot objective addresses this threat by providing the TOE self-protection. The O.Iden_Auth objective protects the TSF data from an unauthorized user (I&A from the OS) and provides the attributes for the authentication process to both the Tripwire for Servers and Tripwire Manager. These attributes will be checked prior to allowing any modifications to be made to any configurations within the Tripwire for Servers.

The O.System_Integrity addresses this threat by detecting any violation on all system objects covered within the integrity policy. The O.Audit_Data objective provides that Tripwire for Servers will generate audit data that will be included into the audit reports (O.Audit_Rep_Gen). Those reports will be reviewed (O.Audit_Rep_Rev) and proper action will be taken to ensure the TOE configuration data integrity (O.System_Action). All audit data will be time-stamped from the OS (O.Time_Stamp).

T.Integrity: IT System data integrity
The integrity of the IT system data may be compromised as a result of an attacker action or due to software, hardware, or user errors.
Coverage Rationale:

The O.Iden_Auth objective provides that only authorized user will be able to access and mange the TSF data (Identification and Authentication to the OS). This objective also provides the attributes for authentication to both the Tripwire for Servers and Tripwire

Manager, which will be checked prior to allowing any modifications to be made to any configurations within the Tripwire for Servers. The O.TW_Agent and O.TW_Config objectives provide the ability to configure the access rights to the Tripwire for Servers agent service and to the Tripwire for Servers configuration.

The O.System_Integrity provides the ability to detect any violation on all system objects covered within the integrity policy for the IT system caused as a result of an attack, or due to software, hardware, or user errors. The O.Audit_Data objective provides that Tripwire for Servers will generate audit data that will be included into the audit reports (O.Audit_Rep_Gen).

Based on the generated and reviewed reports (O.Audit_Rep_Rev), the proper actions will be taken from the administrator(s) to ensure the integrity of the IT system data (O.System_Action). All audit data will be time-stamped from the OS (O.Time_Stamp).

8.2 Security Requirements Rationale

This section provides evidence demonstrating that the security objectives for the TOE and the TOE IT Environment are satisfied by the security requirements. The mapping demonstrate that all TOE security requirements can be traced back to one or more TOE security objective(s), and all TOE security objectives are supported by at least one security requirement.

8.2.1 Security Functional Requirements Coverage

This section provides evidence demonstrating that the security objectives of the TOE are satisfied by the security requirements. The following table represents the mapping of the security requirement to security objective.

Table 4: Mapping of Security Objectives to Security Requirements

	O.Data_Prot	O.Audit_Data	O.Audit_Rep_Gen	O.Audit_Rep_Rev	O.Secure_Comm	O.System_Integrity	O.System_Action	O.Iden_Auth	O.Time_Stamp	O.TW_Agent	O.TW_Config
FDP_ACC.1a										X	
FDP_ACC.1b											X
FDP_ACF.1a										X	
FDP_ACF.1b											X
FDP_SDI.2						X	X				
FIA_UID.1		X		X				X			
FMT_MSA.3a						X				X	
FMT_MSA.3b						X					X
FMT_MSA.1a						X				X	
FMT_MSA.1b						X					X
FMT_SMR.1						X				X	X
FMT_SMF.1										X	X
FIA_UAU.1		X		X				X			
FIA_ATD.1a								X			
FIA_ATD.1b								X			
FAU_SAR.1				X		X					
FAU_STG.1	X					X					
FPT_STM.1		X							X		
FAU_TWG.1		X									
FAU_PRG.1	X		X			X	X				
FAU_PRR.1				X							
FTP_TWI.1					X						

The following discussion provides detailed evidence to justify this mapping.

8.2.2 Requirements Form a Consistent Whole

O.Data_Prot: Data Protection
The TOE must protect its functions and data from deletion and/or unauthorized modification.
Coverage Rationale:

> The TOE is required to protect configuration data from any deletion and unauthorized modification [FAU_TWG.1]. The TOE is required to detect changes (add, remove, modify) to all objects listed within integrity policy file [FAU_PRG.1].

O.Audit_Data: Audit data generation
Tripwire for Servers must be able to generate audit data. Audit data must include the identity of authenticated operating system user responsible for each auditable event.

Coverage Rationale:

The TOE is required to generate records for security relevant events and information describing the security relevant events [FAU_TWG.1]. The TOE will associate the identity of an individual [FIA_UAU.1] and [FIA_UID.1] with audit events created by that individual. The recording of the subject identity provides accountability for each recorded event. [FPT_STM.1] partially implements the objective by providing confidence in the time-stamp associated with events audited by the TOE.

O.Audit_Rep_Gen: Audit report generation

The TOE must be able to generate audit reports that summarize any violations identified during an integrity check of system data.

Coverage Rationale:

The Tripwire for Server is required to generate audit reports to an integrity check for the IT System [FAU_PRG.1].

O.Audit_Rep_Rev: Audit report review

The TOE must enable the user to review the audit reports that summarize any violations identified during an integrity check of system data.

Coverage Rationale:

The Tripwire for Server and Tripwire Manger are required to be able to review generated audit reports to an integrity check for the IT System [FAU_PRR.1]. The information will be recorded in a manner suitable for user to interpret it and the access rights to the audit trail will be provided only to the authorized administrator [FAU_SAR.1]. [FIA_UAU.1] and [FIA_UID.1] partially implement this objective by authenticating and identifying the identity of an individual who requires access to review the audit reports.

O.Secure_Comm: Secure communications channel

The TOE must provide a secure communications channel between the Tripwire for Servers product and the Tripwire Manager product.

Coverage Rationale:

[FTP_TWI.1] implements the objective by providing a creation of a trusted communication channel between the Tripwire Manager and other trusted IT products (Tripwire for Servers) for performing the following security critical operations: integrity checks; updating database; retrieving audit report; editing configuration file; editing integrity policy file; editing policy enforcement schedule file; sending a request to a Tripwire for Servers product to be registered.

O.System_Integrity: System data integrity

The TOE must perform integrity checks on all system objects covered within the integrity policy.

Coverage Rationale:

The Tripwire for Server is required to generate audit reports for the integrity check on the objects of the IT System listed within the integrity policy [FAU_PRG.1]. These audit reports will be stored [FDP_SDI.2]. Only the user on an administrator role [FMT_SMR.1] will be able to specify alternative initial values to override the default values of the security attributes that are used to enforce the SFP. [FAU_MSA.1a]/ [FAU_MSA.1b] and [FAU_MSA.3a]/[FAU_MSA.3b] partially implement the objective by restricting the ability to modify security attributes, and to enforce the default values. [FAU_STG.1] partially implements the objective by restricting the ability to delete or

modify the information in the audit trail.[FAU_SAR.1] partially implements the objective by enforcing restrictions on the access rights to the audit trail only to the user on an administrator role.

O.System_Action: System action
The TOE must perform assigned actions upon detection of any violations of the integrity policy.
Coverage Rationale:

The Tripwire for Server is required to generate audit reports for the integrity check on the objects of the IT System listed within the integrity policy [FAU_PRG.1], and to perform an action upon detection of the integrity error to the IT system data that the TOE checks the integrity [FDP_SDI.2].

O.Iden_Auth: Identification and authentication
The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

Coverage Rationale:

[FIA_UAU.1, FIA_UID.1] implement the objective by requiring the authorized users to identify and authenticate themselves before giving access to the TOE data and functions. [FIA_ATD.1a] and [FIA_ATD.1b] implement the objective by associating attributes with each individual user so that once a user is authenticated the attributes may be used to enforce the TSPs, respectively for Tripwire for Server and Tripwire Manager.

O.Time_Stamp: Time stamp

The TOE must provide the time stamp for the audit data generation.

Coverage Rationale:

[FPT_STM.1] implements reliable time-stamp for the TSF.

O.TW_Agent: Tripwire agent
The TOE must provide the ability to configure the access rights to the Tripwire for Servers agent service.

Coverage Rationale:

[FDP_ACC.1a] implements the objective by defining an access control policy that allows authorized users to control access and to share the objects they own. Only the users on an administrator role [FMT_SMR.1] will be able to perform the security management functions [FMT_SMF.1] and will be allowed to specify alternative initial values to override the default values of the security attributes that are used to enforce the SFP. [FDP_ACF.1a] implements the objective by enforcing the rules that implement the various access control SFPs defined for the TOE. [FAU_MSA.1a] and [FAU_MSA.3a] partially implement the objective by restricting the ability to modify security attributes, and to enforce the default values.

O.TW_Config: Tripwire configuration
The TOE must provide the ability to configure access rights to the Tripwire for Servers configuration files.

Coverage Rationale:

[FDP_ACC.1b] implements the objective by defining an access control policy that allows authorized users to control access and to share the objects they own. Only the users on an administrator role [FMT_SMR.1] will be able to perform the security management functions [FMT_SMF.1] and to specify alternative initial values to

override the default values of the security attributes that are used to enforce the SFP. [FDP_ACF.1b] implements the objective by enforcing the rules that implement the various access control SFPs defined for the TOE. [FAU_MSA.1b] and [FAU_MSA.3b] partially implement the objective by restricting the ability to modify security attributes, and to enforce the default values.

8.2.3 Justification of Explicitly Stated Security Functional Requirements

This section identifies the appropriateness for the explicitly stated requirements of the TOE.

8.2.3.1 Explicitly Stated Requirements for the TOE

FAU_TWG.1 (Tripwire Security audit data generation)

FAU_TWG.1 was explicitly stated in this ST because the functionality alone is not intended to meet FAU_GEN.1, in that it does not record the start-up and shutdown of the audit function. However it does satisfy the rest of the requirement's functionalities as defined within the CC context. Therefore, an explicit requirement was stated to provide appropriate definition to the intended functionality for audit data generation.

FAU_PRG.1 (Policy audit report generation)

FAU_PRG.1 is explicitly stated in this ST because FAU_GEN.1 is not stated in a manner for audit reports, rather for audit records. Therefore, an explicit requirement was stated to provide definition to the intended functionality for the policy audit report generation.

FAU_PRR.1 (Policy audit report review)

FAU_PRR.1 is explicitly stated in this ST because FAU_SAR.1 it does not provide review of audit reports, but review of audit records. In addition, the explicitly stated requirement was tailored to identify the different formats that should be provided for an audit report. Therefore, an explicit requirement was stated to provide definition to the intended functionality for a policy audit report review.

FTP_TWI.1 (Tripwire Inter-TSF trusted channel)

FTP_TWI.1 was explicitly stated because TSF does not provide the endpoint to endpoint identification that is required in FTP_ITC.1 within the CC. However it does satisfy the rest of the requirement's functionalities as defined within the CC context. Therefore, an explicit requirement was stated to provide appropriate definition to the intended functionality for the secure communications channel within Tripwire products.

8.2.4 Requirements are Justified

The following table provides a cross reference for each security functional requirement within this ST and their dependencies, showing overall that all requirements are satisfied.

Table 5: Security Functional Requirements Dependencies Mapping

Security Functional Requirements	Dependencies	Included
FDP_ACC.1a	FDP_ACF.1a	Yes
FDP_ACC.1b	FDP_ACF.1b	Yes
FDP_ACF.1a	FDP_ACC.1a	Yes
	FMT_MSA.3a	Yes
FDP_ACF.1b	FDP_ACC.1b	Yes
	FMT_MSA.3b	Yes
FDP_SDI.2	No dependencies	N/A
FMT_MSA.3a	FMT_MSA.1a	Yes
	FMT_SMR.1	Yes
FMT_MSA.3b	FMT_MSA.1b	Yes
	FMT_SMR.1	Yes
FMT_MSA.1a	FDP_ACC.1a	Yes
	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_MSA.1b	FDP_ACC.1b	Yes
	FMT_SMF.1	Yes
	FMT_SMR.1	Yes
FMT_SMR.1	FIA_UID.1	Yes
FMT_SMF.1	No dependencies	N/A
FIA_UID.1	No dependencies	N/A
FIA_UAU.1	FIA_UID.1	Yes
FIA_ATD.1a	No Dependencies	N/A
FIA_ATD.1b	No Dependencies	N/A
FAU_SAR.1	FAU_TWG.1 – replacing FAU_GEN.1	Yes
FAU_STG.1	FAU_TWG.1 – replacing FAU_GEN.1	Yes
FPT_STM.1	No Dependencies	N/A
FAU_TWG.1	FPT_STM.1	Yes
FAU_PRG.1	No Dependencies	N/A
FAU_PRR.1	No Dependencies	N/A
FTP_TWI.1	No Dependencies	N/A

8.3 EAL Justification

Tripwire has chosen to pursue an EAL 1 assurance level of the TOE because of the government customer requirements that are mandated by NSTISS Policy 11. This policy requires a Common Criteria certification for all products to be used within systems used for entering, processing, storing, displaying, or transmitting national security information.

8.4 TOE Summary Specification Rationale

8.4.1 Security Functions Satisfy Functional Requirements

The following table represents a mapping between the security functions identified in Clause 6.1 to their related security functional requirements identified in section 5.1.

Table 6: Mapping of Security Functions to Security Functional Requirements

Security Functions (6.1)	Security Functional Requirements	Rationale
Access Control	**FDP_ACC.1a** **FDP_ACC.1b** **FDP_ACF.1a** **FDP_ACF.1b** **FMT_MSA.1a** **FMT_MSA.1b** **FMT_MSA.3a** **FMT_MSA.3b** **FMT_SMF.1**	The TOE implements configuration policy and agent configuration policy to control the control the access to the critical security components within the Tripwire for Servers product. The *FDP_ACC.1a* and *FDP_ACC.1b* implement the enforcing access control to critical security components of the TOE that are defined within the agent configuration policy and configuration policy, the *FDP_ACF.1a* and *FDP_ACF.1b* describe the rules for the access control policy based on the security attributes. The TSF provide default values for security attributes (*FMT_MSA.3a* and *FMT_MSA.3b*), which can be overridden by an initial value and managed by users in certain roles (*FMT_MSA.1a* and *FMT_MSA.1b*). The TOE can implements managing the group of roles that can interact with the security attributes and the initial values of security attributes for the access control SFP (*FMT_SMF.1*).
Auditing	**FAU_TWG.1** **FAU_SAR.1** **FPT_STM.1** **FAU_STG.1**	The auditing function provides the ability to generate auditable events for the Tripwire for Servers product. The *FAU_TWG.1* defines the level of auditable events, and specifies the list of data that shall be recorded in each record generated by TSF and *FAU_SAR.1* provides the authorized users the capability to obtain and interpret the information. Audit data will be saved in suitable form for the administrator to interpret the information and will be protected from unauthorized deletion (*FAU_STG.1*). Tripwire for Servers underlying operating system provides the capabilities to time stamp all auditable events (*FPT_STM.1*).
Authentication	**FIA_UID.1** **FIA_UAU.1** **FIA_ATD.1a**	To gain access to the TOE data and functionality the authorized users must successfully authenticate and identify themselves via OS (*FIA_UID.1, FIA_UAU.1*) and the authentication TFS / TWM (*FIA_ATD.1a*

	FIA_ATD.1b **FMT_SMR.1** **FMT_SMF.1**	and the authentication TFS / TWM (*FIA_ATD.1a*, *FIA_ATD.1b*). *FMT_SMR.1* specifies the roles with respect to security that the TSF recognizes. The TOE allows authorized administrators to be able to define additional security attributes for users and to manage the user identities (*FMT_SMF.1*).
Communications	**FTP_TWI.1**	Inter-TSF trusted channel requires that the TSF provide a trusted communication channel between itself and another trusted IT product (*FTP_TWI.1*).
Integrity Checking	**FAU_PRG.1** **FAU_PRR.1** **FDP_SDI.2** **FMT_SMF.1**	The integrity checking function provides the Tripwire for Servers product with the capability of monitoring stored data within the system's file system for any changes. TFS will generate reports for violations discovered from the integrity check of a Tripwire for Servers machine (*FAU_PRG.1*). Objects to be monitored are determined by the objects defined within the integrity policy file. When violations are identified (*FAU_PRR.1*), additional actions may be taken (*FMT_SMF.1*). *FDP_SDI.2* provides requirements that address protection of user data while it is stored within the TSC.

8.4.2 Assurance Measures Meet Assurance Requirements

The following table represents the assurance requirements for an assurance level of EAL 1, along with a mapping of the assurance measures (Tripwire documentation) that are required to demonstrate the products conformance to an EAL 1 assurance level.

Table 7: Assurance Measures that Fulfill Assurance Requirements (EAL1)

Assurance Requirements	Tripwire Documentation	Rationale
ACM_CAP.1.1D	— Tripwire Manager version 3.0 — Tripwire for Servers version 3.0 — Tripwire for Servers Check Point Edition version 3.0	Tripwire will provide Tripwire products listed here.

Assurance Requirements	Tripwire Documentation	Rationale
ADO_IGS.1.1D	— Tripwire Manager Quick Start version 3.0, (TW1052-00) — Tripwire for Servers Installation Guide version 3.0, (TW1002-03) — Tripwire for Servers, Check Point Edition Configuration Guide version 3.0, (TW1053-02) — Tripwire Manager User Guide version 3.0, (TW1004-02) — Tripwire for Servers User Guide 3.0, (TW1005-02) — Tripwire Manager & Tripwire for Servers Reference Guide version 3.0, (TW1003-03) — "Secure Installation, Generation and Startup Procedure for Tripwire Manager Version 3.0 with Tripwire for Servers Version 3.0; Tripwire Manager version 3.0 with Tripwire for Servers Check Point Edition Version 3.0" Version 2.1	The steps necessary for secure installation, generation, and start-up of the TOE are described within the documents listed here.
ADV_FSP.1.1D ADV_RCR.1.1D	— "Functional Specification and Correspondence Analysis for Tripwire Manager Version 3.0 with Tripwire for Servers Version 3.0; Tripwire Manager Version 3.0 with Tripwire for Servers Check Point Edition Version 3.0" Version 2.2.	The functional specification describes the TSF and the external interface to the TOE. The representation correspondence is a demonstration of mappings between all adjacent pairs of available TSF representations, from the TOE summary specification through to the least abstract TSF representation that is provided. Document listed here satisfies these requirements.

Assurance Requirements	Tripwire Documentation	Rationale
AGD_ADM.1.1D	— Tripwire Manager User Guide version 3.0, (TW1004-02) — Tripwire for Servers User Guide 3.0, (TW1005-02) — Tripwire Manager & Tripwire for Servers Reference Guide version 3.0, (TW1003-03) — "Secure Installation, Generation and Startup Procedure for Tripwire Manager Version 3.0 with Tripwire for Servers Version 3.0; Tripwire Manager version 3.0 with Tripwire for Servers Check Point Edition Version 3.0" Version 2.1	Administrative guidance provides the TOE administrators with detailed, accurate information of how to administer the TOE in a secure manner. Documents listed here satisfy these requirements.
AGD_USR.1.1D	— Tripwire Manager User Guide version 3.0, (TW1004-02) — Tripwire for Servers User Guide version 3.0, (TW1005-02) — Tripwire Manager & Tripwire for Servers Reference Guide version 3.0, (TW1003-03) — "Secure Installation, Generation and Startup Procedure for Tripwire Manager Version 3.0 with Tripwire for Servers Version 3.0; Tripwire Manager version 3.0 with Tripwire for Servers Check Point Edition Version 3.0" Version 2.1	User guidance provides the TOE users with the necessary background and specific information on how to correctly use the TOE's protection functions. Documents listed here satisfy these requirements.
ATE_IND.1.1D	— Tripwire Manager, Tripwire for Servers, & Tripwire for Servers Check Point Edition Version 3.0 products	Tripwire will provide the Tripwire products for testing.

8.4.3 Validation of Strength-of-Function

No strength of function claims are specified for this security target

8.5 PP Claims Rationale

There are no protection profile claims for this security target.

9 References

9.1 Acronyms

This section provides a list of acronyms used within the ST

CC	Common Criteria version 2.1 (ISO/IEC 15408)
EAL	Evaluation Assurance Level
OS	Operating System
SFP	Security Function Policy
SFR	Security Functional Requirements
SOF	Strength of Function
ST	Security Target
TFS	Tripwire for Servers
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function(s)
TSP	TOE security Policy
TFS CPE	Tripwire for Servers, Check Point Edition
TWM	Tripwire Manager

9.2 National and International interpretations

This section provides a list of National and International Interpretation used within the ST:

NIAP-0405	American English Is An Acceptable Refinement
NIAP-0407	Empty Selections Or Assignments
NIAP-0416	Association Of Access Control Attributes With Subjects And Objects
NIAP-0422	Clarification Of "Audit Records"
NIAP-0423	Some Modifications To The Audit Trail Are Authorized
NIAP-0429	Selecting One Or More
INTERP-051	Use of documentation without C & P elements
INTERP-065	No component to call out security function management