Tripwire IP360 Version 9.0.1
Security Target

Release Date: August 10, 2018

Version: 0.10

Prepared By: Saffire Systems
P.O. Box 40295
Indianapolis, IN 46240

Prepared For: Tripwire, Inc.
101 SW Main Street
Suite 1500
Portland, OR 97204

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target, Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

This section will provide information necessary to identify and control the Security Target and the TOE.

ST Title	Tripwire IP360 Version 9.0.1 Security Target
Version:	0.10
Publication Date:	August 10, 2018
ST Author	Michelle Ruppel, Saffire Systems
Assurance Level:	EAL 2 + ALC_FLR.2

1.2 TOE Reference

The TOE claiming conformance to this ST is identified as:

> Tripwire IP360, Version 9.0.1 using Axon Agent version 3.7.0 (VnE build 9.0.1-20180731163509; DP build 9.0.1-20180731141911)

The Tripwire IP360 TOE provided in two configurations: physical hardware appliances or supported virtual platforms, including cloud platforms. In both cases, the Tripwire IP360 Version 9.0.1 software is installed on the platform. The TOE includes the following physical hardware appliances:

Device Profiler appliances	**VnE Manager appliances**
DP 6000P	VnE 1700, 4700, 5700
DP Ev	VnE Ev

The following virtual cloud platforms are in the operating environment for the Tripwire IP360 evaluation:

Amazon EC2

Microsoft Azure

The following virtual platforms are in the operating environment for the Tripwire IP360 evaluation:

Microsoft Hyper-V 2012 R2

VirtualBox 5.X

VMware ESXi 6.0, 6.5

VMware Fusion 10

VMware Workstation 14

The Tripwire IP360 Version 9.0.1 software includes a Device Profiler, VnE Manager, and Agent software.

1.3 Document Terminology

Please refer to CC Part 1 Section 2.3 for definitions of commonly used CC terms.

1.3.1 Acronyms

AC	Access Control
ACL	Access Control List
ANSI	American National Standards Institute
CC	Common Criteria
CLI	Command Line Interface
DP	Device Profiler
EAL2	Evaluation Assurance Level 2
FIPS	Federal Information Processing Standard (NIST)
GUI	Graphical User Interface
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
NIST	National Institute of Standards and Technology
OSP	Organisational Security Policy
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UI	User Interface
VnE	Vulnerability and Exposure

1.4 TOE Overview

The TOE is Tripwire IP360, Version 9.0.1 using Axon Agent version 3.7.0 (IP360 v9.0.1), provided by Tripwire, Inc. Tripwire IP360 (also known as IP360) supports being executed on a hardened appliance and on the virtual platforms listed in Section 1.2.

The TOE type is a vulnerability and risk management solution. IP360 is a scalable vulnerability management system that safely identifies network vulnerabilities, enabling enterprises to proactively protect digital assets from attack. IP360 provides discovery and profiling of network assets, as well as vulnerability scoring and prioritization to identify high risks. It provides a measurable and structured approach to detecting, identifying, understanding, and responding to network vulnerabilities.

Tripwire IP360's vulnerability risk score helps customers instantly identify hosts that have unacceptable levels of risk and the vulnerabilities that are creating that risk. The Tripwire IP360 vulnerability risk score combines the human judgment of Tripwire's Vulnerability and Exposure Research Team with an algorithm that weighs the risk characteristics of each vulnerability (Risk Class, Available Exploits, and Vulnerability Age) to compute a numerical score that can range from zero to more than 50,000. These scores are combined for each host to produce its Host Score, which lets you know at a glance if a host has any significant vulnerabilities.

Tripwire IP360 can be administered remotely or locally. IP360 provides multiple administrative interfaces, including a command line interface (CLI), web interface, and two application programming interfaces (APIs).

The TOE implements the following security functions:

- Security Audit
  The TOE generates audit records for security related audit events and provides a mechanism to allow authorized administrators to export the records for review. Audit records are protected from unauthorized deletion and modification and mechanisms are in place to prevent audit data loss.
- Cryptographic Support
  Cryptographic capabilities within the TOE are provided by an OpenSSL FIPS-certified cryptographic module. OpenSSL is used to implement the cryptography used by TLS to protect communications between distributed parts of the TOE
- Identification and Authentication
  The TOE provides two mechanisms for the identification and authentication of administrative users: an internal password-based mechanism and external Active Directory (an LDAP-compliant Microsoft directory) mechanism. Use of Active Directory is not included in the evaluated configuration. The IP360 is capable of enforcing password complexity requirements.
- Security Function Management
  The VnE Manager provides remote management via a web-based interface, an XML-RPC API, and a REST API. Both the VnE and DP provide a command line interface (CLI) through the serial port and via SSH. The TOE provides management functions for configuring scanning and vulnerability analysis, managing audit functions, and managing user accounts.
- Protection of the TSF
  IP360 implements many features for protection of the integrity and management of its own security functionality. These features include the protection of sensitive data and reliable time stamps.

- Trusted Path / Channels

  IP360 protects remote connections to the management interfaces with HTTPS, TLS and SSH. Connections between distributed parts of the TOE are protected with TLS.

- Vulnerability Management
  The TOE scans the network for devices and then profiles of the discovered devices. The profiling involves performing a measurable and structured approach to identifying network vulnerabilities based on currently known vulnerabilities.

1.4.1 Required non-TOE hardware/software/firmware

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

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

- SMTP Server – An email server is used to facilitate delivery of vulnerability check results to administrators when the TOE is so configured.
- SNMP recipient -- A network management device is used to facilitate delivery of vulnerability 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 and a PDF 1.4 compatible reader. The TOE supports communications with web browsers that support HTTP over TLS.1.2.

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.

1.4.1.1 IP360 Agent Requirements

IP360 Agents can be installed on systems being monitored by IP 360. The IP360 Agents can be installed on the following operating systems which are in the operating environment:

- RedHat Enterprise Linux version 7.3, 7.4 64-bit
- Ubuntu 14.0.4 64-bit
- Windows Server 2008, 2008 R2, 2012, 2012 R2 64-bit

All current patches and security fixes must be installed upon these operating systems before installing the Tripwire IP360 Agents.

1.5 TOE Description

Tripwire IP360 delivers asset discovery capabilities and risk-based vulnerability assessment. IP360 performs comprehensive discovery and profiling of all network assets and vulnerability scoring to identify top risks. The TOE collects data from the discovered hosts and runs vulnerability checks against the data to identify vulnerabilities. Each vulnerability check is written by Tripwire to specifically identify a known vulnerability, and therefore each vulnerability check is unique to the vulnerability being analyzed. Administrators generate reports to obtain the results of the vulnerability checks.

The TOE provides protected communications between the distributed TOE components and between the

TOE and the administrative user.

1.5.1 TOE Architecture

Tripwire IP360 is delivered on application-specific appliances insuring rapid deployment and minimal upkeep, support and maintenance. Scanning devices (physical or virtual) do not store any scan results locally. A TCP port is open on the scanning devices when configured to use agents, and the SSH port open may also be open. Tripwire IP360 appliances can be distributed throughout the network with no concern for data stored in “less secure” remote locations since client data is not stored locally. All data is stored within the Tripwire IP360 VnE Manager. The scanning appliances are centrally administered for complete automation of application and vulnerability signature updates.

The Tripwire, Inc. IP360 Vulnerability Management System consists of two key components, the VnE Manager and the Device Profiler:

- Vulnerability and Exposure (VnE) Manager — also known as VnE in this ST. The VnE is the centralized management server for administering the recurring and on-demand scanning processes within the enterprise. It serves as the management and central data repository for all vulnerability data. The VnE Manager is available both as physical appliance or virtual edition. The VnE Manager operates as a hardened Linux-based system with a secure web browser interface. The VnE Manager also offers a XML-RPC API that permits programmatic management of the elements of the scanning process and integration with other components of the security solution. It also provides a REST API that offers similar functionality as well the following new features: Default UI, DP pooling, agent-based vulnerability management. The VnE implements role-based access control, which makes it convenient to delegate scan management administration.
- Device Profiler (DP) — also known as Scan Appliance. The DP is the distributed scanning appliance of Tripwire IP360. Device Profilers are available both as physical appliances or virtual edition. Additionally, a single built-in Device Profile (also known as Onebox DP) is provided on the VnE Manager. The Device Profiler has four NICs that can all be used for scanning. In addition to conventional IP addresses, the Device Profiler supports 802.1q VLAN tagging for scanning of multiple VLANs from a trunked switch port. All Device Profilers are centrally managed by the VnE Manager for software and vulnerability signature updates. The Device Profiler appliance executes a hardened Linux-based system that features solid state drives. The DP requires an open TCP port for Agents. No asset or vulnerability data is ever at rest in the Device Profiler. Additionally, load balancing is utilized to distribute scanning jobs across multiple DPs. DP load balancing allows for the definition and configuration of "pools" that contain one or more DPs. If there is more than one Device Profiler in a pool, those profilers work together in order to scan a network target. As DPs become available, IP sections are sent to the available DPs for scanning, thereby optimizing the use of your scanning resources. Performance, scalability, and resilience are improved by distributing scanning workloads across multiple DPs.

In addition to these key components, there is an IP360 Agent portion of the TOE can be installed and executed on RedHat, Ubuntu, and Windows operating systems identified in Section 1.4.1.1. The Agent removes the need to have remote credentials to access the host. The Agent collects information about the host and sends it to the DP.

A host (also known as a scan target) is represented in the TOE by its network IP address.

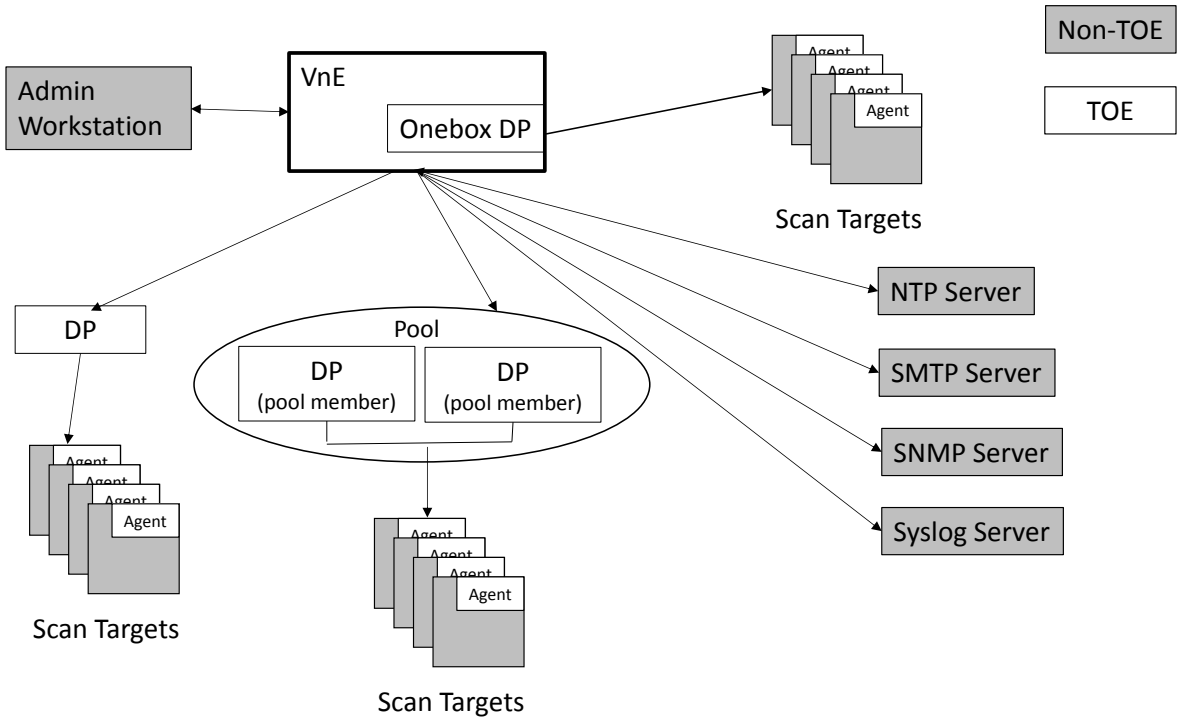

Figure 1: TOE boundary

The TOE uses various network protocols to communicate with other parts of the TOE and with the operational environment. Depending upon the communication pathway the TOE acts either as a server or as a client on each pathway. The following summarize the network communication pathways that exist.

- VnE – DP communication.

  The DP initiates communication with the VnE. Once communication is established, the secure channel is bi-directional. The VnE sends configuration changes and management requests to the DP, including vulnerability signature updates. Both the VnE and DP components of the TOE use TLS to communicate with each other.

- DP – Scan Targets

  The DP initiates connections to hosts to obtain information made available by protocols supported by the node (e.g., FTP, Telnet, SSH). For protocols requiring user authentication, the DP provides login data for the specific node being accessed, then gathers information from the node as determined by rules established for that type of vulnerability check.

- DP – Agent communication.

  The Agent initiates communication with the DP. Once communication is established, the secure channel is bi-directional. Communications are used to download new vulnerability signatures or to satisfy a request to search for vulnerabilities. The Agents communicate over

an authenticated TLS connection established with a DP.

- VnE –GUI, CLI, XML-RPC API, REST API

  The GUI is a web server running on the VnE for use by an external web browser. The web server supports HTTPS (HTTP over TLS) connections from a web browser to the TOE's GUI. The web browser is not part of the TOE. The connection between the web browser and the GUI uses HTTPS to protect the integrity of the connection. User identification and authentication is handled through the GUI.

  The SSH daemon on the VnE can be enabled to remotely access the CLI. The VnE also provides access to the CLI through the serial port or on the console.

  TLS is used to protect XML-RPC API and REST API transmissions.

- DP – CLI

  Administrators remotely access the DP CLI using SSH. The DP also provides access to the CLI through the serial port.

- VnE – NTP/SMTP/SNMP/Syslog server

  The VnE is a client to NTP/SMTP/SNMP/Syslog servers. In addition to the time source, notification mechanisms such as email, SNMP, and syslog server are outside of the TOE boundary. The TOE implements only client-side protocols for these communications. The VnE uses these notification servers as configurable delivery mechanisms for TOE generated messages. The TOE utilizes external (non-TOE) mechanisms for delivery of notifications, thus the TOE cannot guarantee delivery of notifications. (Note: Use of an NTP server is optional.)

1.5.2 Physical Boundaries

The evaluated configuration includes components running in the TOE boundary and components running outside the TOE boundary. Inside the TOE boundary are Tripwire IP360 Vulnerability and Exposure (VnE) Manager, Device Profiler, and Tripwire IP360 Agents running on administrative workstations.

The Tripwire IP360 VnE Manager and Device Profiler component can operate on several supported platforms. Refer to Section 1.5.2.1 for a list of supported platforms.

The operational environment also includes a web browser and a network connecting all of the other components into a single LAN.

When deployed using a virtual platform, the TOE relies upon the virtual platform for virtual machine separation, process-related (e.g., time) and network-related (e.g., name resolution) services.

The TOE assumes the following network IT entities described in Section 1.4.1 are in the operating environment.

- SMTP Server
- SNMP recipient
- Syslog Server
- Workstation to be used by an administrator

- Network hosts to scan

1.5.2.1 Hardware Components

The TOE can be deployed as an appliance or on a virtual platform. When deployed as an appliance, the TOE includes both the hardware and software. When deployed in a virtual environment, all hardware used to deploy the TOE is in the operational environment.

When not operating on virtual platforms, the Tripwire IP360 VnE Manager operates on a hardened appliance that serves as the central data repository and management platform. The Device Profiler is a hardened, diskless appliance that profiles devices and securely reports its findings to the centralized Tripwire IP360 VnE Manager. When operating on a virtual platform, both the Tripwire IP360 VnE Manager and the Device Profiler execute on the same hardened operating system as the physical hardware appliance.

When the TOE is deployed using a hardware appliance, the following table details the acceptable appliance compatibility configuration:

	VnE 1700, 4700, 5700	**VnE Ev**
DP 6000P	OK	OK
DP Ev	OK	OK

Table 1: Hardware Platforms

When the TOE is deployed in a virtual environment, the hardware must be compliant with the hardware supported by the virtual platforms listed in Section 1.2

1.5.2.2 Software Components

This table identifies software components.

TOE or Environment	**Component**	**Description**
TOE	Tripwire Vulnerability and Exposure (VnE) Manager, Version 9.0.1	Centralized management server for administering the recurring and on-demand scanning processes
TOE	Device Profiler, Version 9.01	The Scan Appliance that is the distributed scanning appliance.
TOE	Tripwire IP360 Axon Agent Version 3.7.0	The Agent that is installed on the host to collect data from the host and send it to the DP.
Environment	Virtual Platform (Refer to Section 1.2 for additional details)	The virtual platform on which the TE VnE Manager and Device Profiler are installed when deployed in a virtual environment.

Table 2: Software Components

1.5.2.3 Guidance Documentation

Tripwire provides administrator and user guidance on how to utilize the TOE security functions and

warnings to administrators and users about actions that can compromise the security of the TOE.

The Tripwire IP360 9.0.1 Supplemental Common Criteria Guidance contains details regarding the common criteria specific instructions and warning provided to administrators.

These activities are documented in:

- Tripwire IP360 9.0.1 Default UI Administrator's Guide
- Tripwire IP360 9.0.1 Legacy UI Administrator's Guide
- Tripwire IP360 9.0.1 API Guide
- Tripwire VnE Manager 1700, 4700, 5700 & Ev Quickstart Guide
- Tripwire IP360 Device Profiler 5000 5050, 6000P & Ev User Guide
- Tripwire Device Profiler Command Line Interface Guide
- Tripwire VnE CLI Guide
- Tripwire IP360 9.0 Agent Based Vulnerability Management Installation and Configuration Guide
- Tripwire IP360 9.0.1 Agent Based Vulnerability Management Getting Started Guide
- Tripwire IP360 9.0.1 Release Notes
- Tripwire IP360 v9.0.1 Supplemental Common Criteria Guidance

1.5.3 Logical Boundaries

This section identifies the security functions that the TSF provides**.**

- Vulnerability Detection System (VDS)
- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

1.5.3.1 Vulnerability Detection System

Tripwire IP360 begins each scan with a discovery phase for IP addresses within the scope of the defined network configuration. This discovery process is user-configurable, but typically consists of ICMP echo requests (pings) to each IP address first, and then scanning for a short list of open TCP ports on each IP address if a ping response is not received. Once an active host is detected, Tripwire IP360 begins a systematic process of profiling the host. These steps may include TCP and UDP port scan, external application identification, external vulnerability, etc.

Tripwire IP360 vulnerability scanning combines both remote assessment and local authenticated checks when credentials are available. The scans begin with inventorying the applications installed on the host. This list of applications determines which vulnerability checks are performed. The application inventory

is also populated into the system database and can be used as criteria for reporting.

Tripwire IP360 provides granular scheduling capabilities. Scheduling options include immediate "On Demand" scan, one-time "On Demand" scan scheduled for a specified date and time, recurring scans.

Credentials can be provided for Windows (either WMI or SMB access will work transparently), SSH with a password or a private key, SNMPv1andv2, Web authentication to a form, and Web authentication via HTTP.

The Tripwire IP360 vulnerability risk score combines the human judgment of Tripwire's Vulnerability and Exposure Research Team with an algorithm that weighs the risk characteristics of each vulnerability(Risk Class, Available Exploits, Vulnerability Age) to compute a numerical score that can range from zero to more than50,000. These scores are combined for each host to produce its Host Score, which lets you know at a glance if a host has any significant vulnerabilities. Automatic consolidation of data from all scans provides the ability to view network trends over time. Report filters let you refine the report contents to the precise set of hosts and vulnerabilities that you need to analyze.

Tripwire IP360 can generate alerts for new hosts, hosts with an excessive Host Score, and any specified list of high risk vulnerabilities.

1.5.3.2 Security Audit

Audit data of the TOE is stored in a database in the VnE and in flat files on the hard drive. The TOE controls access to the audited data. The TOE records GUI activities, SSH login attempts, web GUI login attempts, user group modifications, and manual changes to the system time.

The audit data can be viewed, sorted and filtered using the VnE GUI.

Administrators can export data from the system log and IP360 log in order to view it on another machine in the TOE environment.

1.5.3.3 Identification and Authentication

Users must be identified and authenticated prior to interacting with the TOE. All security-relevant mediated functions require the user to be authenticated. The TOE creates and maintains the user account information in the IP360 database. The TOE itself identifies and authenticates the username and password supplied. Always used for identifying and authenticating the default "administrator" account.

The TOE maintains the following security attributes for each Internal User: user identity, authentication data, user type, user groups, role information, and user access rights.

The TOE enforces the following password complexity requirements when creating users and changing a password.

- Password length of 8-12.
- Minimum number of numeric characters 1.
- Minimum number of alphabetic characters 1.
- Minimum number of non-alphanumeric ASCII characters 1.
- Minimum number of hours required before changing a password again: 48.

Guidance provides recommendations to the users for creating strong passwords. In addition, the TOE is

able to lockout user accounts after three consecutive unsuccessful authentication attempts.

1.5.3.4 Security Management

The TOE restricts the ability to execute commands by restricting access to the user interfaces and the functions they provide based on the access rights assigned to that user account. Roles allow for access rights to be configured based on the management role as needed. A user role is defined the access rights granted to any number of independent functional areas or objects within the TOE. The access rights associated with a role to a date/function can be Read Only, Read-Scan, Read-Write, Create. Access rights are paired with tasks to control access to management functions.

The VnE Manager provides remote management via a GUI (web-based interface) and an API. It also provides a command line interface (CLI) through the serial connection. Administrators can connect to the VnE CLI either with a keyboard and monitor or with a serial connection to the VnE's serial port using a terminal emulator. It is also possible to enable the SSH daemon on the VnE Manager to remotely access the CLI.

The VnE administrative interfaces provide the ability to:

- Configure network settings
- Configure user access and user account settings
- Configure Scan Attributes
- Configure DP Settings
- Configure Scanning Activities
- Generate Reports
- Manage Certificates and Cryptography

The Device Profiler provides a command line interface (CLI) accessible using SSH or the serial port. The TOE provides management functions for configuring scanning and vulnerability analysis, managing audit functions, and managing user accounts.

The DP administrative interfaces provide the ability to:

- Configure network settings
- Configure user access settings
- Manage Certificates and Cryptography

The API included with Tripwire IP360 enables users to programmatically command and control the functionality of Tripwire IP360 through the use of scripts. By using scripts, you can remotely control Tripwire IP360 and integrate it with third-party products. Tripwire supports the XML-RPC and JSON-RPC protocols, although use of JSON-RPC is not included in the evaluation.

1.5.3.5 Protection of the TSF

The TOE ensures the availablily of audit data and System data by protecting it from modification and deletion.

Network hosts 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 SSH or telnet). For hosts 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 hosts for TOE's self-protection.

The VnE, DP, and Agents include the OpenSSL FIPS Object Module SE v2.0.16 library (which is a FIPS certified cryptographic module[1]) that is used to implement TLS to protect communications between the TOE's distributed components, and between the TOE and the remote IT entities. This cryptographic module is also used to protect communications with the administrative workstation using TLS and SSH.

The VnE 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.

1.5.4 Items Excluded from the TOE

This section identifies any items that are specifically excluded from the TOE.

Tripwire IP360 integration with the Tripwire Security Intelligence Hub (SIH), Tripwire Log Center (TLC), Tripwire Enterprise (TE) is excluded from the evaluated configuration. Integration with these components is not tested or evaluated. SIH is an advanced reporting and analytics portal for IP360. TLC is a log and event management center. TE is a security configuration management suite.

Use of PureCloud in the evaluated configuration is also excluded. PureCloud is a cloud hosted implementation of Tripwire IP360 that allows the scanning of your network perimeter without any local hardware.

Use of json-rpc API will be disabled in the evaluated configuration.

Use of SAML and Active Directory / LDAP is not included in the evaluated configuration.

[1] The OpenSSL FIPS Object Module SE v2.0.16 library is associated with FIPS certificate number 2398.

2 Conformance Claims

2.1 CC Conformance Claims

This ST was developed to Common Criteria (CC) for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

The ST claims to be:

CC Version 3.1 Revision 5 Part 2 extended

CC Version 3.1 Revision 5 Part 3 conformant

2.2 PP and Package Claims

The ST claims to be Evaluation Assurance Level 2 augmented with ALC_FLR.2.

The ST does not claim conformance to any Protection Profiles.

2.3 Conformance Rationale

Not applicable.

3 Security Problem Definition

The TOE is intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the sensitivity level of information in both the internal and external networks is equivalent.

This section contains assumptions regarding the security environment and the intended usage of the TOE and threats on the TOE and the TOE environment.

3.1 Threats

The threats identified in this section may be addressed by the TOE, the host system the TOE monitors or a combination of both. The threat agents are authorized persons/processes, unauthorized persons/processes, or external IT entities not authorized to use the TOE itself. The threats identified assume that the threat agent is a person with a low attack potential who possesses an average expertise, few resources, and low to moderate motivation.

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

3.1.1 TOE Threats

T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

3.1.2 Host System Threats

The following identifies threats to the host system that may be indicative of vulnerabilities.

T.SCNMLC	Users could execute malicious code on a host system that the TOE monitors which causes modification of the host system protected data or undermines the host system security functions.
T.SCNVUL	Unauthorized users may be able to exploit vulnerabilities in hosts on the network that the TOE monitors.
T.FALASC	The TOE may fail to recognize or identify vulnerabilities or inappropriate activity based on association of data received from each host.

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

3.3 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

3.3.1 Intended Usage Assumptions

A.ACCESS	The TOE has access to all of the host system data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable[2] to the network of host systems the TOE monitors.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the host systems the TOE monitors.

3.3.2 Physical Assumptions

A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

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

Application Note: This assumption is also intended to apply to the required items of the IT environment, such as the private physical network.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.RTIME When configured to use a remote time source, the IT environment shall include a trusted source for the system time.

3.3.3 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

4 Security Objectives

This chapter describes the security objectives for the TOE and the TOE's environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Operating Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.VDSCAN	The TOE must scan the network to discover hosts (IP addresses) to analyze for potential vulnerabilities.
O.VDPROF	The TOE must systematically profile the host to detect vulnerabilities that match the set of vulnerabilities that the TOE is configured to detect.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.AUDITS	The TOE must record audit records for use of management functions.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.
O.TIME	The TOE must provide reliable timestamps.

4.2 Security Objectives For The Environment

The security objectives for the environment are listed below.

The following security objectives for the environment are satisfied through application of procedural or administrative measures.

OE.INSTAL	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.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.

The following security objectives for the environment are satisfied through technical measures.

OE.INTROP The TOE is interoperable with the host systems on the network it monitors.

OE.TIME When configured to use a remote time source to provide reliable timestamps, the IT environment shall provide an accurate timestamp.

4.3 Security Objectives Rationale

4.3.1 Tracings between Security Objectives and the Security Problem Definition

Table 3 demonstrates that the tracing between the assumptions, threats, and policies to the security objectives is complete.

	O.PROTCT	O.VDSCAN	O.VDPROF	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.TIME	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME
T.COMINT	X				X	X			X							
T.COMDIS	X				X	X										
T.LOSSOF	X				X	X			X							
T.NOHALT					X	X						X				
T.PRIVIL	X				X	X										
T.IMPCON				X	X	X					X					
T.INFLIX							X									
T.FACCNT								X								
T.SCNMLC		X	X													
T.SCNVUL		X	X													
T.FALASC			X													
P.MANAGE	X			X	X	X					X		X	X		
P.ACCESS	X				X	X								X		
P.ACCACT						X		X		X			X	X		X
P.INTGTY									X							
P.PROTCT							X					X				
A.ACCESS															X	
A.ASCOPE															X	
A.DYNMIC														X	X	

	O.PROTCT	O.VDSCAN	O.VDPROF	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.TIME	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME
A.PROTCT												X				
A.LOCATE												X				
A.RTIME																X
A.MANAGE														X		
A.NOEVIL											X		X			
A.NOTRUST												X	X			

Table 3: Tracings between Threats/OSPs/Assumptions and Security Objectives

4.3.2 Rationale For Assumption Coverage

This section provides a justification that for each assumption, the security objectives for the TOE environment cover that assumption.

A.ACCESS The TOE has access to all of the host System data it needs to perform its functions.

The OE.INTROP objective ensures the TOE has the needed access.

A.ASCOPE The TOE is appropriately scalable to the network of host systems the TOE monitors.

The OE.INTROP objective ensures the TOE has the necessary interactions with the host systems it monitors.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the host systems the TOE monitors.

The OE.INTROP objective ensures the TOE has the access required to interoperate with the host system it is monitoring. The OE.PERSON objective ensures that the TOE will managed appropriately.

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

The OE.PHYCAL provides for the physical protection of the TOE hardware and software.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

The OE.PHYCAL provides for the physical protection of the TOE.

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OE.INSTAL objective ensures that the TOE is properly installed, operated, and managed. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRST	The TOE can only be accessed by authorized users. The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

4.3.3 Rationale For Threat Coverage

This section provides a justification that for each threat, the security objectives counter the threat.

T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no system and Audit data, which includes data collected and produced by the TOE, will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no system and Audit data, which includes data collected and produced by the TOE, will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions, including halting execution of the TOE. The OE.PHYCAL objective ensures that the critical TOE components are protected from physical attack.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle. The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected. The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.SCNMLC	Users could execute malicious code on a host system that the TOE monitors which causes modification of the host system protected data or undermines the host system security functions. The O.VDSCAN objective counters this threat by requiring that the TOE scan the network for hosts to analyze. The O.VDPROF objective counters this threat by providing the capability for the TOE to detect vulnerabilities, including malicious code.
T.SCNVUL	Unauthorized users may be able to exploit vulnerabilities in hosts on the network that the TOE monitors.

The O.VDSCAN objective counters this threat by requiring that the TOE scan the network for hosts to analyze. The O.VDPROF objective counters this threat by providing the capability for the TOE to detect vulnerabilities.

T.FALASC The TOE may fail to recognize or identify vulnerabilities or inappropriate activity based on association of data received from each host.

The O.VDPROF objective provides the function that the TOE will detect vulnerabilities.

4.3.4 Rationale For Organizational Security Policy Coverage

This section provides a justification that for each organizational security policy, the security objectives address the OSP.

P.MANAGE The TOE shall only be managed by authorized users.

The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.PERSON objective requires authorized users are carefully selected and trained for proper TOE operation. The combination of O.IDAUTH, O.ACCESS, and OE.PERSON ensure that the data collected and produced by the TOE is only used for authorized purposes by authorized users. The O.PROTCT objective addresses this policy by providing TOE self-protection.

P.ACCACT Users of the TOE shall be accountable for their actions within the TOE.

The O.AUDITS objective implements this policy by requiring auditing of all TOE management functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The O.TIME objective ensures that the TOE provide reliable time stamps for association with an audit record. The OE.CREDEN objective requires administrators to protect all authentication data ensuring no-one can masquerade as them. The OE.PERSON objective ensures that the TOE will be managed appropriately to ensure that they

	following all guidance and forensic records are maintained according to policy. The OE.TIME objective ensures that a reliable timestamp is available for use in audit records.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGR objective ensures the protection of system and Audit data, which includes data collected and produced by the TOE from modification.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The O.OFLOWS objective counters this policy by requiring the TOE handle storage overflows. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

5 Extended Components Definition

This section defines the newly defined components (also known as extended components) used to define the security requirements for this ST. The extended components defined in this section are based on the existing CC Part 2 SFRs.

5.1 Class VDS: Vulnerability Detection System

A VDS class was created to specifically address vulnerability detection capabilities. The Security Audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this functional class is to address the unique nature of vulnerability detection systems.

The requirements defined in this class have no dependencies since the stated requirements embody all the necessary security functions.

5.1.1 System Data Collection (VDS_SDC)

This family defines requirements for collecting system data information from targeted host system resources. This family has one component: VDS_SDC.1

Management: VDS_SDC.1

The following actions could be considered for the management functions in FMT:

- Modifying the behavior of system data collection.

Audit: VDS_SDC.1

There are no auditable events foreseen.

5.1.1.1 VDS_SDC.1 System Data Collection

This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the collection of information on system data from targeted host system resources.

Hierarchical to: No other components.

Dependencies: No dependencies.

VDS_SDC.1.1 The TSF shall be able to collect the following information from the targeted device(s):

a) [**selection: network traffic, registry key values, file versions, file contents, command output, access control lists, service interrogation**]; and

b) **[assignment: *other specifically defined information*].**

VDS_SDC.1.2 At a minimum, the TSF shall collect and record the following information:

a) Date and time of the executed scan; and

b) The additional information used to analyze the application and vulnerability state of a device when the information is relevant to determining the device's vulnerability state and can be presented in a human-readable manner.

5.1.2 Analyser Analysis (VDS_ANL)

This family defines requirements for performing analysis function(s) on all data received from the targeted host system resource(s). This family has one component: VDS_ANL.1

Management: VDS_ANL.1

The following actions could be considered for the management functions in FMT:

- Modifying the behaviour of analyzer analysis function(s).

Audit: VDS_ANL.1

There are no auditable events foreseen.

5.1.2.1 VDS_ANL.1 Analyser analysis

This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the analysis of information on system data collected from targeted host system resources.

Hierarchical to: No other components.

Dependencies: No dependencies.

VDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all data received from the targeted device at the request of the administrator [**assignment: *analytical functions***].

5.1.3 Analyser react (VDS_RCT)

This family defines the response to be taken in case of a detected vulnerability. This family has one component: VDS_RCT.1

Management: VDS_RCT.1

The following actions could be considered for the management functions in FMT:

- Modifying the behaviour of analyzer reaction(s).

Audit: VDS_RCT.1

There are no auditable events foreseen.

5.1.3.1 VDS_RCT.1 Analyser analysis

This extended requirement is necessary since a CC Part 2 SFR does not exist that requires the details of a detected vulnerability to be recorded.

Hierarchical to: No other components.

Dependencies: No dependencies.

VDS_RCT.1.1 When a vulnerability is detected, the TSF shall record the details of a vulnerability scan and, if configured by the security administrator, generate an alert.

5.1.4 Restricted Data Review (VDS_RVR)

This family defines the requirement for tools that should be available to authorised users to assist in generating and reviewing vulnerability detection reports. This family has one component: VDS_RVR.1.

Management: VDS_RVR.1

There are no management functions foreseen.

Audit: VDS_RVR.1

There are no auditable events foreseen.

5.1.4.1 VDS_RVR.1 Restricted Vulnerability Report Review

This extended requirement is necessary since a CC Part 2 SFR does not exist that the TOE be able to generate vulnerability detection reports and prepare them for review by a user.

Hierarchical to: No other components.

Dependencies: No dependencies.

VDS_RVR.1.1 The TSF shall provide [**assignment: authorised users**] with the capability to generate a vulnerability detection report.

Application Note: This requirement applies to authorised users of the System.

VDS_RVR.1.2 The TSF shall provide the report in a manner suitable for the user to interpret the information.

VDS_RVR.1.3 The TSF shall prohibit all users read access to the System data and the corresponding vulnerability detection report, except those users that have been granted explicit read-access.

Application Note: The System needs to define the authorised users that may view the vulnerability detection report.

Family Application Note: Available results from any component evaluation may be applicable to this requirement. Note that the definition of authorised users and System data may vary.

5.1.5 System Data Storage (VDS_STG)

This family defines the requirements for the TSF to be able to create and maintain a location to store system data collected from the host system(s). This family has one component: VDS_STG.1.

VDS_STG.1 Protected System Data Storage, specifies that the system data will be protected from unauthorised deletion and/or modification.

Management: VDS_ STG.1

The following actions could be considered for the management functions in FMT:

- Maintenance of the parameters that control the system data storage capability.

Audit: VDS_ STG.1

There are no auditable events foreseen.

5.1.5.1 VDS_STG.1 Protected System Data Storage

This extended requirement is necessary since a CC Part 2 SFR does not exist that the TOE store and protect System data collected from host system(s).

Hierarchical to: No other components.

Dependencies: No dependencies.

VDS_STG.1.1 The TSF shall protect the stored System data from unauthorised deletion.

VDS_STG.1.2 The TSF shall protect the stored System data from modification.

Application Note: Authorised deletion of data is not considered a modification of System data in this context. This requirement applies to the actual content of the System data, which should be protected from any modifications.

6 Security Requirements

The security requirements that are levied on the TOE are specified in this section of the ST.

TOE Security Functional Requirements (from CC Part 2)	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_STG.1	Protected audit trail storage
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1a-e	Cryptographic operation
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication with a third party
FIA_UID.1	Timing of identification with a third party
FMT_MOF.1a, b	Management of security functions behavior
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection
FPT_STM.1	Reliable time stamps
FTA_SSL.4	User-initiated termination
FTP_TRP.1	Trusted Path
Extended Security Functional Requirements	
VDS_SDC.1	System data collection
VDS_ANL.1	Analyzer analysis
VDS_RCT.1	Analyzer react
VDS_RVR.1	Restricted data review
VDS_STG.1	Protected system data storage

Table 4: Security Functional Requirements

6.1 Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify the operations completed in this ST by the ST author..

Assignment made in ST: **indicated with bold text**

Selection made in ST: indicated with underlined text

Refinement made in ST: ***additions indicated with bold text and italics***

deletions indicated with strike-through ~~bold text and italics~~

Iteration made in ST: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MOF.1a)

6.2 Security Functional Requirements

6.2.1 Security audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

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

c) All audit events detailed in Table 5.

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_SAR.1	Reading of information from the audit records using the Legacy UI	
FIA_UAU.1	All use of the authentication mechanism	User identity, location
FMT_MOF.1a, b	All modifications in the behavior of the functions of the TSF made using the Default UI or the Legacy UI.	
FMT_MTD.1	All modifications to the values of TSF data made using the Default UI or the Legacy UI.	
FMT_SMF.1	Security relevant management functions performed using the Default UI or the Legacy UI.	
FMT_SMR.1	Modifications to the group of users that are part of a role made using the Default UI or the Legacy UI.	User identity

Table 5: Auditable Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **the additional information specified in the Details**

column of Table 5: Auditable Events.

6.2.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **security administrators** with the capability to read **all audit information in the User Activity Log** 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.

6.2.1.3 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.1.4 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

6.2.2 Cryptographic Support (FCS) [3]

6.2.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate ***asymmetric*** cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA schemes** and specified cryptographic key sizes **2048 bits for RSA** that meet the following: **FIPS PUB 186-4, "Digital Signature Standard (DSS)" Appendix B.3 for RSA**.

6.2.2.2 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **cryptographic key zeroization method** that meet the following: **FIPS 140-2**.

6.2.2.3 FCS_COP.1a Cryptographic operation (hashing)

FCS_COP.1.1a The TSF shall perform **cryptographic hashing operations** in accordance with a specified cryptographic algorithm **SHA-1, SHA-256, SHA-384** and cryptographic key sizes **not applicable[4]** that meet the following: **FIPS Pub 180-4, "Secure Hash Standard"**.

6.2.2.4 FCS_COP.1b Cryptographic operation (encryption/decryption)

FCS_COP.1.1b The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **AES and AES operating in CTR and GCM mode** and cryptographic key sizes **128, 192 (CTR mode only), and 256 bits** that meet the following: **FIPS Pub 197, "Advanced Encryption Standard (AES)"**.

---

[3] The TOE uses OpenSSL FIPS Object Module SE v2.0.16 library (certificate number 2398).

[4] SHA-1 does not use cryptographic keys in its calculation. The message digest size is 160, 256, or 384bits, depending upon the algorithm.

6.2.2.5 FCS_COP.1c Cryptographic operation (encryption/decryption)

FCS_COP.1.1c The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm **Triple DES operating in CDC mode** and cryptographic key sizes **128 and 192 bits** that meet the following: **NIST Special Publication 800-67**.

6.2.2.6 FCS_COP.1d Cryptographic operation (RSA signature services)

FCS_COP.1.1d The TSF shall perform **RSA digital signature generation and verification** in accordance with a specified cryptographic algorithm **RSA Digital Signature Algorithm** and cryptographic key sizes **2048 bits** that meet the following: **FIPS Pub 186-4, "Digital Signature Standard (DSS)"**.

6.2.2.7 FCS_COP.1e Cryptographic operation (message authentication code)

FCS_COP.1.1e The TSF shall perform **message authentication code operations** in accordance with a specified cryptographic algorithm **HMAC-SHA-1** and cryptographic key sizes **32-byte** that meet the following: **FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code" and FIPS Pub 180-4, "Secure Hash Standard"**.

6.2.3 Identification and authentication (FIA)

6.2.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **three** unsuccessful authentication attempts occur related to **REST API logins, and Legacy UI logins**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall **lock out (disable) the user account for 20 minutes**.

6.2.3.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) User identity

b) Password

c) Access Rights

d) User group memberships

e) Role(s).

6.2.3.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **the following passwords complexity requirements unless set by an Administrator using the CLI:**

- **Minimum password length 8 -12 characters**
- **Minimum number of numeric characters 1 or greater**
- **Minimum number of alphabetic characters 1 or greater**
- **Minimum number of non-alphanumeric ASCII characters 1 or greater**
- **Minimum number of hours required before changing a password again: 48.**

6.2.3.4 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **no actions** 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.

6.2.3.5 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **no actions** 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.

6.2.4 Security management (FMT)

6.2.4.1 FMT_MOF.1a Management of security functions behavior

FMT_MOF.1.1a The TSF shall restrict the ability to modify the behavior of the functions **of scan discoveries, host profiling, System data collection, analysis and reaction** to **security administrators.**

6.2.4.2 FMT_MOF.1b Management of security functions behavior

FMT_MOF.1.1b The TSF shall restrict the ability to disable, enable the functions **related vulnerability scanning** to **security administrators.**

6.2.4.3 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to query ***(view)***, modify, delete, **bind, test, duplicate, import, export, assign, and add** the **TSF data identified in Table 11 and Table 12** to **security administrators**.

6.2.4.4 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- **management of network configurations and credentials**
- **management of scan appliances (device profilers)**
- **management of scan discoveries**
- **management of host profiling**
- **generation of reports**
- **management of user accounts (including assigning user access rights and unlocking a user account)**
- **management of roles**
- **management of TOE data**.

6.2.4.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **security administrator**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.5 Protection of the TSF (FPT)

6.2.5.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE.

6.2.5.2 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.6 TOE access (FTA)

6.2.6.1 FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.2.7 Trusted Path/channels (FTP)

6.2.7.1 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification, disclosure.

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication, **and all remote administrative actions**.

6.2.8 Vulnerability Detection System (VDS)

6.2.8.1 VDS_SDC.1 System Data Collection

VDS_SDC.1.1 The TSF shall be able to collect the following information from the targeted device(s):

a) [network traffic, registry key values, file versions, file contents, command output, access control lists, service interrogation]; and

b) **no other specifically defined information.**

VDS_SDC.1.2 At a minimum, the TSF shall collect and record the following information:

a) Date and time of the executed scan; and

b) The additional information used to analyze the application and vulnerability state of a device when the information is relevant to determining the device's vulnerability state and can be presented in a human-readable manner.

6.2.8.2 VDS_ANL.1 Analyser analysis

VDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all data received from the targeted device at the request of the administrator [**direct condition tests, inference**].

6.2.8.3 VDS_RCT.1 Analyser react

VDS_RCT.1.1 When a vulnerability is detected, the TSF shall record the details of a vulnerability scan and,

if configured by the security administrator, generate an alert.

6.2.8.4 VDS_RVR.1 Restricted Vulnerability Report Review

VDS_RVR.1.1 The TSF shall provide **security administrators** with the capability to generate a vulnerability detection report.

VDS_RVR.1.2 The TSF shall provide the report in a manner suitable for the user to interpret the information.

VDS_RVR.1.3 The TSF shall prohibit all users read access to the System data and the corresponding vulnerability detection report, except those users that have been granted explicit read-access.

6.2.8.5 VDS_STG.1 Protected System Data Storage

VDS_STG.1.1 The TSF shall protect the stored System data from unauthorised deletion.

VDS_STG.1.2 The TSF shall protect the stored System data from modification.

6.3 TOE Security Assurance Requirements

The Security assurance requirements (SARs) provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, and vulnerability assessment). The table below identifies the security assurance requirements for the TOE drawn from CC Part 3: Security Assurance Requirements that meet an Evaluation Assurance Level 2 augmented with ALC_FLR.2 as defined by the CC.

Assurance Class	Assurance Component ID	Assurance Component Name
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	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
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements

Assurance Class	Assurance Component ID	Assurance Component Name
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

Table 6: Security Assurance Requirements

6.4 Security Requirements Rationale

6.4.1 Rationale For Not Satisfying All Dependencies

This section includes a table of all the TOE security functional requirements and their associated dependencies with a rationale for any dependencies that are not satisfied.

SFR	Dependencies	Met by the TOE?
FAU_GEN.1	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FAU_STG.1	FAU_GEN.1	Yes
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Yes
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes
FCS_COP.1a-e	FDP_ITC.1 or FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4	Yes
FIA_AFL.1	FIA_UAU.1	Yes
FIA_ATD.1	None	N/A
FIA_SOS.1	None	N/A
FIA_UAU.1	FIA_UID.1	Yes
FIA_UID.1	None	N/A
FMT_MOF.1a, b	FMT_SMR.1 FMT_SMF.1	Yes

FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	Yes
FPT_ITT.1	None	N/A
FPT_STM.1	None	N/A
FTA_SSL.4	None	N/A
FTP_TRP.1	None	N/A
VDS_SDC.1	None	N/A
VDS_ANL.1	None	N/A
VDS_RCT.1	None	N/A
VDS_RVR.1	None	N/A
VDS_STG.1	None	N/A

Table 7: SFR Dependencies

6.4.2 TOE SFR to TOE Security Objective Tracings

	O.PROTCT	O.VDSCAN	O.VDPROF	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.TIME
FAU_GEN.1								X		
FAU_SAR.1				X						
FAU_SAR.2					X	X				
FAU_STG.1	X				X	X	X		X	
FCS_CKM.1	X									
FCS_CKM.4	X									
FCS_COP.1a-e	X									
FIA_AFL.1						X				
FIA_ATD.1						X				
FIA_SOS.1						X				

	O.PROTCT	O.VDSCAN	O.VDPROF	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.TIME
FIA_UAU.1					X	X				
FIA_UID.1					X	X				
FMT_MOF.1a	X				X	X				
FMT_MOF.1b	X				X	X				
FMT_MTD.1	X				X	X			X	
FMT_SMF.1	X				X	X			X	
FMT_SMR.1						X				
FPT_ITT.1	X								X	
FPT_STM.1								X		X
FTA_SSL.4				X	X					
FTP_TRP.1	X								X	
VDS_SDC.1		X	X							
VDS_ANL.1			X							
VDS_RCT.1			X							
VDS_RVR				X	X	X				
VDS_STG.1	X				X	X	X		X	

Table 8: Mappings between TOE SFRs and Security Objectives

6.4.3 TOE SFR Rationale

The following discussion provides detailed evidence of coverage for each security objective.

O.PROTCT — The TOE must protect itself from unauthorized modifications and access to its functions and data.

The TOE is required to protect the audit data from unauthorized modification and unauthorized deletion [FAU_STG.1]. The TOE is required to protect the System data from any modification and unauthorized deletion [VDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1a, b]. Only security administrators may manage TOE data [FMT_MTD.1]. The TOE provides a set of management functions for use by administrators [FMT_SMF.1]. The TOE includes FIPS certified OpenSSL cryptographic modules to provide the

	cryptography used by the TLS implementation which protects network communications. It performs key generation, key distribution, key destruction, hashing, encryption/decryption, public key generation, message authentication code and digital signing [FCS_CKM.1, FCS_CKM.4, FCS_COP.1a-e]. The TOE protects the collected data from modification and ensure its integrity when the data is transmitted between distributed TOE components [FPT_ITT.1]. The TOE ensures authentication of communication end points and protects management data from modification and ensure its integrity when the data is transmitted between the TOE and the management workstation [FTP_TRP.1].
O.VDSCAN	The TOE must scan the network to discover hosts (IP addresses) to analyze for potential vulnerabilities. The TOE is required to collect information from targeted host System resources [VDS_SDC.1].
O.VDPROF	The TOE must systematically profile the host to detect vulnerabilities that match the set of vulnerabilities that the TOE is configured to detect. The TOE is required to collect information from targeted host System resources [VDS_SDC.1].The TOE is required to perform vulnerability analysis on all data received from the targeted hosts and generate conclusions [VDS_ANL.1]. The TOE is required to record the details of detected vulnerabilities and generate alerts as configured by the security administrator [VDS_RCT.1].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1a, b]. Only security administrators may manage TOE data [FMT_MTD.1]. The TOE provides a set of management functions for use by administrators [FMT_SMF.1]. The TOE must provide the ability for security administrators to generate and view vulnerability detection reports [VDS_RVR.1]. The TOE provides the ability for users to terminate their session [FTA_SSL.4].
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE must provide the ability for security administrators to generate and view vulnerability detection reports [VDS_RVR.1]. The TOE is required to protect the audit data from unauthorized modification and unauthorized deletion [FAU_STG.1]. The TOE is required to protect the System data from any modification and unauthorized deletion, [VDS_STG.1]. Users authorized to access the TOE are defined using an

identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1a, b]. Only security administrators may manage TOE data [FMT_MTD.1]. The TOE provides a set of management functions for use by administrators [FMT_SMF.1]. The TOE provides the ability for users to terminate a session with the TOE [FTA_SSL.4]

O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE is required to restrict the review of vulnerability detection reports to those granted with explicit read-access [VDS_RVR.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.1]. The System is required to protect the System data from any modification and unauthorized deletion[VDS_STG.1]. Security attributes of subjects used to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. The TOE provides restrictions on the complexity of passwords unless set by an Administrator [FIA_SOS.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE provides the ability to disable (lock out) user accounts after three unsuccessful authentication attempts using the REST API, Default UI, and Legacy UI [FIA_AFL.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1a, b]. Only security administrators may manage TOE data [FMT_MTD.1]. The TOE provides a set of management functions for use by administrators [FMT_SMF.1]. The TOE must be able to recognize the user roles that exist for the TOE [FMT_SMR.1].
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows. The TOE is required to protect the audit data from unauthorized modification and unauthorized deletion [FAU_STG.1]. The TOE is required to protect the System data from any modification and unauthorized deletion [VDS_STG.1].
O.AUDITS	The TOE must record audit records for use of the management functions. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1].
O.INTEGR	The TOE must ensure the integrity of all audit and System data. The TOE is required to protect the audit data from unauthorized modification and unauthorized deletion [FAU_STG.1]. The TOE is required to protect the System data from any modification and unauthorized deletion [VDS_STG.1]. Only security administrators may manage TOE data [FMT_MTD.1]. The TOE provides

a set of management functions for use by administrators [FMT_SMF.1]. The TOE protects the collected data from modification and ensure its integrity when the data is transmitted between distributed TOE components [FPT_ITT.1]. The TOE ensures authentication of communication end points and protects management data from modification and ensure its integrity when the data is transmitted between the TOE and the management workstation [FTP_TRP.1].

O.TIME	The TOE must provide reliable time stamps. Time stamps associated with an audit record must be reliable. The hardware and operating system in the TOE provide reliable time stamps upon request [FPT_STM.1].

6.4.4 SAR Rationale

The TOE and this ST are EAL2 conformant, augmented with ALC_FLR.2.

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the system may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the system will have incurred a search for obvious flaws to support its introduction to the non-hostile environment.

7 TOE Summary Specification

This chapter describes the TOE security functions.

7.1 Vulnerability Detection System

Tripwire IP360 enables organizations to detect, understand, and respond to vulnerabilities on their networks. The scanning appliances are centrally administered for complete automation of application and vulnerability signature updates.

Tripwire IP360 scanning is based on Tripwire's ASPL, or Advanced Security Profiling Language. ASPL is a powerful, flexible, and easy-to-use language that can extend Tripwire IP360 discovery and profiling to your custom applications and/or policy monitoring. Tripwire IP360 includes an ASPL Rules Wizard, and training classes and professional services are available.

7.1.1 System Data Collection

Tripwire IP360 begins each scan with a discovery phase for IP addresses within the scope of the defined network configuration. This discovery process is user-configurable, but typically consists of ICMP echo requests (pings) to each IP address first, and then scanning for a short list of open TCP ports on each IP address if a ping response is not received.

Once an active host is detected, Tripwire IP360 begins a systematic process of profiling the host. These steps may include:

- Stack fingerprint
- TCP and UDP port scan
- External application identification
- External vulnerability detection
- Preliminary OS detection
- Host authentication
- Credentialed enumeration of host applications
- Credentialed vulnerability detection
- Final OS detection
- Enumeration and recording of additional host information (e.g., Windows shares, service banners, last logged in user, etc.)

Device Profilers have only the SSH port open (optional) and do not store any scan results locally. All system data collected from the scans is stored within the Tripwire IP360 VnE Manager database with a timestamp. Therefore, Tripwire IP360 appliances can be distributed throughout the network with no concern for data stored in "less secure" remote locations since client data is not stored locally. The TOE does not provide any interfaces to modify system data in the database. In addition, only authorized deletions from database are allowed.

ASPL content updates are released weekly, usually on Wednesdays. These vulnerability signature updates contain detection methods for known vulnerabilities, including vulnerabilities in applications,

protocols, and operating systems.

Tripwire IP360 provides granular scheduling capabilities. Scheduling options include:

- Immediate "OnDemand" scan
- One-time "OnDemand" scan scheduled for a specified date and time
- Recurring scans:
    - Continuous
    - N times per hour, day, or week
    - Scan on specified day or days of week (Monday, Tuesday, etc.)
    - Scan on specified relative days of month (1st Sunday, 2ndMonday, etc.)
    - Scan on specified dates of the month

All recurring scans can be further confined to execute only within a designated scan window which includes the associated Time Zone. If a scan is not completed during the scan window, the scan is suspended and restarted the next time the scan window is available. An authorized user can view the detailed status of all scans within their area of responsibility. All executing scans can be paused with a single click, and individual scans can be paused, resumed, or canceled. The Tripwire IP360 API lets you manage scans from a script to achieve desired customization of scanning processes if necessary.

After the discovery phase, the scans inventory the applications installed on each host. This list of applications determines which vulnerability checks are performed. The application inventory is also populated into the system database and can be used as criteria for reporting.

Tripwire IP360 scanning combines both remote assessment and local authenticated checks when credentials are available. Authenticated checking (checking performed using known credentials) is called deep reflex testing (DRT). Credentials can be provided for Windows (either WMI or SMB access will work transparently), SSH with a password or a private key, SNMPv1andv2, Web authentication to a form, and Web authentication via HTTP.

Tripwire IP360 applies credentials based on the type of host. For example, if a Network Configuration contains a mixture of Windows, *NIX, and network infrastructure, Tripwire IP360 will choose the Windows credential for the Windows hosts, the SSH credential for the *NIX hosts, and either SSH or SNMP v1 or v2 for the network infrastructure. The Tripwire IP360 Agent removes the need to know the host credentials since the Agent is installed on the scanned host.

Remote checking (or non-DRT) involves checking the network traffic, querying a remote service, checking the response or full protocol implementation of a listening port on a device.

The system data collected for each host is dependent upon the vulnerabilities being checked. The system data stored for each host includes the date and time of the scan and is dependent upon the vulnerabilities detected and the type of vulnerabilities. The following types of information can be collected and stored: network traffic, registry keys, file versions, file contents, command outputs, access control lists, and service interrogation. Network traffic and service interrogation are not performed when using the Axon Agent.

7.1.2 Analyser Analysis and Reaction

The Tripwire IP360 VnE Manager is the single point of administration for software and vulnerability signature updates. The VnE Manager automatically checks for and downloads any new updates on a daily basis. Once a software update is initiated by an Administrator, the VnE Manager updates its software as well as the software of all of its scanning appliances (Device Profilers). Software updates may include operating system and database updates as necessary. Software updates must be initiated by a Tripwire IP360 Administrator. Once the update is initiated, all steps for installing the update to the VnE Manager and Device Profilers are completely automated, including reboots of the appliances if required. Vulnerability updates can be fully automated or can be held for manual initiation of the update by an Administrator.

Tripwire IP360's vulnerability risk score aids in identifying hosts that have unacceptable levels of risk and vulnerabilities that are creating that risk. The Tripwire IP360 vulnerability risk score combines the human judgment of Tripwire's Vulnerability and Exposure Research Team with an algorithm that weighs the risk characteristics of each vulnerability (Risk Class, Available Exploits, and Vulnerability Age) to compute a numerical score that can range from zero to more than 50,000. These scores are combined for each host to produce its Host Score, which lets you know at a glance if a host has any significant vulnerabilities.

Tripwire IP360 performs two generic types of analysis:

- Direct Condition Test – communication with a host that directly tests for a vulnerability condition (e.g., Send a payload to a host containing an attack payload); uses a set of interactions with the host used to identify known vulnerabilities
- Inference – communicating with a host to confirm that it responds with a secure, expected response; (e.g., A vulnerability is patched and the data response changes)

Data collected from other hosts is analyzed in real-time and the interpretation of that a data is stored. The system data collected and stored includes all data necessary for detecting vulnerabilities, except for encrypted sessions. In addition, data collection for protocol and service interactions that do not produce a vulnerability risk are not stored.

Tripwire IP360 can generate alerts for new discovered hosts, hosts with an excessive Vulnerability Score, and any specified list of high risk vulnerabilities. The security administrator can configure the system to send an email or generate an SNMP trap when an alert is triggered.

7.1.3 SFR Mapping

The VDS function is designed to satisfy the following security functional requirements:

- VDS_SDC.1: The DP and VnE components work together to collect and store information on hosts needed for vulnerability detection.
- VDS_ANL.1: The TOE can analyze the collected data to detect known vulnerabilities based on the vulnerability signatures distributed by Tripwire, Inc. The TOE uses the direct condition test and inference analysis functions.
- VDS_RCT.1: When a vulnerability is detected, the TOE records the details of detected vulnerabilities and generate alerts (sends an email alert or SNMP trap) as configured by the security administrator.

- VDS_STG.1: The VnE stores the system data in the database which protects the data from unauthorized deletion and modification.

7.2 Security audit

The TOE has five types of audit data logs: User Activity Log, REST API log, REST access log, VnE log, and DP log. No user is able to modify the logs. Only the Administrator role and security administrator with the appropriate access right is able to archive the audit records.

The TOE audits all information described in Table 5: Auditable Events. No users of the TOE have access to stop the collection of Audit Logs. The start-up and shut down of audit functions corresponds to when the VnE and DP are powered on and off. The start-up and shut down of the VnE are logged in the VnE Log. The start-up and shut down of the DP are logged in the DP Log. The VnE and DP logs are presented in a plain text file.

The User Activity Log (UAL) contains audit entries of many of the tasks performed by users using the Legacy UI and Default UI, including all attempts to authenticate. The REST access log contains all audit entries of administrative tasks performed by the Default UI. The Legacy UI and Default UI are the primary interfaces used to access and manage the VnE and the overall TOE. Audit records in the UAL are stored in the database. The UAL can be viewed by the administrator and security administrator with the appropriate access right is able to archive the audit records using the Legacy UI. The REST access log can be viewed from the VnE CLI.

The audit records generated by the TOE also include a timestamp, the event being logged, the subsystem triggering the log, and the outcome of the event. By default all audit records result from successful operations and unsuccessful operations are ceased and not audited with the exception of login failures.

7.2.1 Security Audit Event Storage

Tripwire IP360 does not provide a mechanism for any TOE User to delete the audit logs directly. Audit logs cannot be modified by any level of user of the TOE. Audit logs can be archived. Archiving involves copying records to an external system (outside the TOE) and then deleting the records after they are archived.

7.2.2 SFR Mapping

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE generates audit records for including startup and shutdown of audit functions, for TOE management events performed using the Default UI and Legacy UI, and for user identification and authentication attempts.
- FAU_SAR.1: The TOE provides users with the Administrator role and users with appropriate access rights the ability to read the UAL using the Legacy UI.
- FAU_SAR.2: The TOE protects the audit records by restricting read access to only those users that have been granted read access to the audit records.
- FAU_STG.1: The TOE protects the stored audit records from unauthorized deletion and prevents modifications to the messages.

7.3 Identification and authentication

Users must be identified and authenticated prior to interacting with the TOE. All security-relevant mediated functions require the user to be authenticated. The TOE creates and maintains the user account information in the IP360 database. The TOE itself identifies and authenticates the username and password supplied. Passwords are always used for identifying and authenticating the default "administrator" account.

The TOE maintains the following security attributes for each Internal User: user identity, password, user groups, role information, and user access rights.

Guidance directs the administrator that in the evaluated configuration, the password complexity feature and following rules must be enabled:

- Minimum password length must be 8-12.
- Minimum number of numeric characters must be at least 1.
- Minimum number of alphabetic characters must be at least 1.
- Minimum number of non-alphanumeric ASCII characters must be at least 1.
- Minimum number of hours required before changing a password again: 48.

Administrators can set passwords to any value, regardless of the password policy. Guidance provides recommendations to the users for creating strong passwords. Guidance instructs administrators to adhere to the above password policy.

In the evaluated configuration, all users are internal users whose user identification, hashed password, user access rights, roles, and group memberships are stored in the IP360 database. During login, the TOE checks its user account database for the username provided. If the username is not in the user account database, the login attempt fails. If the username is a valid username, the TOE compares a hash of the password provided against the hashed password value stored in the DB. If either the login name or password is incorrect the login request will fail and no additional functions will be made available. As a result of a successful login, a subject is created on behalf of the client. The TOE assigns the subject the roles and groups associated with the TE user account.

User access rights enable a user to access TOE data and to perform selected functions. A role is a collection of user access rights that may be assigned to a user account. A user group is a collection of user accounts. Note that groups are used to simplify access control management.

The TOE will lock out local user accounts for 20 minutes after three consecutive failed login attempts on any combination of the REST API and Default UI. The TOE implements one failed authentication attempt counter that is shared by the REST API and Default UI. The Legacy UI is accessed by logging into the Default UI and switching to the Legacy UI from within the Default UI.

In addition, the TOE implements a log out capability which allows users to terminate their current session.

7.3.1 SFR Mapping

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1: The TOE disables (locks out) user accounts for 20 minutes after three consecutive failed login attempts on the REST API, Default UI, and Legacy UI interfaces.
- FIA_ATD.1: The TOE defines user identities, authentication data (passwords), user groups, access rights, and role information.
- FIA_SOS.1: The TOE enforces restrictions on the complexity of a password, including password length and minimum length of time before a password can be changed again.
- FIA_UAU.1: The TOE offers no functions until the user is authenticated. The TOE performs password-based user authentication.
- FIA_UID.1: The TOE offers no functions until the user is identified. The TOE performs user identification based on the user name.
- FTA_SSL.4: The TOE implements the ability for users to terminate their own sessions.

7.4 Security management

The TOE provides the following administrative interfaces:

- Default UI (access to VnE)
- Legacy UI (access to VnE)
- VnE CLI
- DP CLI
- XML-RPC API (access to VnE)
- REST API (access to VnE)

The Tripwire IP360 VnE Manager is the single point of administration for software and vulnerability signature updates. The VnE Manager automatically checks for and downloads any new updates on a daily basis. Once a software update is initiated by an Administrator, the VnE Manager updates its software as well as the software of all of its scanning appliances (Device Profilers). Software updates may include operating system and database updates as necessary. Software updates must be initiated by a Tripwire IP360 Administrator. Once the update is initiated, all steps for installing the update to the VnE Manager and Device Profilers are completely automated, including reboots of the appliances if required. Vulnerability updates can be fully automated or can be held for manual initiation of the update by an Administrator.

The TOE data is stored in the database located on the VnE Manager. Only Tripwire Support has the capability to directly access the database. IP360 does provide an interface to allow security administrators to export the database.

The VnE and DP CLI interfaces are accessible through the serial port and via SSH.

Access to the functions provided by the interfaces is based on the roles and access rights assigned to users. Access rights can be assigned by either directly assigning an individual user access rights or by assigning the user a role that contains the access rights. The Administrator role gives the user access to all of Tripwire ip360's functionality and interfaces. When a role is created, access rights are assigned to that role. Users that are assigned a role are provided the access rights specified by the role. Roles can be created and a role's access rights can be modified using the Legacy UI. Roles can be assigned and

removed from a user using either the Default UI or the Legacy UI.

All tasks provided by the CLI require the Administrator role. Tasks that users can perform on objects are based on the following basic access types: Read Only, Read-Write, Read-Scan, Create. For a list of the access rights / roles required to perform tasks in the Default UI, refer to Table 12. For a list of the access rights / roles required to perform tasks in the Legacy UI, refer to Table 11.

The security administrator role is defined in this ST to include the Administrator role, each of the roles defined in Table 11 and Table 12, and any user directly assigned access rights.

Functions for which a user does not have sufficient permissions will either be hidden from the user interface or the options will be disabled.

Users can also be organized into groups to help identify assets that are managed by a group of individuals, as opposed to an individual user. User groups also streamline the management of multiple users at one time. User groups do not have access rights associated with them. Groups can be managed using the Legacy UI.

In the evaluated configuration, all users are internal users whose credentials, roles, and group memberships are stored in the IP360 database.

The Legacy and Default UI provide the ability to manage network configurations, credentials used for scanning/profiling, scans, scan appliances (device profiler), host profiling, custom ASPL, reports, ticketing, certificates, password policy, and users/roles. Refer to Appendix A: Access Rights for a detailed description of what capabilities are provided by each management interface along with the required access rights for each task.

The VnE Manager offers a XML-RPC API and a REST API. The XML-RPC API permits programmatic management of the elements of the scanning process and integration with other components of the security solution. The REST API provides similar functionality as well the following new features: Default UI, DP pooling, agent-based vulnerability management. The XML-RPC API is used by the Legacy API to process the user requests. The REST API is used by the Default API to process the user requests.

Users with the appropriate privilege can generate reports on the scanning and profiling performed on a host. Reports are provided in a human-readable and interpretable manner. Reports are generated on-demand as requested by the security administrator.

7.4.1 SFR Mapping

The Security management function is designed to satisfy the following security functional requirements:

- VDS_RVR.1: The VnE provides the ability for security administrators to generate vulnerability detection reports.
- FMT_MOF.1a: The TOE restricts the ability to manage scan discovery and host profiling functions to authorised system administrators.
- FMT_MOF.1b: The TOE restricts the ability to enable or disable vulnerability scanning functions to authorised system administrators.
- FMT_MTD.1: The TOE restricts the ability to manage TSF data as specified in Section 8.
- FMT_SMF.1: The TOE provides security management functions for use by the administrators.

- FMT_SMR.1: The security administrator role is satisfied by the Administrator role, each of the roles defined in Table 11 and Table 12, and any users assigned access rights.

7.5 Protection of the TSF

The Tripwire IP360 TOE is provided in two configurations: physical hardware appliances or supported virtual platforms. In both cases, the Tripwire IP360 Version 9.0.1 software is installed on the platform. The TOE hardware and operating system provides process isolation to each process with its own unique address space and separation from all processes.

The TOE provides reliable time stamps for use in audit records, system data collection records, and scheduling. The TOE hardware clock and operating system provide reliable time stamps. The TOE can be configured to use NTP to set and synchronize the hardware clock.

The TOE includes the FIPS certified cryptographic modules that are used to implement TLS to protect communications between the TOE's distributed components. The FIPS certified cryptographic modules perform key generation and cryptographic key destruction.

The TOE uses HTTPS to protect TSF and user data transmitted between the Legacy or Default UI and the user's browser. The TOE uses SSH to protect TSF and user data transmitted between the CLI and the remote user's station. TLS is used to protect TSF and user data transmitted using the XML-RPC API and the REST API.

The TOE provides identification and authentication of its administrative interfaces, thereby preventing circumvention of the access control mechanism.

The VnE and DP use the OpenSSL FIPS Object Module SE v2.0.16 library (FIPS certificate number 2398) to implement TLS connections. In the evaluated configuration, the VnE must be configured with FIPS+secure mode enabled, which ensures that only TLS v1.2 is allowed (TLS v1.0 and v1.1 are disabled). In addition, the DP is configured with FIPS mode enabled.

OpenSSL in the VnE and DP implements the following validated algorithms:

Algorithms / Key Sizes	Uses
AES (CTR mode, 128/192/256 bit key sizes)	SSH
AES (GCM mode, 128/256 bit key sizes)	TLS
RSA (2048 bit keys) following FIPS PUB 186-4, Appendix B.3	TLS/key generation and signature services
HMAC with SHA-1	SSH
SHA-256, SHA-384	TLS

Table 9: Cryptographic Algorithms in VnE and DP

The Agents use the OpenSSL FIPS Object Module SE v2.0.16 library (FIPS certificate number 2398) to implement TLS connections with the DP. In the evaluated configuration, the Agents must be configured with FIPS mode enabled and to only use TLS v1.2 (TLS v1.0 and v1.1 are disabled).

The vendor affirms that no source code changes were made to the OpenSSL FIPS Object Module SE v2.0.16 cryptographic software module before compilation of the Tripwire IP360 v9.0.1 software.

The OpenSSL module used by the Agent implements the following validated algorithms:

Algorithms / Key Sizes	Uses
AES 128/256-bit	TLS
AES 256-bit (GCM mode)	TLS
Triple DES 128/192-bit (CDC mode)	TLS
RSA (2048-bit keys) following FIPS PUB 186-4, Appendix B.3	TLS/key generation and signature services
SHA-1, SHA-256, SHA-384	TLS

Table 10: Cryptographic Algorithms in Agent

7.5.1 SFR Mapping

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_ITT.1: OpenSSL protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE by providing a secure channel using TLS.
- FPT_STM.1: The TOE hardware and operating system provides reliable time stamps. The TOE uses this reliable time appropriately.
- FTP_TRP.1: OpenSSL protects TSF data from disclosure and modification when it is transmitted between the user's browser and either the Legacy or Default UI. SSH protects TSF data from disclosure and modification when it is transmitted between the user system and the CLI. TLS is used to protect transmissions using the XML-RPC API and REST API.
- FCS_COP.1a-e: The FIPS certified OpenSSL modules perform the cryptographic operations as listed in the corresponding SFRs. These operations are used to implement TLS/HTTPS and SSH.
- FCS_CKM.1: The FIPS certified OpenSSL module performs key generation necessary to implement TLS.
- FCS_CKM.4: The FIPS certified OpenSSL module destroys the cryptographic keys as specified in FIPS 140-2.

8 Appendix A: Access Rights

All tasks in the CLI require the Administrator role.

The user access rights (permissions) required to perform specific tasks in the XML-RPC API and the Legacy UI are defined in Table 11: Legacy UI Access Rights.

The user access rights (permissions) required to perform specific tasks in the REST API and Default UI are defined in Table 12: Default UI Access Rights.

Task	**Access Rights**
Alerts (Create Ticket, Email, SNMP)	For all Alerts: • Read-Write to Alerts(Email, SNMP, or Create Ticket) and Read-Only access to the network to define alerts • Read-Only to search for and view alerts For SNMP Alerts: • Read-Write to SNMP Alerts and Read-Only to the network. • Read-Write to "SNMP Configuration" to enable SNMP traps. • Read-Write to Alerts (Create Ticket) to enable automatic ticket creation.
Appliance	Often works with Network and Scan Profiles. Assigned globally for all appliances or to specific appliances. For Scans: • Read-Only to run scheduled scans, to pause and resume scans, and to cancel scans. • Read-Write to run manual scans. For Administration: • Read-Write to configure DNS, to set the upper performance limit, to remotely reboot an appliance, and to view the appliance logs. • Read-Only to view a list of appliances. Master Customers: • Read-Write to assign an appliance to a customer. For Ticketing: • Read-Only access to create, view, modify, or resolve a ticket for an appliance. For Appliance Down tickets, all users are available; assign the ticket to a user that has Read-Only access to the appliance.
Broadcast Message	Read-Write to send an email message to user accounts on the VnE. SMTP server must be configured.

Task	Access Rights
Certificate Management	For web and TripwireIP360 certificates: • Read-Write to Certificate Management and to "VnE Manager" to manage web and TripwireIP360 certificates. For authentication keys: • Read-Write to modify authentication keys. Used for additional VnE enrollment to receive package updates from the master VnE.
Contact Support	Read Write to open a case with Tripwire Customer Support. Cases are opened from the TripwireIP360 interface under Administer:Support>SupportContactInformation.
Credentials Management	Read-Write to a network needed to bind credentials to it. • Read-Write to create, modify, and delete credentials and to bind them to networks. • Read-Only to view credentials.
Custom ASPL	Read-Write to define and delete vulnerability conditions. • Read-Write to bind or delete rules. • Read-Write to modify custom conditions. • All users can search ASPL.
Custom OS Group	Read-Write to create OS groups.
Database Settings	Read-Write to change database settings and to configure backup and archive.
Downstream VnEs	Administrator rights to configure a downstream VnE that can use this VnE as an Upstream Software Repository to Download TripwireIP360 packages.
Globally Excluded IPs	Read-Write required to specify a global IP exclusion
Network Group	Permissions assigned to a Network Group apply to all Networks in the group. The user must have permissions to the individual networks contained in a group. • Read-Only or Read-Scan to run reports; but can "Override viewer access rights" for network groups in a report. • Read-Only to export report results. • Read-Write to group networks (requires Read-Write to the specific networks). • Read-Only access to view affiliated networks (requires Read-Only to the specific networks). • Read-Scan to scan the networks contained in a network group (requires ReadScan to the specific networks and at least Read-Only access to appliance and scan profile). • Create to create network groups within an instance
Network	The Network permissions are combined with Appliance and Scan Profiles permissions. For Network Tasks: • Read-Scan to scan a network and to assign an appliance and scan profile to a network.

Task	Access Rights
	(requires at least Read-Only access to appliance and scan profile) • Read-Write to define a new network. • Read-Write to a specific network to modify it. • Read-Write required to setup host tracking on a network. • Read-Write to include or exclude IPs within a network definition. • Read-Write to bind credentials to a network. • Read-Write to place a network in a group. • Read-Write to activate or de-activate a network and to delete a network. • Read-Only to export the network configuration. • Create to create networks within an instance. For Reports: • Read-Scan or Read-Only to run reports; however, can "Override viewer access rights" for networks in a report. • Read-Only to export report results For Focus: • Read-Only to view host information and create tickets in Focus. • Read-Write to modify host in Focus. For Scanning: • Read-Scan to run scheduled or manual scans; note that Read-Only to the appliance is required to run scheduled scans and Read-Write to the appliance is required to run a manual scan. • Read-Write to pause and resume scans. • Read-Write to cancel a scan. • Read-Only to view scan progress. • Read-Only to view scan history and Distinct Audits. • Read-Only to export scan data. For Scan Profiles: • Read-Only access to a network grants implicit Read-Only access to scan profiles and scan configurations bound to the network through the network's definition. For Alerts: • Read-Only to define scan completion alerts for a network. • Read-Only to define an SNMP alert. For Ticketing: • Read-Only to a host's network to create, view, modify, or resolve a ticket for it. Requires Read-Only to the Appliance. For all ticket types except Appliance Down, only those users with access rights to the ticket's network are available for assignment. For Appliance Down tickets, all users are available; assign the ticket to a user that has Read-Only access to the appliance.
Password Policy	Read-Write to set the password policy.
Role	Read-Write to the role and Read-Write to the user account to assign a user to the role, or to assign a role to the user.

Task	Access Rights
Scan Profiles	Notes: The Scan Profiles permissions are often combined with Appliance and Network permissions. Read-Only Permission: • Read-Only to run a scheduled or manual scan. • Read-Only to cancel scans. • Read-Only access to export scan profile configuration. • Read-Only to a network implicitly grants Read-Only access to a scan profile bound to that network. Read-Write Permission: • Read-Write to create or modify scan profiles. • Read-Write to create a schedule for a scan profile. • Read-Write to enable Stack Fingerprinting, SSH-DRT and WDRT, application scans, vulnerability scans, and Full Port Scans. • Read-Write to limit bandwidth usage, to select host discovery method, to specify ports to be scanned, and to fine tune vulnerabilities. CreatePermission: Explicit permission that allows users to create new scan profiles. It includes Read-Write privileges to the scan profile, as well as View and Modify privileges. When Create permission is assigned to a user for the Scan Profile area, a New button is displayed to allow them to create a new scan profile.
SNMP Configuration	• Read Write to configure SNMP. • Read Write to enable and disable SNMP traps. • Read Write to Alerts (SNMP) and at least Read-Only access to the network on which the alert is defined to define an SNMP alert. See “Alerts”.
Software Upgrades	• Administrator rights to configure proxy support. • Administrator rights to configure the software repository. • Administrator rights to upgrade the VnE Manager and to specify upgrade settings. • Administrator to view upgrade settings.
Ticketing Management	• Read Write access to both Ticketing Management and Alerts to enable automatic ticket creation. • Read Write to delete queued tickets, to enable or disable ETS integration, and to invoke any methods in the external API. • Read Write to customize ticket forms. • Read Only to view the related screens. • All users can view ticket statistics. All users can create, view, modify, and delete ticket reports.

Task	Access Rights
Trouble Reporting	• Read Write to close trouble reports. • Read Only to view trouble reports. • Read Only to view VnE Manage Logs.
User Group	• Read Write to create, edit, and delete user groups. • Read Write access both for a user and for a user group to assign the user to the group. Note that a non-Administrator user cannot have Read-Write access to an Administrator user, so a non-Administrator user may not assign or remove Administrator users from groups. • Read Write to import user records. • Read Only to view the members of a user group.
Users Import	Read Write to import external users from LDAP or Active Directory.
Users	The Users permissions apply to both Internal (created in Tripwire IP360) and External (imported from LDAP/ActiveDirectory) users. • Read Write to the user record to assign it individual access rights. • Read Write to both Role and User Account to assign a user to a role. • Read Write to Users or User Groups to create, edit, and delete a user or user group. • Read Write to Users and User Groups to import user records. • Read Write to the user to enable or disable the user account. • Read Write to the user account to force its password to expire. • Read Only to user account to view the activity logs.
VnE Manager	• Read Write to specify system settings. • Read Write access to provide SSH keys and to configure SSH. • Read Write access to configure VnE Manager authentication and communication. • Read Write access to VnE Manager and to Certificate Management to manage web certificates. • Read Write access to configure mail system. • Read Write to install new modules. • Read Write to setup system alert emails. • Read Write to enable or disable FIPS compliance and Strong Session. • Read Write required to provide router configuration files. • Read Write required to create and manage Threat Zone Groups. • Read Only access to the VnE Manager to access VnE configuration data and view system settings. • Read Only to view disk usage statistics.

Table 11: Legacy UI Access Rights

Functional Area	Function	Minimum Access Rights / Role
DNS Servers	View, Add, Duplicate, Edit, Delete DNS Servers	Appliance: Read-Write
Hardware Status	View Hardware Status	VnE Manager: Read Only
Network Credentials	View Network Credentials	Credential Management: Read Only
	Add, Edit, Delete Network Credentials	Credential Management: Read-Write
	Bind Network Credentials	Credential Management: Read-Write and Network Access: Read Only
	Test Network Credentials	Credential Management: Read-Write and Network Access: Read-Scan
Networks	View Networks	Networks Access: Read Only
	Add, Duplicate, Import Networks	Networks Access: Create
	Edit, Delete Networks	Networks Access: Read-Write
Scan Appliances	View Scan Appliances	Appliance: Read Only
	Add, Edit, Delete, Reboot Scan Appliances	Appliance: Read-Write
	View Scan Appliance Pools	Appliance: Read Only Appliance Category: Read Only Note: If the appliance pool is empty then the Read Only permission is required on the Appliances category or on ANY appliance. If the pool contains appliances, then the Read Only permission is required on the Appliances category or on ALL appliances currently assigned to the pool.
	Add, Edit, Delete Scan Appliance Pools	Appliance: Read-Write Appliance Category: Read-Write
	Assign an appliance to an empty Pool	Appliance: Read-Write Note: If the appliance pool contains no other appliances, then the Read-Write permission is required on the appliances category or on ANY appliance.
	Assign an appliance to an occupied Pool	Appliance: Read-Write Note: If the appliance pool contains other appliances, then the Read-Write permission is required on ALL appliances already assigned to the pool, as well as the appliance being added to the pool.

Scan Activity	View Scan Activity View Scan progress details View distinct audit reports	Network: Read Only Note: If a user is assigned permissions to only specific Networks, only the networks for which they have at least Read Only access will be visible in the Scan Activity widget.
	Export Scan Activity and History	Appliance: Read Only Note: If a user is assigned permissions to only specific Networks, only the networks for which they have at least Read Only access will be visible in the Scan Activity export.
	Re-run Scans	Appliance: Read-Write and Network: Read-Scan and Scan Profiles: Read Only Note: If a user is assigned permissions to only specific Networks, only the networks for which they have at least Read Only access will be visible in the Scan Activity widget.
	Pause an in progress scan Resume suspended, paused, or auto-paused scans Cancel in progress, suspended, paused, or auto-paused scans	Appliance: Read-Write and Network: Read-Scan and Scan Profiles: Read Only Note: Appliance, Network, and Scan Profile permissions can be applied at the global level or to specific Appliances, Networks, or Scan Profiles. The widget will only display Appliances, Networks, and Scan Profiles for which the user has the minimal level of permissions.
	View scan progress details View distinct audit reports	Network: Read Only Note: If a user is assigned permissions to only specific Networks, only the networks for which they have at least Read Only access will be visible in the Scan Activity widget.
Scan Profiles	View Scan Profiles	Scan Profiles: Read Only Note: If a user is assigned permissions to only specific Scan Profiles, only the profiles for which they have at least Read Only access will be visible in the Scan Profiles widget.
	Add Scan Profiles	Scan Profiles: Create
	Edit, Duplicate Scan Profiles	Scan Profiles: Create Note: If a user is assigned permissions to only specific Scan Profiles, only the Scan Profiles for which they have at least Read Only access will be visible in the Scan Profiles widget.
	Delete Scan Profiles	Scan Profiles: Read-Write Note: If a user is assigned permissions to only specific Scan Profiles, only the Scan Profiles for which they have at least Read Only access will be visible in the Scan Profiles widget.

Scheduled Scans	View Scans	Appliance Pool: Read Only access to all appliances in the pool and Network Access: Read Only and Scan Profiles: Read Only Note: Appliance, Network, and Scan Profile permissions can be applied at the global level or to specific Appliances, Networks, or Scan Profiles. The widget will only display Appliances, Networks, and Scan Profiles for which the user has the minimal level of permissions.
	Add, Edit Scans	Appliance Pool: Read-Write access to all appliances in the pool and Network Access: Read Scan and Scan Profiles: Read Only Note: Appliance, Network, and Scan Profile permissions can be applied at the global level or to specific Appliances, Networks, or Scan Profiles. The Scheduled Scans widget will only display Appliances, Networks, and Scan Profiles for which the user has the minimal level of permissions.
	Duplicate, Delete Scans	Appliance: Read-Write and Network Access: Read Scan and Scan Profiles: Read Only Note: Appliance, Network, and Scan Profile permissions can be applied at the global level or to specific Appliances, Networks, or Scan Profiles. The Scheduled Scans widget will only display Appliances, Networks, and Scan Profiles for which the user has the minimal level of permissions.
	Resume Scans	Appliance: Read-Write and Network Access: Read Scan and Scan Profiles: Read Only Note: Network, and Scan Profile permissions can be applied at the global level or to specific Networks or Scan Profiles. The Scheduled Scans widget will only display Networks, and Scan Profiles for which the user has the minimal level of permissions.
TE Asset Matching		Administrator Role
TE Consoles		Administrator Role
TE Tag Rules		Administrator Role
Upgrades	View, Upload, Sync, Install Upgrades View Upgrade History	Upgrades
Users	View Users	Users: Read Only access to at least one user

	Add, Edit, Duplicate, Delete Users	Users: Read-Write
	Import Users	Users Import
	Unlock Users	Administrator Role
	Assign user roles Remove roles from users	Users: Read-Write Role: Read-Write
Reporting	Run reports Export report results	Network: Read Only
Focus	View host information	Network: Read Only
Notifications	View notifications	Administrator rights and master customer status to view license notifications Trouble Reports: Read Only to view trouble report notifications

Table 12: Default UI Access Rights