McAfee, Inc.
Vulnerability Manager v7.5.4

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.1

Prepared for:

McAfee, Inc.
2821 Mission College Blvd.
Santa Clara, CA 95054
United States of America

Phone: +1 800 847 8766
Email: sales@mcafee.com
http://www.mcafee.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the McAfee Vulnerability Manager v7.5.4, and will hereafter be referred to as the TOE throughout this document. The TOE is a Vulnerability Management System that scans specified targets for vulnerabilities and noncompliant configurations. It provides a management interface to configure the system and generate reports regarding the results of the scans.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	McAfee, Inc. Vulnerability Manager v7.5.4 Security Target
ST Version	Version 0.1
ST Author	Corsec Security, Inc.
ST Publication Date	2013-09-18
Certified Maintenance Report	McAfee Vulnerability Manager v7.5 CCEVS Approved Assurance Continuity Maintenance Report, VID10461-0001-ACMR, 10/31/2012
TOE Reference	McAfee Vulnerability Manager v7.5.4
Keywords	Vulnerability, vulnerability management, vulnerability assessment, vulnerability scanner, risk management, auditing, policy auditing, compliance, compliance auditing, SOX, FISMA, HIPAA, PCI DSS, SCAP, FDCC, scanner, configuration scanner

1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

Vulnerability Manager v7.5.4 is a software-only TOE that consists of several separate executable components. Figure 1 shows the detailed view of the CC-evaluated configuration of the TOE and contains the following previously-undefined acronyms and abbreviations:

- ePO- epolicy Orchestrator
- IIS - Internet Information Services
- OS- Operating System
- API - Application Program Interface
- LDAP - Lightweight Directory Access Protocol
- MDAC - Microsoft Data Access Components
- SQL - Structured Query Language

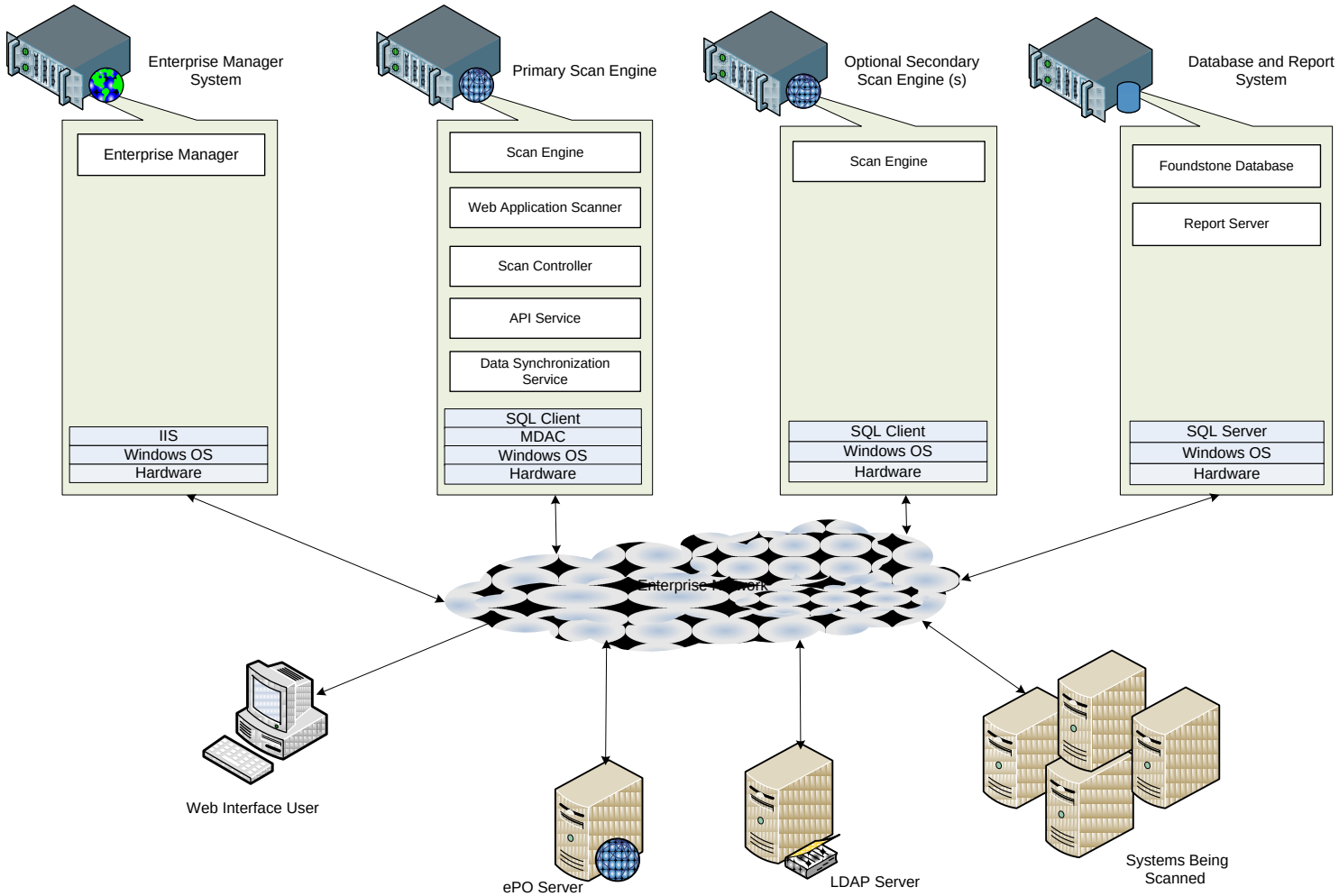

Figure 1 - CC-Evaluated Configuration of the TOE

The CC-evaluated configuration of the TOE is composed of:

- One Windows Server 2008 machine running as the Enterprise Manager System
- One Windows Server 2008 machine running as the Primary Scan Engine with Scan Engine, Web Application Scanner, Scan Controller, API Service, and Data Synchronization Service installed
- **(Optional)** Zero or more Windows Server 2008 machines running as the Secondary Scan Engines with Scan Engine installed
- One Windows Server 2008 machine running as the Database and Report System with Foundstone Database and Report Server installed

1.3.1 Brief Description of the Components of the TOE

The TOE consists of the following software components:

1.3.1.1 Enterprise Manager Component

The Enterprise Manager provides authorized users with access to the TOE through their Web browsers. It allows them to manage and run the TOE from anywhere on the network. Access is protected by user identification and authentication.

1.3.1.2 Scan Engine Component

One or more Scan Engines scan the network environment. Depending on the logistics and size of your network, you may need more than one Scan Engine to scan the network. The Scan Engine performs identification, interrogation, and vulnerability assessment of remote computer systems.

1.3.1.3 Scan Controller Component

The Scan Controller provides the communication between the scan engine and the database. Large or segmented networks (WANs[1]) may require more than one scan controller to be deployed.

1.3.1.4 API Service

The API service provides an interface for Enterprise Manager to store data into and retrieve data from the Foundstone Database. This interaction uses SOAP[2] over SSL[3].

1.3.1.5 Data synchronization service

The Data Synchronization Service enables Vulnerability Manager to import asset information from McAfee's ePO enterprise management system or an LDAP directory such as Microsoft Active Directory. This integration permits Vulnerability Manager to learn about assets through a mechanism other than discovery scans.

1.3.1.6 Foundstone Database

The Foundstone Database is the data repository for the Vulnerability Manager system. It uses Microsoft SQL Server to store everything from scan settings and results to user accounts and Scan Engine settings. It contains all of the information needed to track organizations and workgroups, manage users and groups, run scans, and generate reports.

[1] Wide Area Networks
[2] Simple Object Access Protocol
[3] Secure Sockets Layer

1.3.1.7 Report Server

The Report Server is responsible for generating reports requested by authorized users. It retrieves scan results from the Foundstone Database, prepares the report, and saves it for future review.

1.3.1.8 Web Application Scanner

The Web Application Scanner provides a scan configuration, vulnerability checks, and scan reports for web applications. The web application scanner module is a licensed item which can be purchased and added on to a Vulnerability Manager v7.5.4 deployment at any time. Any scan engine is capable of web application scanning once the module has been purchased with no additional software required.

1.3.2 TOE Environment

The TOE is an Intrusion Detection System (IDS) /Intrusion Prevention System (IPS) which consists of a set of software applications. The hardware, operating systems and all third party support software (e.g., DBMS[4]) on the systems on which the TOE executes are excluded from the TOE boundary.

The platform on which the Enterprise Manager software is installed must be dedicated to functioning as the Enterprise Manager. The TOE requires the following hardware and software configuration on this platform:

Table 2 - Enterprise Manager Component Requirements

Component	Requirement
Processor	Dual Xeon 2Ghz[5], Dual Core Xeon 2.33Ghz, or better
Memory	4 GB[6] RAM
Disk Space	80GB Partition
Supported Operating Systems	Windows Server 2003 SP2 or later Windows Server 2008 R2 Current security updates
Additional Software	Internet Information Services (IIS) 7.5 Current IIS security patches World Wide Web Publishing must be running

The Scan Engine, Scan Controller, API Service, and Data Sync Service are all installed on the same platform. The TOE requires the following hardware and software configuration on this platform:

Table 3 – Primary Scan Engine Component Requirements

Component	Requirement
Processor	Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better
Memory	4 GB RAM
Disk Space	80GB Partition
Supported Operating Systems	Windows Server 2003 SP2 or later Windows Server 2008 R2 Current security updates
Additional Software	MDAC 2.8 SQL Client Tools Microsoft Windows Script 5.6

[4] Database Management System
[5] Gigahertz
[6] Gigabyte

The platform on which the Foundstone Database and Report Server are installed must be dedicated to functioning as the servers for these functions of the TOE. The DBMS is installed on this same platform. The TOE requires the following hardware and software configuration on this platform.

Table 4 – Foundstone Database/Report Server Component Requirements

Component	Requirement
Processor	Dual Xeon 2Ghz, Dual Core Xeon 2.33Ghz, or better
Memory	4 GB RAM
Disk Space	160GB Partition
Supported Operating Systems	Windows Server 2003 SP2 or later Windows Server 2008 R2 Current security updates
Supported Database Management Systems	Microsoft SQL Server 2005 SP2 or later Microsoft SQL Server 2008 SP1 or later Microsoft SQL Express 2008 SP1 or later All SQL hotfixes/patches
SQL Server Memory Settings	900MB

Authorized users can access the Enterprise Manager through their Web browser software. The TOE supports Microsoft Internet Explorer 8.0 and higher, running on a Windows operating system. Latest service packs should be applied to both the web browser and operating system. Recommended minimum screen resolution is 1024 x 768.

1.4 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.4.1 Physical Scope

As stated in section 1.3, the TOE is composed of modular components and thus numerous deployment scenarios are possible. The TOE is evaluated in a distributed server architecture. This architecture is appropriate for complex organizations where large disparate networks in multiple geographical regions may require multiple scan engines. The scan engines generate all scanning traffic on their local network segments and then send the resulting scan data to the Foundstone Database. During the installation of each component, custom certificates are installed for use with the SSL protocol that protects traffic between the components.

For the purpose of CC testing, the following deployment configuration is used:

- One (1) instance of Enterprise Manager on a dedicated platform
- One (1) instance of Scan Engine, Web Application Scanner , Scan Controller, API Service, and Data Sync Service on a dedicated platform (Primary Scan Engine)
- Zero or more instances of Scan Engine on additional dedicated platforms (Secondary Scan Engines).
- One instance (1) of the Foundstone Database and Report Server hosted on a separate dedicated platform (together with the DBMS)

The following configuration option is required in the evaluated configuration:

- Root Organization Administrators are not permitted to switch to Global Administrator access (the user must log out and log back in as a Global Administrator)

The following items are excluded from the evaluation:

- Remediation management and tickets – this is optional functionality that previously required the purchase of a separate license. It is not evaluated in the evaluated configuration as the functions are not needed for the core functionality of the TOE.
- Notification service - this is optional functionality that previously required the purchase of a separate license. This functionality is not evaluated in the evaluated configuration.

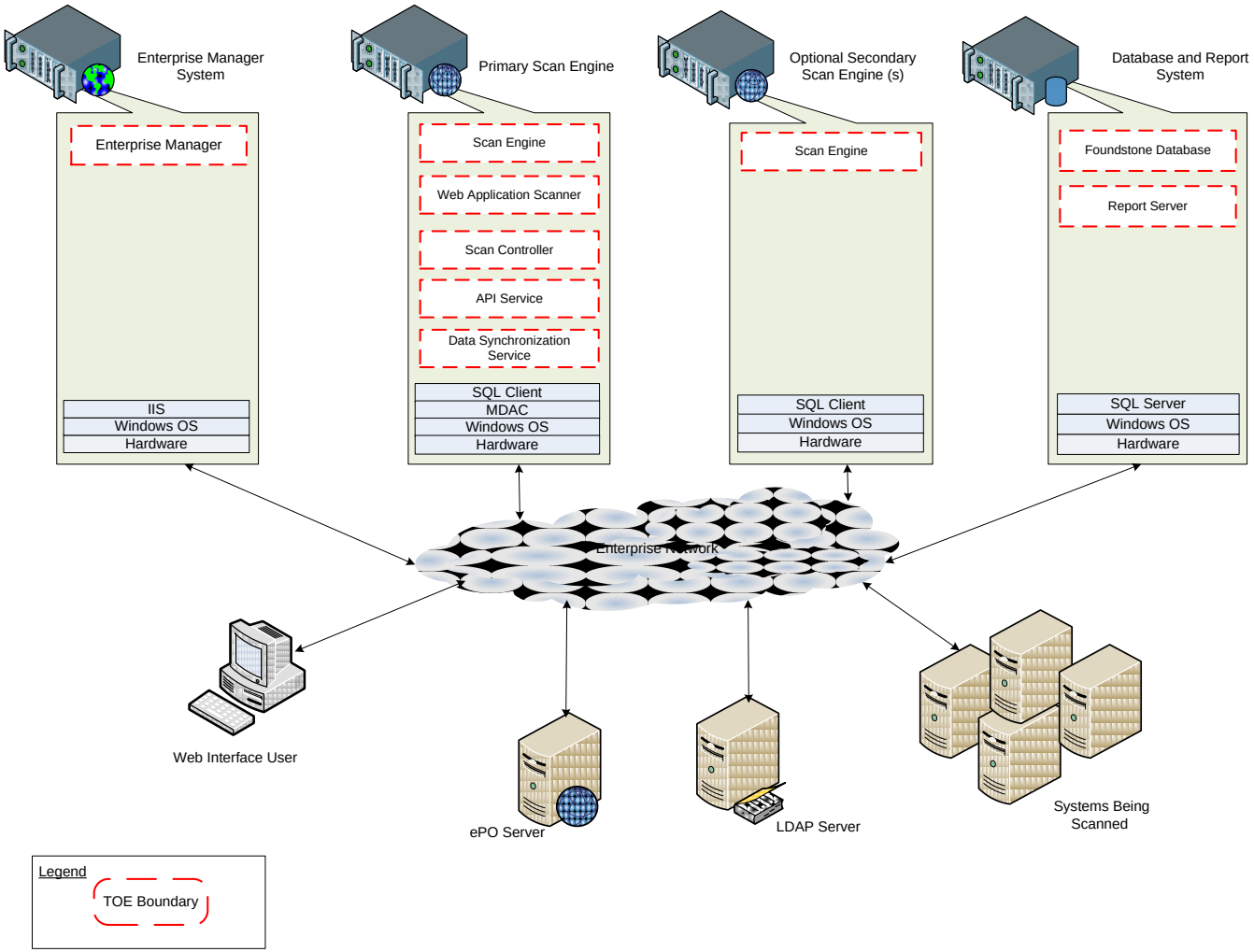

Figure 2 - Physical TOE Boundary

1.4.1.1 Guidance Documentation

The following guides are required reading and part of the TOE:

- McAfee Vulnerability Manager 7.0 Best Practices Guide
- McAfee Vulnerability Manager 7.5 Install Guide
- McAfee Vulnerability Manager 7.5 Product Guide
- McAfee Vulnerability Manager 7.5.1 Release Notes
- McAfee Vulnerability Manager 7.5.4 Release Notes
- McAfee Vulnerability Manager 7.0 Technote System Requirements

The McAfee Vulnerability Manager 7.0 Best Practices Guide and the McAfee Vulnerability Manager 7.0 Technote System Requirements have not been updated to v7.5 or v7.5.4. However, the guidance they provide for managing the TOE remain valid for v7.5.

1.4.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Identification and Authentication
- Security Management
- Asset Data Import
- Scanning

1.4.2.1 Security Audit

The TOE's Audit Security Function provides auditing of management actions performed by administrators. The audit records generated by the TOE are categorized by the following event types: Administrator actions, User actions, and System actions. Audit records include the date and time of the event, the type of the event, the subject identity, and a description of event.

1.4.2.2 Identification and Authentication

The TOE requires users to identify and authenticate themselves before accessing the TOE software or before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with his user account that defines the functionality the user is allowed to perform. When interacting with the TOE via the Enterprise Manager GUI[7], identification and authentication is performed by the TOE. Identification and authentication for local login to the operating system (i.e., via a local console) is performed by Windows (IT Environment).

1.4.2.3 Security Management

The TOE's Management Security Function provides administrator support functionality that enables a human user to configure and manage TOE components.

[7] Graphical User Interface

Management of the TOE may be performed via the Enterprise Manager. All user types may use the Enterprise Manager. The TOE provides the following management functions:

1. User management,
2. Root organization management,
3. Workgroup management,
4. Scan Engine management,
5. Asset management,
6. Scan management,
7. Report management,
8. Known vulnerability management.

1.4.2.4 Asset Data Import

The TOE may be configured to import data about assets from LDAP servers or McAfee ePO. The value of this functionality is that the information about the assets may be more accurate or complete than the information obtained from scans.

1.4.2.5 TSF Data

TOE data consists of both TSF data and user data (information). TSF data consists of authentication data, security attributes, and other generic configuration information. Security attributes enable the TOE to enforce the security policy. Authentication data enables the TOE to identify and authenticate users.
Table 5 below contains the following TOE Data

Table 5 -TOE Data

TSF Data	Description	AD	UA	GE
Asset groups	Grouping of assets for ease of configuring parameters and association with scans.			✓
Assets	Systems that have been discovered by the TOE during scans.			✓
Data Sources	LDAP and/or ePolicy Orchestrator servers from which asset information may be imported. Configuration of data sources is an installation activity only; synchronization updates occur during TOE operation.			✓
Scan Engines configuration	Parameters associated with each Scan Engine, such as which root organization it will perform scans for			✓
Reports	Reports are launched to generate information regarding the results of a specific scan and may be viewed once generated			✓
Report Templates	Report templates define the information that will be included in reports as well as the frequency at which the reports are generated.			✓
Root Organizations	The top level organization of items within the TOE. All items associated with one root organization are shielded from all other root organizations			✓

TSF Data	Description	AD	UA	GE
Scans	Parameters that define the scanning actions to be performed by the TOE and permissions relevant to each scan granted to Foundstone Users			✓
User Accounts	Root Organization, Username and password for each individual user that connects to the TOE via the Enterprise Manager web interface.	✓		
User groups	Grouping of users for ease of configuring parameters and association with workgroups.		✓	
User roles	The administrator type for each individual user that connects to the TOE via the Enterprise Manager web interface.		✓	
Known Vulnerabilities	List of known vulnerabilities that can be associated with individual scans.			✓
Workgroups	One or more levels of hierarchy under root organizations that permit access restrictions to be defined for scans and reports.			✓

Note: AD=Authentication data; UA=User attribute; GE=Generic Information

1.4.2.5.1 Scanning

The TOE scans designated systems to detect known vulnerabilities on those systems. Results of the scans are stored in the database (the DBMS is in the IT Environment), and reports based upon completed scans may be retrieved via the GUI interface of the Enterprise Manager.

1.4.3 Product Physical/Logical Features and Functionality not included in the TOE

Most features and functionality of the Vulnerability Manager v7.5.4 are part of the evaluated configuration of the TOE. The only exceptions are the following:

- Configuration Manager – this functionality is used for infrastructure management, not for everyday vulnerability management.
- McAfee Product Integration – Allows for McAfee Asset Manager integration to allow Vulnerability Manager to import asset information from Asset Manager. McAfee Asset Manager is outside the scope of the TOE boundary.
- RealTime Scanning – RealTime Scanning requires integration with McAfee Asset Manager which is outside the scope of the TOE boundary.
- Telnet only option for Shell credentials – administration is not to be restricted to the Telnet only option. Secure remote authentication methods are required.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 6 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the Common Evaluation Methodology (CEM) as of TBD were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.2)

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[8] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[9] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 7 - Threats

Name	Description
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.

[8] IT – Information Technology
[9] TSF – TOE Security Functionality

Name	Description
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of data received from all data sources.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.
T.FALACT	Issues resulting from scans of monitored systems may fail to be acted upon because the information is not disseminated from the TOE to other IT systems that are responsible for tracking or correcting the issues.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. The following OSPs are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration:

Table 8 - Organizational Security Policies

Name	Description
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events, that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets, must be collected.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to data received from data sources and appropriate response actions taken.
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.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.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 9 - Assumptions

Name	Description
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
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.ALARM	The DBMS will generate an alarm if storage space in the database is exhausted.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 10 - Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDIT	The TOE must record audit records for data accesses and use of the System functions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDANLZ	The TOE must apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.IDSCAN	The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
O.IMPORT	The TOE shall provide mechanisms to import data about assets from LDAP servers and ePO.
O.INTEGR	The TOE must ensure the integrity of all system data.
O.OFLOWS	The TOE must appropriately handle potential system data storage overflows.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.SCAP	The TOE shall provide mechanisms to exchange SCAP Benchmark Assessment data.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 11 - IT Security Objectives

Name	Description
OE.ALARM	The DBMS will generate an alarm if storage space in the database is exhausted.
OE.AUDIT_PROTECT	The IT Environment will provide the capability to protect audit information generated by the TOE.
OE.AUDIT_REVIEW	The IT environment will provide the capability to review audit information generated by the TOE.
OE.CRYPTO	The IT Environment will provide the cryptographic functionality and protocols required for the implementation of secure channels between the TOE components and between the TOE and external IT systems.
OE.IDAUTH	The IT Environment must be able to identify and authenticate users prior to the TOE allowing access to TOE functions and data on the Scan Engine.
OE.INTROP	The TOE is interoperable with the IT System it monitors
OE.PROTECT	The IT Environment will protect itself and the TOE from external interference or tampering.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 12 - Non-IT Security Objectives

Name	Description
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.DATABASE	Those responsible for the TOE must ensure that access to the database, via mechanisms outside the TOE boundary (e.g., DBMS), is restricted to authorized users only.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is

Name	Description
	delivered, installed, managed, and operated 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.
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.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 13 identifies all extended SFRs implemented by the TOE

Table 13 - Extended TOE Security Functional Requirements

Name	Description
EXT_IDS_SDC.1	System Data Collection
EXT_IDS_ANL.1	Analyser analysis
EXT_IDS_RDR.1	Restricted Data Review
EXT_IDS_STG.2	Prevention of System data loss

5.1.1 Class IDS: Intrusion detection function

Intrusion Detection functions involve collecting information from designated systems and analyzing the information for vulnerabilities and compliance. The extended family "EXT_IDS: Intrusion detection function" class was modeled after the CC FAU: Security audit class. The extended family and related components for EXT_IDS_SDC: System data collection was modeled after the CC family and related components for FAU_GEN: Security audit generation. The extended family EXT_IDS_ANL: Analyser analysis was modeled after the family CC family and related components for FAU_SAA: Security audit analysis. The extended family EXT_IDS_RDR: Restrictive Data Review was modeled after the CC family and related components for FAU_SAR: Security audit review. The extended family and related components for EXT_IDS_STG: Prevention of System data loss was modeled after the CC family and related components for FAU_STG: Security audit event storage.

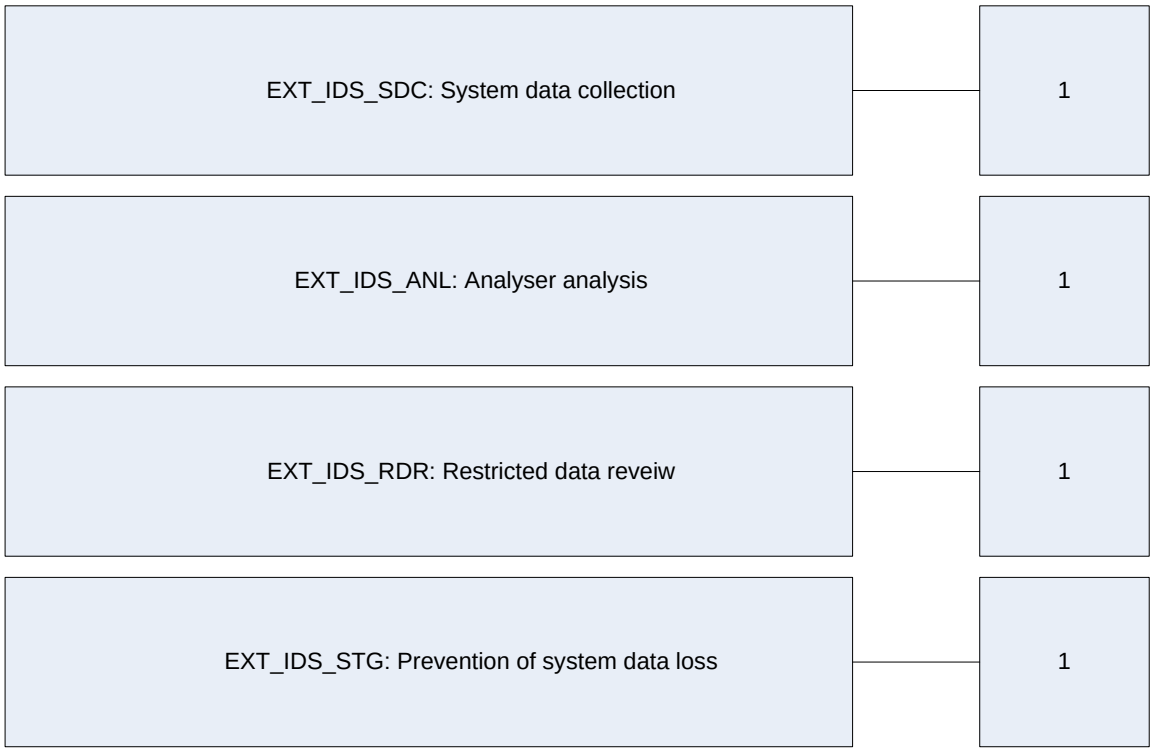

Figure 3 - EXT_IDS: Intrusion Detection Function Class Decomposition

System data collection (EXT_IDS_SDC)

Family Behaviour

This family defines the requirements for recording the information from the targeted IT system resources that take place under TSF control. This family identifies the level of system data collection, enumerates the types of events that shall be collected by the TSF, and identifies the minimum set of IDS-related information that should be provided within various IDS record types.

Component Leveling

Figure 4 – System data collection family decomposition

EXT_IDS_SDC.1 System data collection, defines the level of events, and specifies the list of data that shall be recorded in each record.

Management: EXT_IDS_SDC.1

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

a) Configuration of the events to be collected.

Audit: EXT_IDS_SDC.1

b) There are no auditable events foreseen

EXT_IDS_SDC.1 System data collection
Hierarchical to: No other components
EXT_IDS_SDC.1.1

The System shall be able to collect the following information from the targeted IT System resource(s):

a) [selection: *Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, detected known vulnerabilities*]; and

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

EXT_IDS_SDC.1.2

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

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

b) The additional information specified in the *Details* column of the **table below**.

Table 14 – System data collection Events and Details

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	none
IDS_SDC.1	Identification and authentication events	User identity, location, source address, destination address

Component	Event	Details
IDS_SDC.1	Data accesses	Object IDs, requested access, source address, destination address
IDS_SDC.1	Service Requests	Specific service, source address, destination address
IDS_SDC.1	Network traffic	Protocol, source address, destination address
IDS_SDC.1	Security configuration changes	Source address, destination address
IDS_SDC.1	Data introduction	Object IDs, location of object, source address, destination address
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
IDS_SDC.1	Authentication configuration	Account policy parameters
IDS_SDC.1	Accountability policy configuration	Accountability policy configuration parameters
IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Dependencies: **FPT_STM.1 Reliable time stamps**

5.1.1.1 Analyser analysis (EXT_IDS_ANL)

Family Behaviour

This family defines the analysis the TOE performs on the collected system data. This family enumerates the types of program code that shall be collected by the TSF, and identifies what type of control will be enforced on the executable code. This family also determines which changes are to be prevented, and which are to be monitored and reported.

Component Leveling

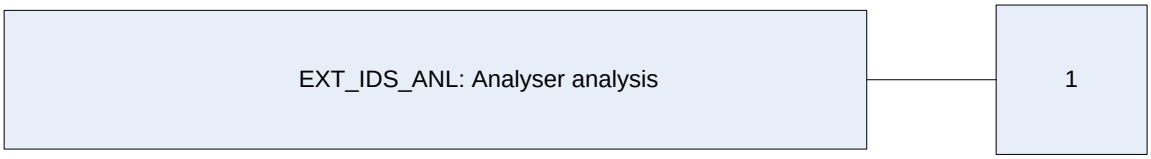

Figure 5 – Analyser analysis family decomposition

EXT_IDS_ANL.1 Analyser analysis, specifies the list of analyses the TOE will perform on the collected system data.

Management: EXT_CCS_ANL.1

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

a) Configuration of the analysis to be performed.

Audit: EXT_CCS_ANL.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Minimal: Enabling and disabling of any of the analysis mechanisms.

EXT_IDS_ANL.1 Analyser analysis
Hierarchical to: No other components
EXT_IDS_ANL.1.1

The System shall perform the following analysis function(s) on all system data received:

a) [selection: *statistical, signature, integrity*]; and

b) [assignment: *other analytical functions*].

EXT_IDS_ANL.1.2

The System shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) [assignment: *other security relevant information about the result*].

Dependencies: EXT_IDS_SDC.1 System Data Collection
FPT_STM.1 Reliable Timestamps

5.1.1.2 Restricted data review (EXT_IDS_RDR)

Family Behaviour

This family defines the requirements for system data tools that should be available to authorized users to assist in the review of system data.

Component Leveling

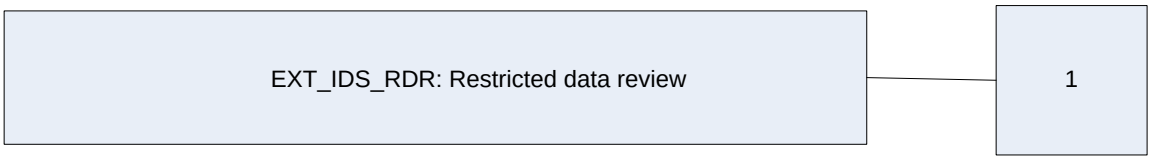

Figure 6 – Restricted data review family decomposition

EXT_IDS_RDR.1 Restricted data review, the TSF shall prohibit all users read access to the audit records, except for those user that have been granted explicit read-access.

Management: EXT_IDS_RDR.1

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

a) maintenance (deletion, modification, addition) of the group of users with read access right to the system data records.

Audit: EXT_IDS_RDR.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Basic: Attempts to read system data that are denied.

b) Detailed: Reading of information from the system data records.

Application Note: The audit event definition is consistent with CCEVS Policy Letter #15, which states that only access failures are auditable at the Basic level of audit.

EXT_IDS_RDR.1 Restricted data review
Hierarchical to: No other components
EXT_IDS_RDR.1.1
The System shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of System data*] from the System data.
EXT_IDS_RDR.1.2
The System shall provide the System data in a manner suitable for the user to interpret the information.
EXT_IDS_RDR.1.3
The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.
Dependencies: EXT_IDS_SDC.1

5.1.1.3 Prevention of System data loss (EXT_IDS_STG)

Family Behaviour

This family defines the requirements for system data tools that should be available to authorized users to assist in the review of system data.

Component Leveling

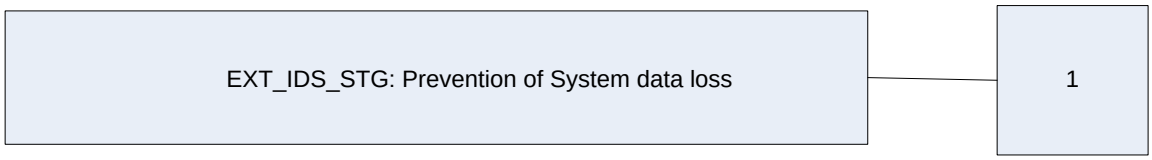

Figure 7 – Prevention of System data loss family decomposition

EXT_IDS_STG.2 Prevention of System data loss, the TSF shall define what actions the System will take if storage capacity has been reached.

Management: EXT_IDS_STG.2

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

b) maintenance (deletion, modification, addition) of actions to be taken in the event that system data storage capacity has been reached.

Audit: EXT_IDS_STG.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

a) Basic: Actions taken if the storage capacity has been reached.

EXT_IDS_STG.2 Prevention of System data loss
Hierarchical to: No other components
EXT_IDS_STG.2

The System shall [selection: ignore System data, prevent System data, except those taken by the authorized user with special rights, overwrite the oldest stored System data] if the storage capacity has been reached.

Dependencies: EXT_IDS_SDC.1 System Data Collection

5.2 Extended TOE Security Assurance Components

There are no extended TOE Security Assurance Components.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 15 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 15 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FIA_ATD.1	User attribute definition		✓		
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.1	Timing of authentication		✓		
FIA_UID.1	Timing of identification		✓		
FMT_MOF.1	Management of security functions behavoir	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓	✓	
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_TDC.1(a)	Inter-TSF Basic TSF Data Consistency		✓		✓
FPT_TDC.1(b)	Inter-TSF Basic TSF Data Consistency		✓		✓
EXT_IDS_SDC.1	System data collection		✓		

Name	Description	S	A	R	I
EXT_IDS_ANL.1	Analyzer analysis	✓	✓		
EXT_IDS_RDR.1	Restricted data review		✓		
EXT_IDS_STG.2	Prevention of system data loss	✓	✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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) [*Access to the System and access to the TOE and System data*].

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, 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 information detailed in Table 16 below*].

Table 16 – Auditable Events

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
	Access to the TOE and System data	Object IDs, Requested access
FIA_UAU.1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions.	User identity, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FPT_TDC.1	Successful use of TSF data consistency mechanisms	Data Source
EXT_IDS_ANL.1	None (the analysis function is always enabled)	
EXT_IDS_RDR.1	None (the user is not given the option of accessing unauthorized system data)	
EXT_IDS_STG.2	None (a common database is used for system data and audits; if the database is full, all new information is discarded)	

Dependencies: FPT_STM.1 Reliable time stamps

6.2.2 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
FIA_ATD.1.1
The TSF shall maintain the following list of security attributes belonging to individual users:
[
a) Login name;
b) Password;
c) User role;
d) Lock status;
e) Organization;
f) Workgroup membership;
g) Group membership and
h) Scan permissions.
].
Dependencies: No dependencies

FIA_SOS.1 Verification of secrets
Hierarchical to: No other components.
FIA_SOS.1.1
The TSF shall provide a mechanism to verify that secrets meet [*the following metrics:*

a) Contains at least 8 characters
b) Contains at least one number
c) Contains at least one non-alpha-numeric character (`~!@#$%^&*()-_=+).

].
Dependencies: No dependencies

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.
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.
Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification
Hierarchical to: No other components.
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.
Dependencies: No dependencies

6.2.3 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1

The TSF shall restrict the ability to [modify the behaviour of] the functions [*of functions System data collection and analysis*] to [*Foundstone Users with permissions for specific scans, Global Administrators, Root Organization Administrators and Workgroup Administrators*].

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1

The TSF shall restrict the ability to [query] [*and add System data*], and ~~the [assignment: *list of TSF data*]~~ **shall restrict the ability to query and modify all other TOE data to** [*the roles associated with specific data and operations as show in Table 17]*

Table 17 – TSF Data Access Permissions

TSF Data	Global Administrator	Root Organization Administrator*	Workgroup Administrator**	Foundstone User
Asset groups	None	Create, Delete, Modify	Create, Delete, Modify	None
Assets	None	Modify	Modify	None
Data Sources	None	Performed during installation only	None	None
Known Vulnerabilities	Create, Delete, Modify	None	None	None
Scan Engines	Modify	Modify	None	None
Reports	None	Submit or Cancel	Report access is determined by the access permission in Table 18	Report access is determined by the access permission in Table 18
Report Templates	None	View and Edit	Report access is determined by the access permission in Table 18	Report access is determined by the access permission in Table 18
Root Organizations	Create, Delete, Modify	Modify	None	None
Scans	View	Create, Delete, Modify, Launch	Create, Delete, Modify, Launch	Scan access is determined by the access permission in Table 18

TSF Data	Global Administrator	Root Organization Administrator*	Workgroup Administrator**	Foundstone User
User Accounts	Create, Delete, Modify	Create, Delete, Modify	Create, Delete, Modify	Modify the user's own password
User Groups	Create, Delete, Modify	Create, Delete, Modify	Create, Delete, Modify	None
User Roles	Create, Delete, Modify	Create, Delete, Modify	Create, Delete, Modify	None
Workgroups	Create, Delete, Modify	Create, Delete, Modify	Create, Delete, Modify	None

**Root Organization Administrators can only have access to the TSF Data within the same root organization*
*** Workgroup Administrators only have access to TSF Data within the workgroups*

Table 18 – Scan and Report Access Permissions

Permissions	Description
View	View the reports, templates and other information displayed in the Enterprise Manager for the selected scan. Reports may be submitted and canceled for any reports for which the user has View access.
Edit IP	Allow the user or group to edit the IP ranges for the selected scan.
Edit Body	Allow the user or group to edit the selected scan's settings, other than the IP ranges and schedule.
Schedule	Allow the user or group to change the times when the selected scan is scheduled to run.
Delete	Allow the user or group to delete the selected scan.
Full	All of the above. Allows the user or group to edit, launch, or delete any scan in the organization or workgroup.

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:
[
1) User management,
2) Root organization management,
3) Workgroup management,
4) Asset management,
5) Scan management,
6) Report management
7) Scan engine management
8) Known vulnerability management
].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*Foundstone User, Root Organization Administrator, Workgroup Administrator, and Global Administrator*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.4 Class FPT: Protection of the TSF

FPT_TDC.1(a) Inter-TSF basic TSF data consistency
Hierarchical to: No other components.
FPT_TDC.1.1a
The TSF shall provide the capability to consistently interpret [*assets*] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2a
The TSF shall use [*the following rules*] when interpreting the TSF data from another trusted IT product:
1) *For LDAP servers, the data is interpreted according to the LDAP version 3 protocol.*
2) *For EPO, the data is interpreted according to McAfee's schema for the ePO database.*
3) *When conflicting information is received from different sources, highest priority is given to ePO data, then to LDAP server data.*

Dependencies: No dependencies

FPT_TDC.1(b) Inter-TSF basic TSF data consistency
Hierarchical to: No other components.
FPT_TDC.1.1b
The TSF shall provide the capability to consistently interpret [*known vulnerabilities*] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2b
The TSF shall use [*the SCAP Benchmark Assessment XCCDF and OVAL standards*] when interpreting the TSF data from another trusted IT product.
Dependencies: No dependencies

6.2.5 Class IDS: Intrusion Detection Functions

EXT_IDS_SDC.1 System data collection
Hierarchical to: No other components
EXT_IDS_SDC.1.1
The System shall be able to collect the following information from the targeted IT System resource(s):

a) access control configuration, service configuration, authentication configuration, detected known vulnerabilities and
b) no other events.

EXT_IDS_SDC.1.2
At a minimum, the System shall collect and record the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) The additional information specified in the *Details* column of **the table below**.

Table 19 – System Data Collection Events and Details

Component	Event	Details
EXT_IDS_SDC.1	Access control configuration	Location, access settings
EXT_IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols
EXT_IDS_SDC.1	Authentication configuration	Account policy parameters
EXT_IDS_SDC.1	Detected known vulnerabilities	Identification of the known vulnerability

Application Note: Access control configuration refers to configuration settings used to restrict access for individual users/roles. Service configuration refers to services made available to users via the network interface and protocol stack. Authentication configuration refers to settings regarding password content parameters and authentication attempts.

Dependencies: FPT_STM.1 Reliable time stamps

EXT_IDS_ANL.1 Analyser analysis
Hierarchical to: No other components
EXT_IDS_ANL.1.1
The System shall perform the following analysis function(s) on all system data received:

a) [signature]; and

b) [*the following analytic functions: operating system identification, registry queries (when credentials are provided), and positive and negative responses to packets transmitted to the scanned systems*].

EXT_IDS_ANL.1.2
The System shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) [*Criticality of the asset on which the vulnerability was detected*].

c) [*Risk factor of the detected vulnerability*]

Dependencies: EXT_IDS_SDC.1 System Data Collection
FPT_STM.1 Reliable Timestamps

EXT_IDS_RDR.1 Restricted IDS data review
Hierarchical to: No other components
EXT_IDS_RDR.1.1
The System shall provide [*Foundstone User, Root Organization Administrator, and Workgroup Administrator*] with the capability to read [*the system data listed in Table 20 below*] from the System data.

Table 20 – System Data Access

User Type	Access
Foundstone User	System data associated with specific scans they are authorized to view.
Workgroup Administrator	System data associated with all workgroups the Workgroup Administrator is associated with.
Root Organization Administrator	System data associated with all scans in the same root organization

EXT_IDS_RDR.1.2
The System shall provide the System data in a manner suitable for the user to interpret the information.
EXT_IDS_RDR.1.3
The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access.

Dependencies: EXT_IDS_SDC.1 System data collection

EXT_IDS_STG.2 Prevention of System data loss
Hierarchical to: No other components
EXT_IDS_STG.2.1
The System shall [ignore System data] if the storage capacity has been reached.
Dependencies: EXT_IDS_SDC.1 System Data Collection

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 21 - Assurance Requirements summarizes the requirements.

Table 21 - Assurance Requirements

Assurance Requirements	
Class 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
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class 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
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 22 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of identification
Security Management	FMT_MOF.1	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_TDC.1(b)	Inter-TSF Basic TSF Data Consistency
Asset Data Import	FPT_TDC.1(a)	Inter-TSF Basic TSF Data Consistency
Scanning	EXT_IDS_SDC.1	System data collection
	EXT_IDS_ANL.1	Analyzer analysis
	EXT_IDS_RDR.1	Restricted data review
	EXT_IDS_STG.2	Prevention of system data loss

7.1.1 Security Audit

The TOE's Audit Security Function provides auditing of management actions performed by administrators. The audit records generated by the TOE include the items listed in Table 16 of this ST and are categorized by the following event types:

- Administrator actions – those that are specific to authorized administrator activities (i.e. add-remove- change user attributes and system attributes.)
- User actions – User actions are those that are specific to user activities (i.e. logon and logoff.)

- System actions – System actions are specific to the TOE performing system operations (i.e. running queries, requesting or setting scan configurations, request scan status, verifying license information, verifying access rights.)

The following information is provided for an audit record generated by the TOE:

- Date and Time of the event
- Type (i.e. category and action) of the event
- Subject (i.e. user and IP address) identity
- Description (i.e. action performed, success or failure, etc.) of event

Audit records are stored in the database. Administrators are advised to configure the database to expand to the limits of the file system. In the unlikely event storage space exhaustion does occur, the TOE discards the most recent results. The database in the IT environment may optionally be configured to send alert notifications to administrators when capacity limits are reached so corrective actions may be taken.

TOE Security Functional Requirements Satisfied: FAU_GEN.1

7.1.2 Identification and Authentication

The TOE enables an authorised user to manage the TOE via a web interface on the Enterprise Manager. The TOE requires users to identify and authenticate themselves before accessing the TOE software or before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication.

Each user of the web interface has a root organization, user identity, user password and role associated with their user account. The role defines the functionality the user is allowed to perform. If the role is Workgroup Administrator or Foundstone User, the user also has associations with workgroups within the root organization.

Authentication is required (cannot be bypassed) and the password is configured when the user account is created. The TOE implements restrictions on the passwords:

- Contains at least 8 characters
- Contains at least one number
- Contains at least one non-alpha-numeric character (`~!@#$%^&*()-_=+)

TOE Security Functional Requirements Satisfied: FIA_UAU.1, FIA_ATD.1, FIA_SOS.1

7.1.3 Security Management

The TOE's Management Security Function provides administrator support functionality that enables a human user to configure and manage TOE components.

Management of the TOE may be performed via the Enterprise Manager. All user types may use the Enterprise Manager.

The TOE provides the following management functions:

1. User management,

2. Root organization management,
3. Workgroup management,
4. Scan Engine management,
5. Asset management,
6. Scan management,
7. Report management,
8. Known vulnerability management.

7.1.3.1 User Management

Each User Account must be defined to the TOE. In addition to a login name and password, a user includes the following security attributes: user role, lock status (whether the account is administratively enabled), organization, workgroup membership, group membership and scan permissions. A role may be any of the following: Global Administrator, Root Organization Administrator, Workgroup Administrators, or Foundstone User. User Accounts may be associated with one or more groups, which may be used to assign permissions to all members of a group rather than individual users. The purpose of each role is described in table 20 below:

Table 23 – Role Descriptions

Role	Description
Global Administrator	The Global Administrator sets up the top-level organization(s), and creates an administrator for the organization(s). The Global Administrator can also set up workgroups under an organization, and can create users and user groups. The Global Administrator can also move top-level organizations to become workgroups under other organizations.
Root Organization Administrator	The Root Organization Administrator can manage assets, scan configurations, user accounts, and scan engines. These administrators also have full access to any workgroups created under their organization. The Root Organization Administrator manages the Scan Engine settings from the Enterprise Manager.
Workgroup Administrators	The Workgroup Administrator can manage assets, scan configurations, and user accounts. These administrators also have full access to any workgroups created under their workgroup.
Foundstone User	Each Foundstone User is granted access to scans. Users are associated with an organization and may be granted access to any or all workgroups within that organization, and any or all scans defined for that organization. Scan access is configurable per scan.

Administrative capabilities for each role are described in Table 17 of this ST.

Foundstone Users may be associated with one or more groups within a root organization, or with a root organization as a whole. Scan access for Foundstone Users may be any of the following permissions described in Table 18 of this ST.

7.1.3.2 Root Organization Management

Root organizations are configured by the Global Administrator. The IP addresses and scan engines available to the root organization are part of this configuration. When a root organization is created, a single Root Organization Administrator must also be defined.

Root Organization Administrators may configure users, groups and scans within their root organization. Root Organization Administrators, Workgroup Administrators and Foundstone Users may only belong to a single root organization.

7.1.3.3 Workgroup Management

Workgroups are configured by the Root Organization Administrators. The IP addresses and scan engines available to the workgroup are part of this configuration and must be a subset of the IP addresses and scan engines configured for the root organization. When any workgroup is created, an administrator group is automatically created for that workgroup. Users are designated as Workgroup Administrators by associating the user account with the appropriate administrator group(s).

Workgroup Administrators may configure users, groups and scans within their workgroups.

7.1.3.4 Scan Engine Management

After a scan engine has been added to an organization, the following scan engine setting can be managed by a Global Administrator or Root Organization Administrator associated with the same root organization:

- **Name** – Provides the ability to type a descriptive name for the scan engine. The name and description are stored in the engine registry.
- **Description** – The optional description can provide additional information about the location or purpose of this scan engine.
- **Type** – Displays the type of system on which the scan engine is running. If the product is running on a McAfee appliance, it appears here. If it is running on customer-supplied equipment, Custom appears.
- **Status** – Shows whether the scan controller is communicating with this scan engine. If the status is online, the scan controller is able to communicate with the scan engine. This status is updated every 30 seconds as the database polls each engine.
- **Action**
  - Update – Click Update to submit changes to the scan engine.
  - Delete – Removes this scan engine from the list. Engines that are online cannot be deleted from the list.
  - Pause engine/Resume engine – Pauses all scans on this scan engine (Global Administrator only).
  - Preferences – Edit the settings for this engine.
- **Refresh** – Refreshes the engine list to display the latest settings.

Network connectivity detection can also be configured to monitor the scan engine's connectivity to the network. If the network connectivity becomes unreliable, the scan engine will pause its scan until the connection is restored.

7.1.3.5 Asset Management

Assets are systems or URLs being scanned by the TOE. Assets are automatically created as scans are performed. A Root Organization Administrator or Workgroup Administrator may associate a Criticality with individual assets. The defined Criticality values are None, Low, Limited, Moderate, Significant and Extensive. Vulnerabilities found on hosts marked with a lower criticality count less than vulnerabilities found on hosts with a high criticality level.

A Root Organization Administrator or Workgroup Administrator can combine multiple assets into groups, organizing them into hierarchies. This makes it easier to manage assets, add groups of assets to scans, and monitor risk. Any number of groups and sublevels of groups may be created. A Criticality may be assigned to an entire asset group. An asset can belong to only one group at a time.

The Root Organization Administrator can delete any asset group. The Workgroup Administrator can delete asset groups if the group only contains assets belonging to the IP pool for that workgroup. If the asset group contains assets from other workgroups, only the assets belonging to that IP pool are removed and the asset group itself is not deleted.

7.1.3.6 Scan Management

Scans may be created by Root Organization Administrators and Workgroup Administrators. They may be modified by those same roles as well as Foundstone Users with appropriate permissions. The parameters that may be configured are:

1. IP addresses/assets to be included in the scan
2. ICMP, TCP and UDP protocol options for discovery scans
3. Credentials to be used during scans to help identify access configuration settings
4. Service discovery
5. Type of vulnerability scans to be performed. The list of known vulnerabilities may be updated so that scans are kept current as new vulnerabilities are identified. Updates are made to the TOE's vulnerability signature libraries by importing new data files, which does not require updating the version of the product.
6. Schedule a recurring scan
7. The scan engine and network interface to be used
8. Windows (time slots) during which the scan may execute

7.1.3.7 Report Management

Reports may be generated for any scan by users with View access to that scan. Reports are generated based upon Report Templates, which specify the format of the output, the frequency with which the report is generated, the assets to be addressed by the report, and the type of information to be included in the report. Many templates are supplied with Vulnerability Manager and additional templates may be created by users.

The assets specified by IP address and URLs in a report template are limited by the following restrictions:

Table 24 – Report Template IP Address and URL Restrictions

User Type	Asset by IP Address
Root Organization Administrator	All IP addresses and URLs in the organization's IP Pool
Workgroup Administrator	All IP addresses and URLs in the workgroup's IP Pool
Foundstone User with View access to a scan	All IP addresses and URLs included in the scan
Foundstone User with privilege to edit the IP addresses associated with a scan	All IP addresses and URLs within the workgroup to which the scan belongs. If the scan belongs to the organization, this user has access to all IP addresses within the organization.

Users may cause reports to be generated for any scan for which they have View access. Once a report is initiated, it is generated by the Report Service executing on the system with the Foundstone Database.

Reports in the process of being generated are displayed in a queue and may be canceled by any user with View access to the associated scan.

The three most recent reports associated with each scan are saved. Older reports are automatically deleted.

7.1.3.8 Known Vulnerability Management

Global Administrators may import (create) known vulnerabilities by importing XML files conforming to the SCAP Benchmark Assessment XCCDF and OVAL standards. After the information has been imported it is available for association with scans. Global Administrators may customize the Windows Policy settings, Registry Key permissions, File and Root File permissions, and Service settings in these vulnerability definitions.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FPT_TDC.1(b)

7.1.4 Asset Data Import

The TOE dynamically learns about assets when it conducts scans. The TOE may also be configured to import data about assets from external Data Sources, such as LDAP servers or ePO servers in the IT environment. Both LDAP and ePO databases contain detailed information about computer assets that may be of interest to administrators. This information may be imported from these Data Sources to be used by the TOE. The value of this functionality is that the information about the assets may be more accurate or complete than the information obtained from scans. Note that the integration of the TOE with ePO is for data import only; ePO does not provide any management functionality of the TOE.

Information may be learned about new or existing assets. If conflicting information is learned from different sources, the following precedence rules are applied (from highest to lowest):

1. Information obtained from ePO
2. Information obtained from LDAP servers
3. Information obtained from scans

The TOE must associate an IP address for each asset learned from a Data Source. This may be obtained from the IP Address attribute or by resolving the address from the NetBIOS Name and DNS Name attributes. Assets learned from a Data Source are automatically associated with a workgroup or organization based upon the asset's IP address and the IP address pool for the workgroups and organizations. If the asset's IP address does not correspond to any workgroup or organization, the asset is initially placed into the Unassigned Assets group. The information that can be imported for an asset is:

1. NetBIOS Name
2. DNS Name
3. IP Address
4. Domain/Workgroup Name
5. MAC[10] Address
6. Operating System Name (from ePO data sources only)
7. Operating System Version (from ePO data sources only)

This function is performed according to the frequency configuration of each configured Data Source.

TOE Security Functional Requirements Satisfied: FPT_TDC.1(a)

[10] Media Access Control

7.1.5 Scanning

The TOE performs scanning of designated systems to detect known vulnerabilities on those systems. In order to be able to delegate management of this process to appropriate levels, the TOE supports a hierarchical organization consisting of one or more root organizations and one or more levels of subordinate workgroups. Root organizations are hidden from each other; administrators and users can only view the scans and data that pertain to the organization to which they belong.

Associated with each root organization or workgroup are users, groups, scans, IP addresses, URLs, and scan engines. The IP addresses for subordinate levels (e.g., workgroups within root organizations) must be subsets of the IP addresses defined for the higher levels. The scan engines for subordinate levels must also be subsets of the scan engines defined for the higher levels.

Scans may be defined for root organizations or workgroups. A scan includes a list of IP addresses or URLs to be scanned, parameters concerning the types of network and service scanning to be performed, the time and frequency at which the scan should be executed, and the vulnerabilities to be scanned for. On a per-scan basis, credentials may be defined for logons to the scanned systems for more in-depth scanning. Scan timing may be either on-demand or scheduled to run at a later time. On-demand scans are intended to be run ad-hoc and are launched manually by the administrator when needed. Scheduled scans are intended to be run at specific a date and time in the future. Scheduled scans will run automatically based on the schedule set by the administrator.

The Web Application Scanner provides a scan configuration, vulnerability checks, and scan reports for web applications. Web application scans are used to crawl through web applications to identify high risk vulnerabilities contained within application code. Web vulnerabilities include:

- SQL Injection weaknesses – SQL injection occurs when user input is not sanitized on web forms. Since the forms provide the front-end interface to a back-end database, information can be unintentionally disclosed or tampered with by attackers, by entering escape characters and other methods accompanied with SQL syntax for executing code on the database server.
- Cross-site scripting (XSS) weaknesses – XSS attacks occur when a vulnerable application accepts unsolicited parameters without validating source, user, or session data. As a result, parameters can be passed via a malicious URL that tricks application users into executing code on a system they have been authorized to use.
- Buffer overflows – Occur when memory buffers are overrun, causing adjacent memory blocks to be overwritten, resulting in erratic behavior, memory errors, crashes, or a breach of system security.

Web application scanning can be configured to start on a set of entry paths and exclude a set of URLs and parameters to prevent harmful behavior from the scanner on critical assets. HTTP and HTTPS can be used as the protocol, and can be set to use alternate ports than the standard TCP 80 and 443.

As scans are performed, details such as operating system and network services within the designated address list are learned. As new systems and URLS are discovered during a scan, they are listed as assets. The assets may be associated with one or more scans for future scanning.

Scan results rely upon signature comparisons as well as other analytical functions. For example, when scanning for service configurations, results are determined from responses received as well as the absence of responses. In addition, the responses to multiple packets sent to the scanned systems are used to attempt operating system identification, which enables finer-grained scanning. If login credentials are provided for an asset, access control settings and authentication configuration settings available via remote login (i.e., registry settings) are analyzed.

Results of the scans are stored in the database. The information included with the results are the name of the scan, the time and date the scan was executed, the name of the asset scanned, the criticality of the asset,

vulnerabilities detected on each asset, and the risk factor associated with any detected vulnerabilities. Administrators are advised to purge old scan data from the database on a periodic basis and to configure the database to expand in size as necessary up to the limits of the file system. In the unlikely event storage space exhaustion does occur, the TOE discards the most recent results. Additionally, administrators may choose to configure an alert where the database (provided by the IT environment) sends out a notification for the storage space exhaustion.

Vulnerability Manager supports benchmark scans utilizing all six of the SCAP standards CVE, CPE, CCE, CVSS, XCCDF, and OVAL as well as direct import off SCAP data-feeds. Therefore, systems can be assessed using open community-developed security benchmarks and content, including FDCC benchmarks for Windows XP, Windows Vista, Internet Explorer 7, and more. Benchmark assessment inputs and outputs fully meet SCAP requirements, allowing the results to be used to monitor and audit compliance in accordance with regulatory mandates and other customer requirements.

Reports may be generated from the scan results and viewed according to the following restrictions:

Table 25 – Report Access

User Type	Access
Foundstone User	Reports for specific scans they are authorized to view
Workgroup Administrator	Reports for all scans associated with workgroups the administrator is associated with
Root Organization Administrator	Reports for all scans in the same root organization

TOE Security Functional Requirements Satisfied: EXT_IDS_SDC.1, EXT_IDS_ANL.1, EXT_IDS_RDR.1, EXT_IDS_STG.2

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 extended and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 3

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 26 - Threats:Objectives Mapping

Threats	Objectives	Rationale
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.	OE.PROTECT The IT Environment will protect itself and the TOE from external interference or tampering.	OE.PROTECT counters this threat by protecting the TOE in IT Environment from external interference or tampering..
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	O.ACCESS counters this threat by only permitting authorized users to access TOE data.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	O.IDAUTH counters this threat by ensuring that only authenticated users have access to TOE data.
	O.INTEGR The TOE must ensure the integrity of all system data.	O.INTEGR counters this threat by ensuring that no TOE data will be modified.
	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	O.PROTECT counters 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.	OE.PROTECT The IT Environment will protect itself and the TOE from external interference or tampering.	OE.PROTECT counters this threat by protecting the TOE in the IT environment from external interference or tampering..
T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	O.ACCESS counters this threat by only permitting authorized users to access TOE data.

Threats	Objectives	Rationale
a security mechanism.	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	O.IDAUTH counters this threat by ensuring that only authenticated users have access to TOE data.
	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	O.PROTECT counters 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.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	O.ACCESS counters this threat by only permitting authorized users to access TOE data.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	O.IDAUTH counters this threat by ensuring that only authenticated users have access to TOE data.
	O.INTEGR The TOE must ensure the integrity of all system data.	O.INTEGR counters this threat by ensuring that no TOE data will be deleted.
	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	O.PROTECT counters 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.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	O.ACCESS counters this threat by only permitting authorized users to access TOE data.
	O.IDANLZ The TOE must apply analytical processes and information to derive conclusions about intrusions (past, present, or future).	O.IDANLZ counters this threat by requiring the TOE to analyze System data containing information about attempts to halt the TOE.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	O.IDAUTH counters this threat by ensuring that only authenticated users have access to TOE data.
	O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.	O.IDSCAN counters this threat by requiring the TOE to collect System data containing information about attempts to halt the TOE.

Threats	Objectives	Rationale
T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	O.ACCESS counters this threat by only permitting authorized users to access TOE data.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	O.IDAUTH counters this threat by ensuring that only authenticated users have access to any TOE functions.
	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	O.PROTECT counters 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.	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.INSTAL counters this threat by ensuring that authorized administrators will configure the TOE properly.
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	O.ACCESS counters this threat by only permitting authorized users to access TOE data.
	O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.	O.EADMIN counters this threat by ensuring that the TOE has all the necessary administrator functions to manage the product.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	O.IDAUTH counters this threat by ensuring that only authenticated users have access to any TOE functions.
T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.	O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.	O.IDSCAN counters this threat by requiring a TOE, which contains a scanner, to collect and store static configuration information that may be indicative of a configuration change setting.
	O.IMPORT The TOE shall provide mechanisms to import data about assets from LDAP servers and ePO.	O.IMPORT counters this threat by requiring the TOE to be able to import information about assets so that scanning may be configured for all appropriate IT systems.
	O.SCAP	O.SCAP counters this threat by

Threats	Objectives	Rationale
	The TOE shall provide mechanisms to exchange SCAP Benchmark Assessment data.	requiring the TOE to be able to import additional benchmark assessments, enabling the TOE to address new configuration requirements as they are identified.
T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.	O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.	O.IDSCAN counters this threat by requiring a TOE, which contains a scanner, to collect and store static configuration information that may be indicative of malicious code.
	O.IMPORT The TOE shall provide mechanisms to import data about assets from LDAP servers and ePO.	O.IMPORT counters this threat by requiring the TOE to be able to import information about assets so that scanning may be configured for all appropriate IT systems.
	O.SCAP The TOE shall provide mechanisms to exchange SCAP Benchmark Assessment data.	O.SCAP counters this threat by requiring the TOE to be able to import additional benchmark assessments, enabling the TOE to perform new checks for malicious code as they are identified.
T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.	O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.	O.IDSCAN counters this threat by requiring a TOE, which contains a scanner, to collect and store static configuration information that may be indicative of vulnerability.
	O.IMPORT The TOE shall provide mechanisms to import data about assets from LDAP servers and ePO.	O.IMPORT counters this threat by requiring the TOE to be able to import information about assets so that scanning may be configured for all appropriate IT systems.
	O.SCAP The TOE shall provide mechanisms to exchange SCAP Benchmark Assessment data.	O.SCAP counters this threat by requiring the TOE to be able to import additional benchmark assessments, enabling the TOE to perform new checks for vulnerabilities as they are identified.
T.FALREC The TOE may fail to recognize	O.IDANLZ The TOE must apply analytical	O.IDANLZ counters this threat by ensuring that the TOE will

Threats	Objectives	Rationale
vulnerabilities or inappropriate activity based on data received from each data source.	processes and information to derive conclusions about intrusions (past, present, or future).	recognize vulnerabilities or inappropriate activity from a data source.
T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of data received from all data sources.	O.IDANLZ The TOE must apply analytical processes and information to derive conclusions about intrusions (past, present, or future).	O.IDANLZ counters this threat by ensuring that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.	O.AUDIT The TOE must record audit records for data accesses and use of the System functions.	O.AUDIT counters this threat by ensuring the TOE audits attempts for data access and use of TOE functions.
T.FALACT Issues resulting from scans of monitored systems may fail to be acted upon because the information is not disseminated from the TOE to other IT systems that are responsible for tracking or correcting the issues.	O.SCAP The TOE shall provide mechanisms to exchange SCAP Benchmark Assessment data.	O.SCAP counters this threat by ensuring the TOE supports the export of scan and analysis results in SCAP Benchmark Assessment format so that the information may be imported by other IT systems.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

Table 27 - Policies:Objectives Mapping

Policies	Objectives	Rationale
P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events, that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets, must be collected.	OE.AUDIT_REVIEW The IT environment will provide the capability to review audit information generated by the TOE.	OE.AUDIT_REVIEW supports this policy by providing the ability to review audit events generated by the TOE.
	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	OE.TIME supports this policy by providing a time stamp for insertion into the system data records.
	O.AUDIT The TOE must record audit records for data accesses and use of the System functions.	O.AUDIT addresses this policy by requiring collection of System data.
	O.IDSCAN The Scanner must collect and store static configuration	O.IDSCAN addresses this policy by requiring collection of audit data.

Policies	Objectives	Rationale
	information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.	
P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to data received from data sources and appropriate response actions taken.	O.IDANLZ The TOE must apply analytical processes and information to derive conclusions about intrusions (past, present, or future).	O.IDANLZ supports this policy by requiring analytical processes to be applied to data collected from Sensors and Scanners.
P.MANAGE The TOE shall only be managed by authorized users.	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.CREDEN supports this policy by requiring administrators to protect all authentication data.
	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.INSTAL supports this policy by ensuring administrators follow all provided documentation support procedures and maintain the security policy.
	OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.	OE.PERSON supports this policy by ensuring that competent administrators will manage the TOE
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	O.ACCESS supports this policy by permitting only authorized users to access TOE functions.
	O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.	O.EADMIN supports this policy by ensuring that there is a set of functions for administrators to use.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	O.IDAUTH supports this poilcy by requring the authentication of users prior to any TOE function accesses.
	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	O.PROTCT supports this policy by providing self protection of the TOE .

Policies	Objectives	Rationale
P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.	OE.DATABASE Those responsible for the TOE must ensure that access to the database, via mechanisms outside the TOE boundary (e.g., DBMS), is restricted to authorized users only.	OE.DATABASE supports this policy by requiring those responsible for the TOE to ensure that access to the database, via mechanisms outside the TOE boundary (e.g., DBMS), is restricted to authorized users only.
	OE.IDAUTH The IT Environment must be able to identify and authenticate users prior to the TOE allowing access to TOE functions and data on the Scan Engine.	OE.IDAUTH supports this policy by requiring the authentication of users prior to accessing any TOE functions.
	OE.SD_PROTECTION The IT Environment will provide the capability to protect system data.	OE.SD_PROTECTION supports this policy via IT Environment protections of the system data trail.
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	O.ACCESS supports this policy by only permitting authorized users to access TOE functions.
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	O.IDAUTH supports this policy by requiring the authentication of users prior to accessing any TOE functions via the Foundstone Enterprise Manager web interface.
	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	O.PROTCT supports this policy by providing TOE self-protection.
P.INTGTY Data collected and produced by the TOE shall be protected from modification.	OE.AUDIT_PROTECT The IT Environment will provide the capability to protect audit information generated by the TOE.	OE.AUDIT_PROTECT supports this policy by ensuring that the integrity of audit records in the database, generated by the TOE, is protected.
	OE.CRYPTO The IT Environment will provide the cryptographic functionality and protocols required for the implementation of secure channels between the TOE components and between the TOE and external IT systems.	OE.CRYPTO supports this policy by requiring the IT environment to provide secure channels via cryptographic functionality and protocols that can be used by the TOE to protect the data during transit.
	O.INTEGR The TOE must ensure the integrity of all system data.	O.INTEGR supports this policy by ensuring that data within the TOE's Scope of Control (TSC) is protected from modification.

Policies	Objectives	Rationale
P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.	OE.CRYPTO The IT Environment will provide the cryptographic functionality and protocols required for the implementation of secure channels between the TOE components and between the TOE and external IT systems.	OE.CRYPTO supports this policy by requiring the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit.
	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.PHYCAL supports this policy by ensuring the TOE is protected from unauthorized physical modifications
	OE.PROTECT The IT Environment will protect itself and the TOE from external interference or tampering.	OE.PROTECT supports this policy by ensuring the TOE is protected by the IT Environment.
	O.OFLOWS The TOE must appropriately handle potential system data storage overflows.	O.OFLOWS supports this policy by requiring the TOE to handle system data storage disruptions.
P.ACCACT Users of the TOE shall be accountable for their actions within the TOE.	O.AUDIT The TOE must record audit records for data accesses and use of the System functions.	O.AUDITS supports this policy by requiring auditing of all data accesses and use of TOE functions
	O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	O.IDAUTH supports this policy by ensuring each user is uniquely identified and authenticated.

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 28 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.	OE.INTROP The TOE is interoperable with the IT System it monitors	The OE.INTROP objective ensures the TOE has the needed access.
A.ASCOPE The TOE is appropriately scalable to the IT System the TOE	OE.INTROP The TOE is interoperable with the IT System it monitors	The OE.INTROP objective ensures the TOE has the necessary interactions with the IT

Assumptions	Objectives	Rationale
monitors.		System it monitors.
A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.	OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.	The OE.PERSON objective ensures that the TOE will be managed appropriately.
	OE.INTROP The TOE is interoperable with the IT System it monitors	The OE.INTROP objective ensures the TOE has the proper access to the IT System.
A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.	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.	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.	The OE.INSTAL objective ensures that the TOE is properly installed and operated by authorized administrators.
	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.	The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	OE.PHYSICAL	The OE.PHYCAL objective supports this assumption by providing the physical protection of the TOE hardware and software.
A.LOCATE	OE.PHYSICAL	The OE.PHYCAL objective supports this assumption by providing the physical protection of the TOE hardware and software.
A.ALARM The DBMS will generate an alarm if storage space in the database is exhausted.	OE.ALARM The DBMS will generate an alarm if storage space in the database is exhausted.	The OE.ALARM objective ensures that the DBMS will generate an alarm if storage space in the database is exhausted.
A.DATABASE Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.	OE.DATABASE Those responsible for the TOE must ensure that access to the database, via mechanisms outside the TOE boundary (e.g., DBMS), is restricted to authorized users only.	The OE.DATABASE objective ensures that access to any mechanisms outside the TOE boundary that may be used to access the database is configured by the administrators such that only authorized users may utilize the mechanisms.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

A family of EXT_IDS requirements is copied from the IDS System PP to specifically address the data collected and analysed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of system data and provide for requirements about collecting, reviewing and managing the data.

All of the components in this section are taken from the pp_ids_sys_br_v1.7 Protection Profile. IDS_STG.1.1 has been modified from the PP to delete the text "and send an alarm". An alarm is sent by the DBMS, which is part of the operational environment. Therefore, that portion of the SFR from the PP has been deleted but is addressed by A.ALARM and OE.ALARM.

These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no Extended SARs defined for this ST.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 29 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	FIA_UAU.1 Timing of authentication	This requirement supports O.ACCESS by ensuring that The TOE will not give any user access to the TOE's data and functions until the TOE has authenticated the user.
	FIA_UID.1 Timing of identification	This requirement supports O.ACCESS by ensuring that the users are identified before access to TOE administrative functions is allowed.
	FMT_MOF.1 Management of security functions behavior	The requirement supports O.ACCESS by ensuring that the TOE provides the ability to

Objective	Requirements Addressing the Objective	Rationale
		restrict managing the behavior of TOE functions to authorized users.
	FMT_MTD.1 Management of TSF data	This requirement supports O.ACCESS by ensuring that only authorized administrators of the system may query and add system data, and authorized administrators of the TOE may query and modify all other TOE data.
	EXT_IDS_RDR.1 Restricted data review	This requirement supports O.ACCESS by ensuring that the TOE provides the ability to restrict the review of system data to those granted with explicit read-access.
O.AUDIT The TOE must record audit records for data accesses and use of the System functions.	FAU_GEN.1 Audit data generation	This requirement supports O.AUDIT by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.	EXT_IDS_RDR.1 Restricted data review	This requirement supports O.EADMIN by ensuring that the TOE provides the ability for authorized administrators to view all system data collect and produced.
O.IDANLZ The TOE must apply analytical processes and information to derive conclusions about intrusions (past, present, or future).	EXT_IDS_ANL.1 Analyzer analysis	This requirement supports O.IDANLZ by ensuring that TOE can perform intrusion analysis and generate conclusions.
O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	FIA_ATD.1 User attribute definition	This requirement supports O.IDAUTH by ensuring that the TOE maintains the specified security attributes belonging to individual users.
	FIA_SOS.1 Verification of secrets	This requirement supports O.IDAUTH by ensuring that minimum password requirements are defined to provide a robust authentication process.
	FIA_UAU.1 Timing of authentication	This requirement supports O.IDAUTH by ensuring that users are authenticated before access to TOE administrative functions is

Objective	Requirements Addressing the Objective	Rationale
		allowed.
	FIA_UID.1 Timing of identification	This requirement supports O.IDAUTH by ensuring that the users are identified before access to TOE administrative functions is allowed.
	FMT_MOF.1 Management of security functions behavior	This requirement supports O.INTEGR by ensuring that the TOE provides the ability to restrict managing the behavior of TOE functions to users who have been identified and authenticated by the TOE.
	FMT_MTD.1 Management of TSF data	The requirement supports O.IDAUTH by ensuring that only authorized administrators of the system may query and add system data, and authorized administrators of the TOE may query and modify all other TOE data.
	FMT_SMF.1 Specification of management functions	The requirement supports O.IDAUTH by ensuring that the set of management functions to be restricted are defined.
	FMT_SMR.1 Security roles	This requirement supports O.IDAUTH by ensuring that the TOE is able to recognize the different administrative and user roles that exist for the TOE.
	EXT_IDS_RDR.1 Restricted data review	This requirement supports O.IDAUTH by ensuring that the TOE provides the ability to restrict the review of system data to those granted with explicit read-access.
O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.	EXT_IDS_SDC.1 System data collection	This requirement supports O.IDSCAN by ensuring that the TOE can scan, collect, and store static configuration information of an IT system. The type of configuration information collected must be defined in the ST.
O.IMPORT The TOE shall provide mechanisms to import data about assets from	FPT_TDC.1(a) Inter-TSF Basic TSF Data Consistency	This requirement supports O.IMPORT by ensuring that the TOE is able to define management

Objective	Requirements Addressing the Objective	Rationale
LDAP servers and ePO.		functionality to import asset data from configured sources.
O.INTEGR The TOE must ensure the integrity of all system data.	FMT_MOF.1 Management of security functions behavior	This requirement supports O.INTEGR by ensuring that only authorized administrators of the system may query or add System data.
O.OFLOWS The TOE must appropriately handle potential system data storage overflows.	EXT_IDS_STG.2 Prevention of system data loss	This requirement supports O.OFLOWS by ensuring that the TOE prevents the loss of system data in the event that its storage capacity has been reached.
O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	FMT_MOF.1 Management of security functions behavior	This requirement supports O.PROTECT by ensuring that the TOE provides the ability to restrict managing the behavior of TOE functions to authorized users.
	FMT_MTD.1 Management of TSF data	The requirement supports O.PROTECT by ensuring that only authorized administrators of the system may query and add system data, and authorized administrators of the TOE may query and modify all other TOE data.
O.SCAP The TOE shall provide mechanisms to exchange SCAP Benchmark Assessment data.	FPT_TDC.1(b) Inter-TSF Basic TSF Data Consistency	This requirement supports O.SCAP by ensuring that the TOE includes mechanisms to exchange SCAP Benchmark Assessment data with external systems.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional 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 into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 30 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 30 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Satisfied by the IT Environment (OE.TIME)
FIA_ATD.1	No dependencies	N/A	
FIA_SOS.1	No dependencies	N/A	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UID.1	No dependencies	N/A	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_SMF.1	No dependencies	N/A	
FMT_SMR.1	FIA_UID.1	✓	
FPT_TDC.1(a)	No dependencies	N/A	
FPT_TDC.1(b)	No dependencies	N/A	
EXT_IDS_SDC.1	FPT_STM.1	✓	Satisfied by the IT Environment (OE.TIME)
EXT_IDS_ANL.1	EXT_IDS_SDC.1	✓	
	FPT_STM.1	✓	Satisfied by the IT Environment (OE.TIME)
EXT_IDS_RDR.1	EXT_IDS_SDC.1	✓	
EXT_IDS_STG.2	EXT_IDS_SDC.1	✓	

9 Acronyms and Terms

This section describes the acronyms and terms.

9.1 Acronyms

Table 31 - Acronyms and Terms

Acronym	Definition
API	Application Program Interface
BSD	Berkeley Software Distribution
CC	Common Criteria
CM	Configuration Management
CPE	Common Platform Enumeration
CCE	Common Configuration Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DBMS	Database Management System
DNS	Dynamic Name Resolution
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface
IBM	International Business Machines
IDS	Intrusion Detection System
IIS	Internet Information Services
IOS	Internetwork Operating System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
ME	Millennium Edition
MAC	Media Access Control
MDAC	Microsoft Data Access Components
NetBIOS	Network Basic Input/Output System
NIST	National Institute of Standards and Technology

Acronym	Definition
NT	New Technology
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
PHP	PHP Hypertext Processor
PP	Protection Profile
SAR	Security Assurance Requirement
SCAP	Security Content Automation Protocol
SP	Service Pack
SFR	Security Functional Requirement
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
UDP	User Datagram Protocol
URL	Uniform Resource Locator
WAN	Wide Area Network
XCCDF	Extensible Configuration Checklist Description Format
XP	Experience

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com