McAfee Foundstone Enterprise Vulnerability Management Solution 5.0.4

Security Target

Document Version 1.11

October 25, 2007

COPYRIGHT

TRADEMARKS

LICENSE AND PATENT INFORMATION

License Agreement

License Attributions

This product includes the distribution of third-party or open source code, which may be subject to the terms of different license agreements. Refer to the `Foundstone_Licenses.pdf` file and the applicable third-party code files included with this product distribution.

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite N
Columbia, MD 21046-2587
Phone: 301-498-0150
Fax: 301-498-0855

DOCUMENT INTRODUCTION

Prepared By:

COACT, Inc.
Rivers Ninety Five
9140 Guilford Road, Suite N
Columbia, Maryland 21046-2587

Prepared For:

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the McAfee Foundstone Enterprise Vulnerability Management Solution Version 5.0.4. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Date	Description
1.0	September 23, 2006	Initial release
1.1	September 27, 2006	Addressed vendor comments and EORs
1.2	November 22, 2006	Addressed Initial VOR results
1.3	November 23, 2006	Incorporated vendor comments
1.4	December 15, 2006	Additional changes for Initial VOR and TOE version
1.5	December 18, 2006	Corrected an incorrect reference to HIP
1.6	January 10, 2007	Added FAU_SAR.1 and FAU_STG.2
1.7	May 24, 2007	Added configuration option for custom certificates
1.8	July 23, 2007	Corrected FAU_GEN.1
1.9	September 5, 2007	Provided more detail on scan, analysis and report functions.
1.10	September 13, 2007	Incorporated vendor comments
1.11	October 25, 2007	Updates per Final VOR

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

CC ..... Common Criteria
EAL2 ..... Evaluation Assurance Level 2
GUI ..... Graphical User Interface
I&A ..... Identification and Authentication
IP ..... Internet Protocol
IT ..... Information Technology
NIAP ..... National Information Assurance Partnership
PP ..... Protection Profile
SF ..... Security Function
SFP ..... Security Function Policy
SOF ..... Strength of Function
ST ..... Security Target
TOE ..... Target of Evaluation
TSC ..... TOE Scope of Control
TSF ..... TOE Security Function
TSFI ..... TSF Interface
TSP ..... TOE Security Policy

CHAPTER 1

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for McAfee Foundstone Enterprise Vulnerability Management Solution Version 5.0.4. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 2.3*, the ISO/IEC JTC 1/SC27, *Guide for the Production of PPs and STs, Version 0.9*, and all international interpretations through 1/11/07. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

This section provides identifying information for the McAfee Foundstone Enterprise Vulnerability Management Solution Version 5.0.4 Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target

McAfee Foundstone Enterprise Vulnerability Management Solution Version 5.0.4 Security Target, version 1.10, dated September 13, 2007.

1.1.2 TOE Reference

McAfee Foundstone Enterprise Vulnerability Management Solution Version 5.0.4. The system is hereafter collectively referred to as Foundstone Enterprise.

1.1.3 Security Target Authors

COACT, Inc.

1.1.4 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) from the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

1.2 TOE Overview

This Security Target defines the requirements for the Foundstone Enterprise. The TOE is a vulnerability management system designed to scan specified targets for vulnerabilities and includes a management system that provides management and monitoring functionality.

1.2.1 Security Target Organisation

Chapter 1 of this ST provides introductory and identifying information for the TOE.

Chapter 2 describes the TOE and provides some guidance on its use.

Chapter 3 provides a security environment description in terms of assumptions, threats and organisational security policies.

Chapter 4 identifies the security objectives of the TOE and of the Information Technology (IT) environment.

Chapter 5 provides the TOE security and functional requirements, as well as requirements on the IT environment.

Chapter 6 is the TOE Summary Specification, a description of the functions provided by the TOE to satisfy the security functional and assurance requirements.

Chapter 7 identifies claims of conformance to a registered Protection Profile (PP).

Chapter 8 provides a rationale for the security objectives, requirements, TOE summary specification and PP claims.

1.3 Common Criteria Conformance

This ST is compliant with the Common Criteria (CC) Version 2.3 assurance requirements (Part 3) for EAL2. This ST uses explicitly stated functional requirements in addition to functional requirements drawn from CC Version 2.3 (Part 2).

1.4 Protection Profile Conformance

This ST does not claim conformance to any Protection Profile. However, many of the concepts from the Intrusion Detection System System Protection Profile (Version 1.6) have been incorporated into this ST.

CHAPTER 2

2. TOE Description

This section provides the context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Foundstone Enterprise Overview

Foundstone Enterprise is a Vulnerability Management System that scans specified targets for vulnerabilities. It provides a management interface to configure the system and generate reports regarding the results of the scans.

Foundstone Enterprise consists of three main components:

A) The Foundstone Enterprise Manager uses Microsoft Internet Information Services (IIS) to provide authorized users with access to Foundstone Enterprise through their Web browsers. It allows them to manage and run Foundstone Enterprise from anywhere on the network. Access is protected by user identification and authentication.

B) One or more FoundScan Engines scan the network environment. The FoundScan Engine is the server that scans your network. Depending on the logistics and size of your network, you may need more than one FoundScan Engine to scan the network. The one required FoundScan Engine is referred to as the primary engine. All others (if present) are referred to as secondary engines.

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

All traffic between the components is encrypted for secure communication.

2.2 Physical Boundary

The physical boundary of the TOE includes:

A) The Foundstone Enterprise Manager application

B) The FoundScan application software on each FoundScan Engine

C) The database on the Foundstone Database system

Note specifically that the hardware and operating systems on each of the systems are excluded from the TOE boundary. IIS on the Foundstone Enterprise Manager and SQL Server 2000 are also excluded from the TOE boundary.

2.3 Logical Boundary

The logical boundaries of the TOE are defined by the functions provided by the TOE and are described in the following sections.

2.3.1 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 Foundstone Enterprise manager.

2.3.2 Identification and Authentication (I&A)

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 their user account that defines the functionality the user is allowed to perform.

When interacting with the TOE via the Foundstone Enterprise Manager GUI, I&A is performed by the TOE. On all three components, I&A for local login to the operating system (i.e., via the local console) is performed by Windows (IT Environment).

2.3.3 Self Protection

The TOE provides for self protection and non-bypassability of functions within the TOE's scope of control (TSC). The TOE controls actions carried out by an administrator by controlling a session and the actions carried out during a session. When multiple administrators are connected simultaneously, the roles (and therefore permissions) are tracked individually to ensure proper access restrictions are applied to each session. By maintaining and controlling a user session a user has with the TOE, the TOE ensures that no security functions within the TSC are bypassed and that there is a separate domain for the TOE that prevents the TOE from being interfered with or tampered with for those users that are within the TSC.

Since the TOE consists of a set of applications, the TOE cannot provide complete self-protection for itself. The TOE depends on the operating systems and hardware (IT Environment) to protect the TOE from interference or bypass from users or processes outside the TSC. The IT Environment also provides the SSL functionality used to protect communications between the TOE components.

2.3.4 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 Foundstone Enterprise Manager. All user types may use the Foundstone Enterprise Manager.

The TOE provides the following management functions:

A) User management,

B) Root organization management,

C) Workgroup management,

D) FoundScan Engine management,

E) Asset management,

F) Scan management,

G) Report management

2.3.5 Audit

The TOE's Audit Security Function provides auditing of management actions performed by administrators.

2.4 Foundstone Enterprise Evaluated Configuration

Foundstone Enterprise 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 FoundScan Engines. The scan engines generate all scanning traffic on their local network segments. They send the resulting scan data back over the WAN to the Foundstone Database.

In this architecture the following components exist:

A) One instance of Foundstone Enterprise Manager on a dedicated platform

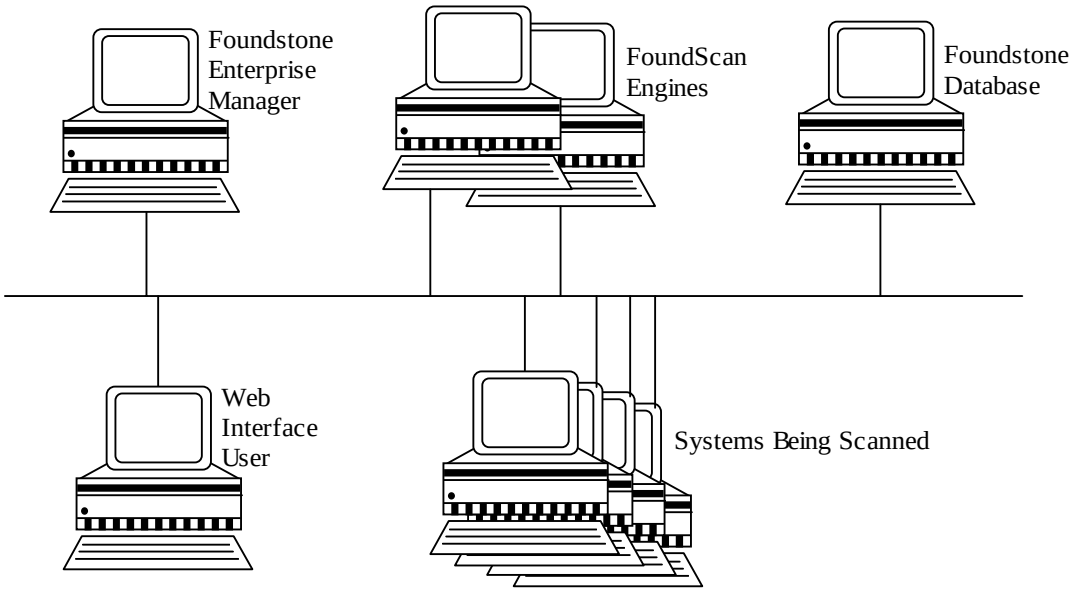
B) One instance of FoundScan Engine (primary engine) on a dedicated platform

C) Zero or more instances of FoundScan Engine (secondary engines) on additional dedicated platforms

D) One instance of the Foundstone Database hosted on a separate dedicated platform (together with the DBMS)

The evaluated configuration is illustrated in the following figure.

Figure 1 - Typical Foundstone Enterprise Configuration



2.4.1 Foundstone Enterprise Configuration Options

A) The Microsoft IIS Lockdown tool (for IIS 5.0 running on Windows 2000 Server) is used.

B) Custom certificates are installed on all components during installation.

2.4.2 Foundstone Enterprise Manager Configuration

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

Table 1 - Foundstone Enterprise Manager Component Requirements

Component Minimum Requirements	
Processor	Dual Xeon 2Ghz
Memory	2 GB RAM
Disk Space	80GB Partition
Operating System	Windows 2000 Server or Windows Server 2003 Current service pack: Windows 2000 - SP4 (minimum) Windows 2003 - SP1 (minimum) Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023
Additional Software	IIS 5.0 if using Win 2000 Server IIS 6.0 if using Win 2003 Server Current IIS security patches MDAC 2.7 SP1
Network Card	Dual 10/100/1000 Ethernet
Disk Partition Formats	NTFS
Required Services	n/a

2.4.3 FoundScan Engine (Primary or Secondary) Configuration

The platform on which the FoundScan Engine software is installed must be dedicated to functioning as a FoundScan Engine (Primary or Secondary). The TOE requires the following hardware and software configuration on this platform.

Table 2 - FoundScan Engine (Primary or Secondary) Component Requirements

Component Minimum Requirements	
Processor	Dual Xeon 2Ghz
Memory	2 GB RAM
Disk Space	80GB Partition
Operating System	Windows 2000 Server or Windows Server 2003 Current service pack: Windows 2000 - SP4 (minimum) Windows 2003 - SP1 (minimum) Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023
Additional Software	MDAC 2.7 SP1 SQL Client Tools (for Microsoft SQL Server 2000) JRE Java Runtime Environment 1.5.0_06
Network Card	Dual 10/100/1000 Ethernet
Virtual Memory	2.0 GB
Disk Partition Formats	NTFS
Required Services	NetBIOS over TCP/IP Print Spooler

An Administrator account must be defined on the platform for use by the TOE.

2.4.4 Foundstone Database Configuration

The platform on which the Foundstone Database is installed must be dedicated to functioning as the database server for the TOE. The DBMS is installed on this same platform. The TOE requires the following hardware and software configuration on this platform.

Table 3 - Foundstone Database Component Requirements

Component Minimum Requirements	
Processor	Dual Xeon 2Ghz
Memory	2 GB RAM
Disk Space	80GB Partition
Operating System	Windows 2000 Server or Windows Server 2003 Current service pack: Windows 2000 - SP4 (minimum) Windows 2003 - SP1 (minimum) Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023
Additional Software	Microsoft SQL Server 2000 (SP4 and all hotfixes/patches)
Network Card	Dual 10/100/1000 Ethernet
Virtual Memory	2.0 GB
Disk Partition Formats	NTFS
SQL Server Memory Settings	900MB
Required Services	n/a

2.4.5 Supported Web Browsers

Authorized users can access the Foundstone system through their Web browser software from anywhere on the network, depending on your network settings.

Foundstone 5.0.4 supports Microsoft Internet Explorer 6.0 and higher, running on Windows 2000 SP2 and higher, Windows 2003 Server, or Windows XP. Latest service packs should be applied to both your browser and operating system. Foundstone 5.0.4 requires the Java Runtime Environment version Java Runtime Environment 1.5.0_06. If this is not found on the user's system when it is needed, the user's Web browser silently installs it.

2.4.6 Foundstone Enterprise Functionality Not Included in the Evaluation

The functionality of Foundstone Enterprise that is not included in the evaluation is described below:

A) The optional Remediation Module.

B) The optional Threat Correlation Module.

C) The optional Notification Module.

D) The Foundstone Configuration Manager/Foundstone Update (software updates).

E) Integration with a third-party Single-Sign-On server.

F) Management via FoundScan Console. As part of the TOE installation process, all ability to manage users and reports via FoundScan Console is disabled. FoundScan Console is used for initial configuration of the local FoundScan Engine only.

2.5 TOE 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.

Users are administrators that manage the TOE.

Table 4 - TOE Data

TSF Data	Description	AD	UA	GE
Asset groups	Grouping of assets for ease of configuring parameters and association with scans.			X
Assets	Systems that have been discovered by the TOE during scans.			X
FoundScan Engines configuration	Parameters associated with each FoundScan Engine, such as which root organization it will perform scans for			X
Reports	Reports are launched to generate information regarding the results of a specific scan and may be viewed once generated			X
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			X
Scans	Parameters that define the scanning actions to be performed by the TOE and permissions relevant to each scan granted to Foundstone Users			X

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

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

2.6 Rationale for Non-Bypassability and Separation for the TOE

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment. Foundstone Enterprise components are software only products and therefore the non-bypassability and non-interference claims are dependent upon hardware and OS mechanisms. The TOE runs on top of the IT Environment supplied OSs.

Non-bypassability

The TOE ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: the interfaces are well defined and insure that the access restrictions are enforced. Non-security relevant interfaces do not interact with the security functionality of the TOE. The TOE depends upon OS mechanisms to protect TSF data such that it can only be accessed via the TOE.

Non-interference

The TOE is implemented with well defined interfaces that can be categorized as security relevant or non-security relevant. The TOE is implemented such that non-security relevant interfaces have no means of impacting the security functionality of the TOE. Unauthenticated users may not perform any actions within the TOE. The TOE tracks multiple administrators by sessions and ensures the access privileges of each are enforced.

The server hardware provides virtual memory and process separation which the server OS utilizes to ensure that other (non-TOE) processes may not interfere with the TOE; all interactions are limited to the defined TOE interfaces.

CHAPTER 3

3. TOE Security Environment

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies 1) assumptions about the environment, 2) threats to the assets and 3) organisational security policies.

This chapter identifies assumptions as A.*assumption*, organizational security policies as P.*policy* and threats as T.*threat*.

3.2 Assumptions

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

Table 5 - Intended Usage Assumptions

A.Type	Description
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
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.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.

Table 6 - Physical Assumptions

A.Type	Description
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

Table 7 - Personnel Assumptions

A.Type	Description
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.

3.3 Threats

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

The following table identifies threats to the TOE.

Table 8 - TOE Threats

T.Type	TOE Threats
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

The following table identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

Table 9 - IT System Threats

T.Type	IT System Threats
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.

3.4 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the Intrusion Detection System System Protection Profile.

Table 10 - Organizational Security Policies

P.Type	Organizational Security Policy
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.

CHAPTER 4

4. Security Objectives

This section identifies the security objectives of the TOE, the TOE's IT environment and the TOE's non-IT environment. The security objectives identify the responsibilities of the TOE, the TOE's IT environment, and the TOE's non-IT environment in meeting the security needs.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 11 - Information Technology (IT) Security Objectives

Objective	Definition
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its 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.IDANLZ	The Analyzer must accept data from Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential System data storage overflows.
O.INTEGR	The TOE must ensure the integrity of all System data.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.

4.2 Security Objectives for the Environment

The TOE's operating environment must satisfy the following objectives.

Table 12 - Security Objectives of the Environment

Objective	Definition
O.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.
O. PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
O.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.
O.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
O.INTROP	The TOE is interoperable with the IT System it monitors
OE.TIME	The IT Environment will provide reliable timestamps to the TOE
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.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 FoundScan Engine.
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.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 for authorized administrators to review audit information generated by the TOE.

.

CHAPTER 5

5. IT Security Requirements

This section identifies the security functional requirements for the TOE and for the IT environment. The functional requirements included in this section are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3* with the exception of italicised items listed in brackets.

The CC defines four operations on security functional requirements. The font conventions listed below identify the conventions for the operations defined by the CC.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Explicitly stated requirements are included in this ST. The names of these requirements start with IDS_.

5.1 Security Functional Requirements for the TOE

The functional security requirements for the TOE consist of the following components, summarized below.

Table 13 - TOE SFRs

Functional Components	
FAU_GEN.1	Audit Data Generation
FIA_UAU.1	Timing of authentication
FIA_ATD.1	User attribute definition
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_RVM_SFT.1	Non-Bypassability of the TSP for Software TOEs
FPT_SEP_SFT.1	TSF Domain Separation for Software TOEs
IDS_SDC.1	System Data Collection
IDS_ANL.1	Analyzer analysis
IDS_RDR.1	Restricted Data Review
IDS_STG.2	Prevention of System data loss

5.1.1 5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

b) All auditable events for the basic 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 the following table*.

Application Note: The auditable events for the basic level of auditing are included in the following table.

Table 14 - TOE SFRs

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to the TOE and System data	Object IDs, Requested access
FIA_UAU.1(1)	All use of the authentication mechanism	User identity, location
FIA_UID.1(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

Application Note: The IDS_SDC and IDS_ANL requirements in this PP address the recording of results from scanning and analysing tasks (i.e., System data).

5.1.2 Identification and authentication (FIA)

5.1.2.1 FIA_ATD.1 User Attribute Definition

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

a) *User identity;*

b) *User password;*

c) *User Account Type;*

d) *Associated Root Organization;*

e) *Associated Workgroups*; and

f) *No other security attributes*.

5.1.2.2 FIA_UAU.1(1) Timing of authentication

FIA_UAU.1.1(1) The TSF shall allow *no actions* on behalf of the user to be performed before the user is authenticated **on the Foundstone Enterprise Manager web interface**.

FIA_UAU.1.2(1) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user **on the Foundstone Enterprise Manager web interface**.

Application Note: The IT Environment is responsible for I&A to access the operating systems. The TOE is responsible for I&A before management access is granted on the Foundstone Enterprise Manager.

5.1.2.3 FIA_UID.1(1) Timing of Identification

FIA_UID.1.1(1) The TSF shall allow *no actions* on behalf of the user to be performed before the user is identified **on the Foundstone Enterprise Manager web interface**.

FIA_UID.1.2(1) The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user **on the Foundstone Enterprise Manager web interface**.

Application Note: The IT Environment is responsible for I&A to access the operating systems. The TOE is responsible for I&A before management access is granted on the Foundstone Enterprise Manager.

5.1.3 Security Management (FMT)

5.1.3.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of the functions *of System data collection, analysis and reaction* to *Foundstone Users with permissions for specific scans, Global Administrators, Root Organization Administrators and Workgroup Administrators*.

5.1.3.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query *and add* *System data*, **and shall restrict the ability to query and modify all other TOE data** to *the roles associated with specific data and operations as shown in the following table*.

Table 15 - TSF Data Access Permissions

TSF Data	Global Administrator	Root Organization Administrator	Workgroup Administrator	Foundstone User
Asset groups	None	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None
Assets	None	Modify properties within the same root organization	Modify properties within the workgroups	None
FoundScan Engines	None	Modify properties within the same root organization	None	None
Reports	None	Submit, Delete, Cancel within the same root organization	Report access is determined by the access permissions listed below	Report access is determined by the access permissions listed below
Root Organizations	Create, Delete, Modify properties	Modify properties	None	None
Scans	Create, Delete, Modify properties, Launch	Create, Delete, Modify properties, Launch within the same root organization	Create, Delete, Modify properties, Launch within the workgroups	Scan access is determined by the access permissions listed below
User Accounts	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None
User groups	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None
User roles	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None

TSF Data	Global Administrator	Root Organization Administrator	Workgroup Administrator	Foundstone User
Workgroups	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None

Table 16 - Scan/Report Access Permissions

Scan Access	Description
View	View the reports and other information displayed in the Foundstone Enterprise Manager for the selected scan. Reports may be submitted 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 or report.
Full	All of the above. Allow the user or group to edit, launch, or delete any scan in the organization or workgroup.

5.1.3.3 FMT_SMF.1 Specification of Management Functions

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

A) User management,

B) Root organization management,

C) Workgroup management,

D) Asset management,

E) Scan management,

F) Report management.

5.1.3.4 FMT_SMR.1 Security Roles

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.

5.1.4 Protection of the TSF (FPT)

5.1.4.1 FPT_RVM_SFT.1 Non-Bypassability of the TSP for Software TOEs

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_RVM by themselves. This explicitly stated SFR states the portion of FPT_RVM that can be addressed by the TOE. See FPT_RVM_OS (levied on the IT Environment) for the remaining functionality.

FPT_RVM_SFT.1.1 The TSF, when invoked shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed

5.1.4.2 FPT_SEP_SFT.1 TSF Domain Separation for Software TOEs

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_SEP by themselves. This explicitly stated SFR states the portion of FPT_SEP that can be addressed by the TOE. See FPT_SEP_OS (levied on the IT Environment) for the remaining functionality.

FPT_SEP_SFT.1.1 The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_SFT.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.5 IDS Component Requirements (IDS)

Rationale for explicitly stated SFR: This family of 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. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

5.1.5.1 IDS_SDC.1 System Data Collection

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 and

b) *no other events*.

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 17 - System Data Collection Events and Details

Component	Event	Details
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols

5.1.5.2 IDS_ANL.1 Analyser analysis

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all system data received:

a) signature; and

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

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*.

5.1.5.3 IDS_RDR.1 Restricted Data Review (EXP)

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 the table below* from the System data.

Table 18 - 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

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information.

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.

5.1.5.4 IDS_STG.2 Prevention of System data loss

IDS_STG.2.1 The System shall ignore System data if the storage capacity has been reached.

5.2 Security Functional Requirements for the IT Environment

The functional security requirements for the IT Environment consist of the following components, summarized below.

Table 19 - IT Environment SFRs

Functional Components	
FAU_SAR.1	Audit review
FAU_STG.2	Guarantees of audit data availability
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of Identification
FPT_ITT.1	Basic Internal TSF Data Transfer Protection
FPT_RVM_OS.1	Non-bypassability of the TSP
FPT_SEP_OS.1	TSF domain separation
FPT_STM.1	Reliable time stamps
IDS_STG.1	Guarantee of System Data Availability

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_SAR.1: Audit review

FAU_SAR.1.1 The TSF shall provide *authorized administrators with permission to view audit records generated by the TOE* with the capability to read **all** *audit record detail* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.1.2 FAU_STG.2: Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to prevent unauthorized modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that *the oldest* audit records will be maintained when the following conditions occur: audit storage exhaustion.

5.2.2 Identification and authentication (FIA)

5.2.2.1 FIA_UAU.1(2) Timing of authentication

FIA_UAU.1.1(2) The TSF shall allow *no actions* on behalf of the user to be performed before the user is authenticated **on the Foundstone Enterprise Manager, FoundScan Engine and Foundstone Database local consoles**

FIA_UAU.1.2(2) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user **on the Foundstone Enterprise Manager, FoundScan Engine and Foundstone Database local consoles**.

Application Note: The IT Environment is responsible for I&A to access the operating systems. The TOE is responsible for I&A before management access is granted on the Foundstone Enterprise Manager.

5.2.2.2 FIA_UID.1(2) Timing of Identification

FIA_UID.1.1(2) The TSF shall allow *no actions* on behalf of the user to be performed before the user is identified **on the Foundstone Enterprise Manager, FoundScan Engine and Foundstone Database local consoles**.

FIA_UID.1.2(2) The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user **on the Foundstone Enterprise Manager, FoundScan Engine and Foundstone Database local consoles**.

Application Note: The IT Environment is responsible for I&A to access the operating systems. The TOE is responsible for I&A before management access is granted on the Foundstone Enterprise Manager.

5.2.3 Protection of the TSF (FPT)

5.2.3.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

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

5.2.3.2 FPT_RVM_OS.1 Non-Bypassability of the TSP for OSs

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_RVM by themselves. This explicitly stated SFR states the portion of FPT_RVM supplied by the OS and hardware in support of the overall FPT_RVM functionality. See FPT_RVM_SFT (levied on the TOE) for the remaining functionality.

FPT_RVM_OS.1.1 The security functions of the host OS shall ensure that host OS security policy enforcement functions are invoked and succeed before each function within the scope of control of the host OS is allowed to proceed.

5.2.3.3 FPT_SEP_OS.1 TSF Domain Separation for OSs

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_SEP by themselves. This explicitly stated SFR states the portion of FPT_SEP supplied by the OS and hardware in support of the overall FPT_SEP functionality. See FPT_SEP_SFT (levied on the TOE) for the remaining functionality.

FPT_SEP_OS.1.1 The security functions of the host OS shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host OS.

FPT_SEP_OS.1.2 The security functions of the host OS shall enforce separation between the security domains of subjects in the scope of control of the host OS.

5.2.3.4 FPT_STM.1Reliable time stamps

FPT_STM.1.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for ~~its own~~ **the TOE's** use.

Rationale for refinement: Time stamps are a dependency of FAU_GEN.1, which is levied on the TOE. The time stamps are provided by the IT Environment.

5.2.4 IDS Component Requirements (IDS)

5.2.4.1 IDS_STG.1 Guarantee of System Data Availability

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

IDS_ STG.1.2 The System shall protect the stored System data from modification.

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

IDS_ STG.1.3 The System shall ensure that *system data for at least the number of days specified by the administrator* System data will be maintained when the following conditions occur: System data storage exhaustion.

5.3 Strength of Function for the TOE

The minimum SOF claimed is SOF-Basic. FIA_UAU.1(1) utilizes a probabilistic or permutational mechanism.

5.4 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2. These requirements are summarised in the following table:

Table 20 - TOE Security Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration management	ACM_CAP.2	Configuration Items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive High Level Design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

CHAPTER 6

6. TOE Summary Specification

6.1.1 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, 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 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.

As scans are performed, details about systems within the designated address list are learned. As new systems 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, access control 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.

Reports may be generated for any scan by a Root Organization Administrator. A report summarizes the results of the scan; it also enables a user to drill down to

more specific information concerning the results. Reports are generated on a FoundScan Engine, then uploaded to the Foundstone Enterprise Manager.

Reports may be viewed according to the following restrictions:

Table 21 - 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

6.1.2 Identification and Authentication (I&A)

The TOE enables an authorised user to manage the TOE via a web interface on the Foundstone 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:

A) Contains at least 8 characters

B) Contains at least one number

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

The TOE also protects the password from visual detection by echoing back asterisks ("*") for the entered passwords.

6.1.3 Self Protection

The TOE provides for self protection and non-bypassability of functions within the TOE's scope of control (TSC). The TOE controls actions carried out by an administrator by controlling a session and the actions carried out during a session. When multiple administrators are connected simultaneously, the roles (and therefore permissions) are tracked individually to ensure proper access restrictions are applied to each session. By maintaining and controlling a user session a user has with the TOE, the TOE ensures that no security functions within the TSC are bypassed and that there is a separate domain for the TOE that prevents the TOE from being interfered with or tampered with for those users that are within the TSC.

6.1.4 Management (MGMT)

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 Foundstone Enterprise Manager. All user types may use the Foundstone Enterprise Manager.

The TOE provides the following management functions:

A) User management,

B) Root organization management,

C) Workgroup management,

D) FoundScan Engine management,

E) Asset management,

F) Scan management,

G) Report management

6.1.4.1 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, 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 the following table.

Table 22 - 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 FoundScan Engine settings from the Foundstone 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 the following table.

Table 23 - Administrative Capabilities

TSF Data	Global Administrator	Root Organization Administrator	Workgroup Administrator	Foundstone User
Asset groups	None	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None
Assets	None	Modify properties within the same root organization	Modify properties within the workgroups	None
FoundScan Engines	None	Modify properties within the same root organization	None	None
Reports	None	Submit, Delete, Cancel within the same root organization	Report access is determined by the access permissions listed below	Report access is determined by the access permissions listed below
Root Organizations	Create, Delete, Modify properties	Modify properties	None	None
Scans	Create, Delete, Modify properties, Launch	Create, Delete, Modify properties, Launch within the same root organization	Create, Delete, Modify properties, Launch within the workgroups	Scan access is determined by the access permissions listed below
User Accounts	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None
User groups	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None
User roles	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None
Workgroups	Create, Delete, Modify properties	Create, Delete, Modify properties within the same root organization	Create, Delete, Modify properties within the workgroups	None

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:

Table 24 - Scan/Report Access Descriptions

Scan Access	Description
View	View the reports and other information displayed in the Foundstone Enterprise Manager for the selected scan. Reports may be submitted 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 or report.
Full	All of the above. Allow the user or group to edit, launch, or delete any scan in the organization or workgroup.

6.1.4.2 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.

6.1.4.3 Workgroup Management

Workgroups are configured by the Global Administrator. 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.

6.1.4.4 FoundScan Engine Management

A Root Organization Administrator may configure the following security-relevant settings for any engine associated with the same root organization.

Table 25 - FoundScan Engine Management

Area	Parameter	Description
Report	Generate Reports for	Choose the role that this engine will assume on your network. • This engine - This engine will only generate reports for scans created by this engine. Then it uploads the report to the Foundstone Enterprise Manager so everyone can access it. • Any engine - This engine will generate reports in the database queue. Then it uploads the report to the Foundstone Enterprise Manager so everyone can access it. • Do not generate reports - This engine will not generate reports. When this engine finishes a scan, the reports are queued in the database to wait for an available engine to generate the report.
Console Management	Remove scans	Select this option to set the time for keeping non-active scans.
	Limit number of nonactive scans	Select this option to limit the number of non-active scans.
	Perform db maintenance	Use this option to set up regular maintenance on the Foundstone Database.
	Delete jobs older than	Check this option to automatically delete old scan jobs after a specified number of days. This helps reduce the amount of disk space required by the database.
Engine Connection	Address	Enter the IP address, DNS name, or NetBIOS name for the Web server running the Foundstone Enterprise Manager.
	Port	Enter the port number that the Web server uses to receive McAfee information.
	Use SSL	Use Secure Socket Layer between this FoundScan Engine and the Foundstone Enterprise Manager. This option is always selected for the evaluated version.
	Authentication Scheme	Shows the authentication method being used to communicate from the Foundstone Enterprise Manager to the FoundScan Engine.
Enterprise Manager Connection	Address	Enter the IP address, DNS name, or NetBIOS name for the Web server running the Foundstone Enterprise Manager.
	Port	Enter the port number that the Web server uses to receive McAfee information.

Area	Parameter	Description
	Use SSL	Use Secure Socket Layer between this FoundScan Engine and the Foundstone Enterprise Manager. This option is always selected for the evaluated version.
	Authentication Scheme	Shows the authentication method being used to communicate from the Foundstone Enterprise Manager to the FoundScan Engine.
Default Ports	Host Detection Ports	Specifies the default TCP and UDP ports to be used during scans to discover hosts.
	Service Detection Ports	Specifies the default TCP and UDP ports to be used during scans to discover services running on scanned systems.

6.1.4.5 Asset Management

Assets are systems 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.

6.1.4.6 Scan Management

Scans may be created by Global Administrators, 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:

A) IP addresses/assets to be included in the scan

B) ICMP, TCP and UDP protocol options for discovery scans

C) Credentials to be used during scans to help identify access configuration settings

D) Service discovery

E) Vulnerability scans to be performed; the list of known vulnerabilities may be updated so that the scans are kept current as new vulnerabilities are identified

F) Web application assessment

G) Schedule a recurring scan

H) The scan engine and network interface to be used

I) Windows (time slots) during which the scan may execute

6.1.4.7 Report management

Report management may be performed by Root Organization Administrators. This role may:

A) Submit a report (associated with any scan defined within the root organization) for processing

B) Delete reports from a scan engine (they are uploaded to the Foundstone Enterprise manager)

C) Cancel a report queued for processing on a scan engine

Report management may also be performed by Workgroup Administrators and Foundstone Users based upon specific scan access permissions they have been granted.

6.1.5 Audit

The TOE's Audit Security Function provides auditing of management actions performed by administrators. The following audit information is collected:

A) Start-up and shutdown of audit functions

B) Access to the TOE and System data, including the information being accessed and the type of access

C) Successful and unsuccessful I&A attempts, including the supplied user identity and IP address of the browser session

D) All modifications in the behavior of the functions of the TSF

E) All modifications to the values of TSF data

F) Use of the management functions, including the IP address of the browser session (user identity) and the function used

G) Modifications to the group of users that are part of a role, including the IP address of the browser session (user identity)

All audit records include the date and time of the event, type of event, and subject identity performing the action (the user identifier supplied by the user and/or IP address of the browser session associated with the event). The type of event implicitly states whether or not the action succeeded (i.e., there are separate event types for successful and unsuccessful I&A attempts).

Audit records are stored in the database. Administrators and 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.

6.2 Assurance Measures

6.2.1 TOE Security Assurance Requirements

The following table provides a reference between each TOE assurance requirement and the related vendor documentation that satisfies each requirement.

Table 26 - Assurance Measures

Assurance Component	Documentation Satisfying Component	Rationale
ACM_CAP.2	Configuration Items	McAfee performs configuration management on configuration items of the TOE. Configuration management is performed on the TOE and the implementation representation of the TOE. The configuration items are uniquely identified and each release of the TOE has a unique reference.
ADO_DEL.1	Delivery process documentation	McAfee documents the delivery procedure for the TOE to include how components of the TOE are delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained.
ADO_IGS.1	Installation guidance	McAfee documents the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ADV_FSP.1	Functional specification	The externally visible interfaces of the TOE used by the users of the TOE along with the description of the security functions and a correspondence between the interfaces and the security functions from the ST

Assurance Component	Documentation Satisfying Component	Rationale
		are documented by McAfee development evidence.
ADV_HLD.1	Descriptive High Level Design	The subsystems and the communication between the subsystems of the TOE are documented in McAfee development evidence.
ADV_RCR.1	Correspondence analysis	The correspondence is contained in the documents used for ADV_FSP.1 and ADV_HLD.1.
AGD_ADM.1	Administrator guidance	The administrative guidance is detailed to provide descriptions of how administrative users of the TOE can securely administer the TOE using those functions and interfaces detailed in the guidance.
AGD_USR.1	User guidance	User guidance is provided for those roles defined in the TOE that do not have all the authorizations as the administrative role.
ATE_COV.1	Evidence of Coverage	McAfee demonstrates the external interfaces tested during functional testing using a coverage analysis.
ATE_FUN.1	Test plan, procedures, and results	McAfee functional testing documentation contains a test plan, a description of the tests, along with the expected and actual results of the test conducted against the functions specified in the ST.
ATE_IND.2	TOE	McAfee will help meet the independent testing by providing the TOE to the evaluation facility.
AVA_SOF.1	Strength of function analysis	McAfee documents the strength of function associated with any permutational or probabilistic mechanisms satisfies the minimum strength of function claimed in the ST.
AVA_VLA.1	Vulnerability analysis	McAfee documents their vulnerability analysis search for obvious flaws and weaknesses in the TOE.

6.2.2 Rationale for TOE Assurance Requirements

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.

CHAPTER 7

7. Protection Profile Claims

This chapter provides detailed information in reference to the Protection Profile conformance identification that appears in Chapter 1, Section 1.4 Protection Profile Conformance.

7.1 Protection Profile Reference

This Security Target does not claim conformance to any Protection Profile.

7.2 Protection Profile Refinements

This Security Target does not claim conformance to any Protection Profile.

7.3 Protection Profile Additions

This Security Target does not claim conformance to any Protection Profile.

CHAPTER 8

8. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functionality.

8.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each threat and assumption, the security objective(s) that address it.

Table 27 - Threats and Assumptions to Security Objectives Mapping

	O.PROTCT	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.INTEGR	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	O.AUDITS	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.IDAUTH	OE.DATABASE	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW
A.ACCESS													X								
A.DYNMIC												X	X								
A.ASCOPE													X								
A.PROTCT										X											
A.LOCATE										X											
A.MANAGE												X									
A.NOEVIL									X	X	X										
A.NOTRUST										X	X										
A.DATABASE																			X		
T.COMINT	X				X	X		X								X					
T.COMDIS	X				X	X										X					
T.LOSSOF	X				X	X		X													
T.NOHALT		X	X		X	X															
T.PRIVIL	X				X	X															

	O.PROTCT	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.INTEGR	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	O.AUDITS	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.IDAUTH	OE.DATABASE	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW
T.IMPCON				X	X	X			X												
T.SCNCFG		X																			
T.SCNMLC		X																			
T.SCNVUL		X																			
T.FALREC			X																		
T.FALASC			X																		
T.FACCNT														X							
P.DETECT		X												X	X						
P.ANALYZ			X																		
P.MANAGE	X			X	X	X			X		X	X									
P.ACCESS	X				X	X											X	X	X		
P.INTGTY								X												X	
P.PROTCT							X			X						X					
P.ACCACT						X								X							X

8.1.1 Rationale Showing Threats to Security Objectives

The following table describes the rationale for the threat to security objectives mapping.

Table 28 - Threats to Security Objectives Rationale

T.TYPE	Security Objectives Rationale
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions. The O.INTROP objective ensures the TOE has the needed access.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors. The O.INTROP objective ensures the TOE has the proper access to the IT System. The O.PERSON objective ensures that the TOE will managed appropriately.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors. The O.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The O.PHYCAL provides for the physical protection of the TOE hardware and software.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The O.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The O.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The O.INSTAL objective ensures that the TOE is properly installed and operated and the O.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRUST	The TOE can only be accessed by authorized users. The O.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users. The OE.DATABASE objective ensures that access to any mechanisms

T.TYPE	Security Objectives Rationale
	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.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.PROTCT objective addresses this threat by providing TOE self-protection. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDSCAN and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt 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. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The O.INSTAL objective states the authorized administrators will configure

T.TYPE	Security Objectives Rationale
	the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change.
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. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on data received from each data source. The O.IDANLZ objective provides the function that the TOE will 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. The O. IDANLZ objective provides the function 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. The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
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. The O.AUDITS and O.IDSCAN objectives address this policy by requiring collection of audit and Scanner data. The OE.TIME objective supports this policy by providing a time stamp for insertion into the system data records.

T.TYPE	Security Objectives Rationale
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to data received from each data source and appropriate response actions taken. The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners.
P.MANAGE	The TOE shall only be managed by authorized users. The O.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses via the Foundstone Enterprise Manager web interface. The OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH and OE.IDAUTH objectives by only permitting authorized users to access TOE functions. The OE.SD_PROTECTION objective counters this threat via IT Environment protections of the system data trail. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGR objective ensures the protection of data from modification. The OE.AUDIT_PROTECT objective ensures the integrity of audit records in the database generated by the TOE.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The O.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The OE.AUDIT_REVIEW objective provides the ability for administrators to review the audit records generated by the TOE so that accountability for administrator actions can be determined.

8.2 Rationale for Security Functional Requirements (SFRs)

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 29 - TOE SFRs to Security Objectives Mapping

	O.PROTCT	O.IDSCAN	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.INTEGR	O.AUDITS
FAU_GEN.1									X
FIA_UAU.1(1)					X	X			
FIA_ATD.1						X			
FIA_UID.1(1)					X	X			
FMT_MOF.1	X				X	X		X	
FMT_MTD.1	X				X	X			
FMT_SMF.1						X			
FMT_SMR.1						X			
FPT_RVM_SFT.1	X								
FPT_SEP_SFT.1	X								
IDS_SDC.1		X							
IDS_ANL.1			X						
IDS_RDR.1				X	X	X			
IDS_STG.2							X		

The following table provides the detail of TOE security objective(s).

Table 30 - TOE Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. 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_MTD.1]. The TOE protects itself from bypass [FPT_RVM_SFT.1] and interference [FPT_SEP_SFT.1] from subjects within the TSC.
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. A System containing a Scanner is required to collect and store static configuration information of an IT System. The type of configuration information collected must be defined in the ST [IDS_SDC.1].
O.IDANLZ	The Analyzer must accept data from Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future). The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1].
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1(1), FIA_UAU.1(1)]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. 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_MTD.1].
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using

Security Objective	SFR and Rationale
	an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. 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_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The set of management functions to be restricted are identified [FMT_SMF.1].
O.OFLOWS	The TOE must appropriately handle potential System data storage overflows. The System must prevent the loss of system data in the event its trail is full [IDS_STG.2].
O.INTEGR	The TOE must ensure the integrity of all System data. Only authorized administrators of the System may query or add System data [FMT_MTD.1].
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1].

8.2.2 Rationale for Security Functional Requirements of the IT Environment Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each IT Environment security objective, the SFR(s) that address it.

Table 31 - IT Environment SFRs to Security Objectives Mapping

	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.IDAUTH	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW
FAU_SAR.1						X
FAU_STG.2					X	
FIA_UAU.1(2)				X		
FIA_UID.1(2)				X		
FPT_ITT.1		X				
FPT_RVM_OS.1		X				
FPT_SEP_OS.1		X				
FPT_STM.1	X					
IDS_STG.1			X			

The following table provides the detail of TOE security objective(s).

Table 32 - TOE Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
OE.TIME	Time stamps associated with audit and system data records must be reliable [FPT_STM.1].
OE.PROTECT	The IT Environment must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM_OS.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP_OS.1]. The IT Environment also protects information being exchanged between distributed TOE components, which would be another attack vector for interference or tampering [FPT_ITT.1].
OE.SD_PROTECTION	The IT Environment is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion [IDS_STG.1].
OE.IDAUTH	The IT Environment is required to successfully identify and authenticate users of the operating system of the TOE components. [FIA_UAU.1(2), FIA_UID.1(2)].
OE.AUDIT_PROTECT	The IT Environment is required to protect audit records generated by the TOE and stored in the database from unauthorized modification and deletion.
OE.AUDIT_REVIEW	The IT Environment is required to provide a mechanism for administrators to review audit records generated by the TOE and stored in the database.

8.3 Rationale for TOE Summary Specification

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

Table 33 - SFRs to TOE Security Functions Mapping

	Scanning	I&A	Self Protection	MGMT	Audit
FAU_GEN.1					X
FIA_UAU.1(1)		X			
FIA_ATD.1		X			
FIA_UID.1(1)		X			
FMT_MOF.1				X	
FMT_MTD.1				X	
FMT_SMF.1				X	
FMT_SMR.1				X	
FPT_RVM_SFT.1			X		
FPT_SEP_SFT.1			X		
IDS_SDC.1	X				
IDS_ANL.1	X				
IDS_RDR.1	X				
IDS_STG.2	X				

Table 34 - SFR to SF Rationale

SFR	SF and Rationale
FAU_GEN.1	**Audit –** Management actions performed by administrators are audited.
FIA_ATD.1	**I&A** – User security attributes are associated with the user upon successful login via the Foundstone Enterprise Manager.
FIA_UAU.1(1)	**I&A** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FIA_UID.1(1)	**I&A** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.
FMT_MOF.1	**Mgmt** – The User Type identifies the privilege level of the user. The User Type determines the level of ability to alter the scan configuration and parameters.
FMT_MTD.1	**Mgmt** – The User Type identifies the privilege level of the user. The User Type determines the permissions for access to the TSF data.
FMT_SMF.1	**Mgmt** – The management functions that must be provided for effective management of the TOE are defined and described.
FMT_SMR.1	**Mgmt** – The TOE provides the roles specified in the SFR. When a User Account is created or modified, the user type is specified. Global Administrator is implicit for FoundScan Engine users.
FPT_RVM_SFT.1	**Self Protection** – The TOE protects itself from bypass within the TSC by providing well-defined interfaces and ensuring that the security policies are enforced for security-relevant interfaces.
FPT_SEP_SFT.1	**Self Protection** – The TOE protects itself from interference within the TSC by providing well-defined interfaces and ensuring that permissions for each administrator are properly associated with each session.
IDS_SDC.1	**Scanning** – The TOE performs scans of specified systems in order to detect vulnerabilities present on those systems in the areas of access control and service configuration. Scan results are stored in the database.
IDS_ANL.1	**Scanning** – The TOE analyzes the results of the scanning performed to identify known vulnerabilities on those systems. Vulnerability information in stored in the database.
IDS_RDR.1	**Scanning** – The TOE provides the ability for authorized administrators to retrieve reports from the database that describe the vulnerabilities detected on the scanned systems. Access is limited to reports for which each administrator is authorized.

SFR	SF and Rationale
IDS_STG.2	**Scanning** – If the storage space is exhausted, the oldest data is saved and the most recent data is ignored.

8.4 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified TOE SFRs include the appropriate hierarchy and dependencies.

8.4.1 TOE Security Functional Component Hierarchies and Dependencies

The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 35 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No Other Components	FPT_STM.1	Satisfied by the IT Environment
FIA_ATD.1	No Other Components	None	N/A
FIA_UAU.1	No Other Components	FIA_UID.1	Satisfied
FIA_UID.1	No Other Components	None	N/A
FMT_MOF.1	No Other Components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No Other Components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No Other Components	None	N/A
FMT_SMR.1	No Other Components	FIA_UID.1	Satisfied
FPT_RVM_SFT.1	No Other Components	None	N/A
FPT_SEP_SFT.1	No Other Components	None	N/A
IDS_SDC.1	No Other Components	FPT_STM.1	Satisfied by the IT Environment
IDS_ANL.1	No Other Components	FPT_STM.1	Satisfied by the IT Environment
IDS_RDR.1	No Other Components	None	N/A

SFR	Hierarchical To	Dependency	Rationale
IDS_STG.2	No Other Components	None	N/A

8.4.2 IT Environment Security Functional Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified IT Environment SFRs include the appropriate hierarchy and dependencies.

The following table lists the IT Environment SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 36 - IT Environment SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied by the TOE
FAU_STG.2	FAU_STG.1	FAU_GEN.1	Satisfied by the TOE
FIA_UAU.1	No Other Components	FIA_UID.1	Satisfied
FIA_UID.1	No Other Components	None	N/A
FPT_ITT.1	No other components.	None	n/a
FPT_RVM_OS.1	No Other Components	None	n/a
FPT_SEP_OS.1	No Other Components	None	n/a
FPT_STM.1	No other components.	None	n/a
IDS_STG.1	No other components.	None	n/a

8.5 PP Claims Rationale

This Security Target does not claim conformance to any Protection Profile.

8.6 Strength of Function Rationale

The password mechanism in the I&A security function is SOF-basic. SOF-basic is defined in CC Part 1 section 2.3 as: "A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential." Because this ST identifies threat agents with low attack potential, SOF-basic was chosen.

McAfee Foundstone
Foundstone Publication
700-27201–00