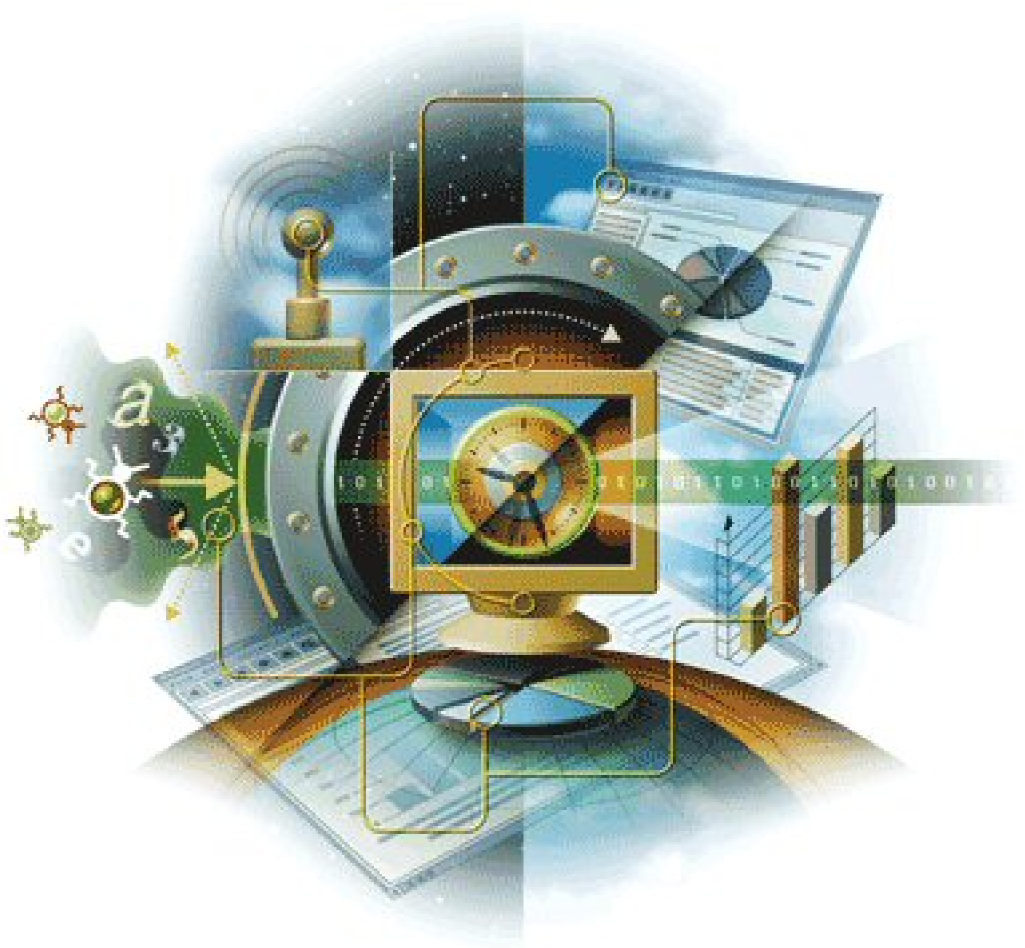
Security Target

Host Intrusion Prevention 6.0.2

and

ePolicy Orchestrator 3.6.1 (Patch 1)



McAfee ®

System Protection

Industry-leading intrusion prevention solutions

McAfee®
Proven Security™

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

ACL	Access Control List
CC	Common Criteria
EAL3	Evaluation Assurance Level 3
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 Host Intrusion Prevention (HIP) v6.0.2 and ePolicy Orchestrator (ePO) v3.6.1 (Patch 1). 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 November 27, 2006. 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 Host Intrusion Prevention (HIP) v6.0.2 and ePolicy Orchestrator (ePO) v3.6.1 (Patch 1) Security Target by defining the Target of Evaluation (TOE).

1.1.1 Security Target

McAfee Host Intrusion Prevention (HIP) v6.0.2 and ePolicy Orchestrator (ePO) v3.6.1 (Patch 1) Security Target, document number SV-0706-001(9), dated April 4, 2007.

1.1.2 TOE Reference

McAfee Host Intrusion Prevention (HIP) v6.0.2 and ePolicy Orchestrator (ePO) v3.6.1. (Patch 1) The system is hereafter collectively referred to as HIP 6.0.2.

1.1.3 Security Target Authors

COACT, Inc.

1.1.4 Evaluation Assurance Level

Assurance claims conform to EAL3 (Evaluation Assurance Level 3) from the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

1.1.5 Keywords

Agent(s)
Agent(s) refer to the HIP 6.0.2 Agents for systems running the Windows operating system.

Exception
Defines a set of attributes that instructs the Agent to not enforce a rule or policy, resulting in an Event not being generated.

Policy File
Each Signature is assigned a Security Level. The Policy File defines the Reaction to take for a specific Security Level. Each Policy File entry includes the Reaction to take if a signature of that severity level occurs.

Reaction
A Reaction is defined in a Policy File. It defines the action (Prevent, Log, or Ignore) the Agent is to take per Event Severity Level (High, Medium, Low, Information).

Severity Level — The available Severity Levels available are: High, Medium, Low, or Information.

Signature — Signatures are patterns that indicate a potential security violation.

Signature File — Agents are installed with a Signature File that contains a list of Signatures. The Agents intercept operating system calls and network packets and compare them to the Signatures File

1.2 TOE Overview

This Security Target defines the requirements for the HIP 6.0.2. The TOE is a host-based intrusion prevention system, designed to protect system resources and applications and includes a host based 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 HIP 6.0.2 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 EAL3. 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

The TOE claims conformance to the Intrusion Detection System System Protection Profile, Version 1.6, dated April 4, 2006.

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 HIP 6.0.2 Component Overview

HIP 6.0.2 is a host-based intrusion prevention system designed to protect system resources and applications. It works to intercept system calls prior to their execution and network traffic prior to their processing. If the HIP Agent determines that a call or packet is symptomatic of malicious code, the call or packet can be blocked and/or an audit log created; if it determines that a call or packet is safe, it is allowed.

There are two components of the TOE:

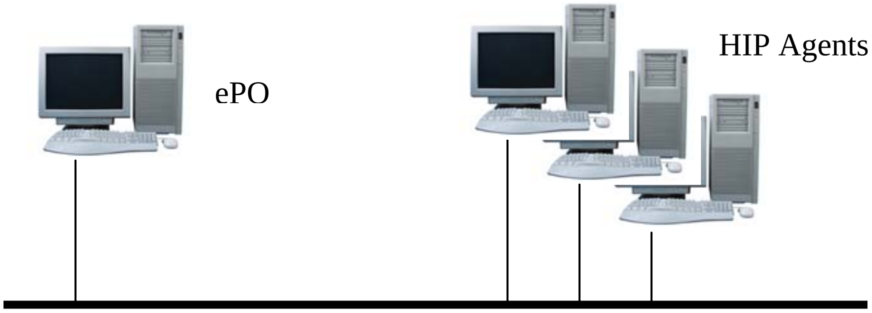
A) HIP 6.0.2 Agents running on any of the following platforms:

   1) Windows 2000 Advanced Server with Service Pack 1, 2, 3, or 4
   2) Windows 2000 Datacenter Server with Service Pack 1, 2, 3, or 4
   3) Windows 2000 Professional with Service Pack 1, 2, 3, or 4
   4) Windows 2000 Server with Service Pack 1, 2, 3, or 4
   5) Windows NT 4.0 Enterprise Server, with Service Pack 6 or 6a
   6) Windows NT Server 4.0 with Service Pack 6 or 6a
   7) Windows NT Workstation 4.0 with Service Pack 6 or 6a
   8) Windows Server 2003 Enterprise with Service Pack 1
   9) Windows Server 2003 Standard with Service Pack 1
   10) Windows Server 2003 Web with Service Pack 1
   11) Windows XP Home with Service Pack 1 or 2
   12) Windows XP Professional with Service Pack 1 or 2

B) ePolicy Orchestrator (ePO) running on any of the following platforms:

   1) Windows 2000 Advanced Server with Service Pack 3 or later
   2) Windows 2000 Server with Service Pack 3 or later
   3) Windows Server 2003 Enterprise
   4) Windows Server 2003 Standard
   5) Windows Server 2003 Web

Figure 1 - HIP 6.0.2 Components



2.1.1 HIP 6.0.2 Windows Agent

The HIP 6.0.2 Windows Agent (hereafter referred to as Agent) provides a protection layer that identifies and prevents malicious attempts to compromise a host. Agent software is installed on the host to be protected. Agents are operating system specific; only the Windows Agent is included in this evaluation.

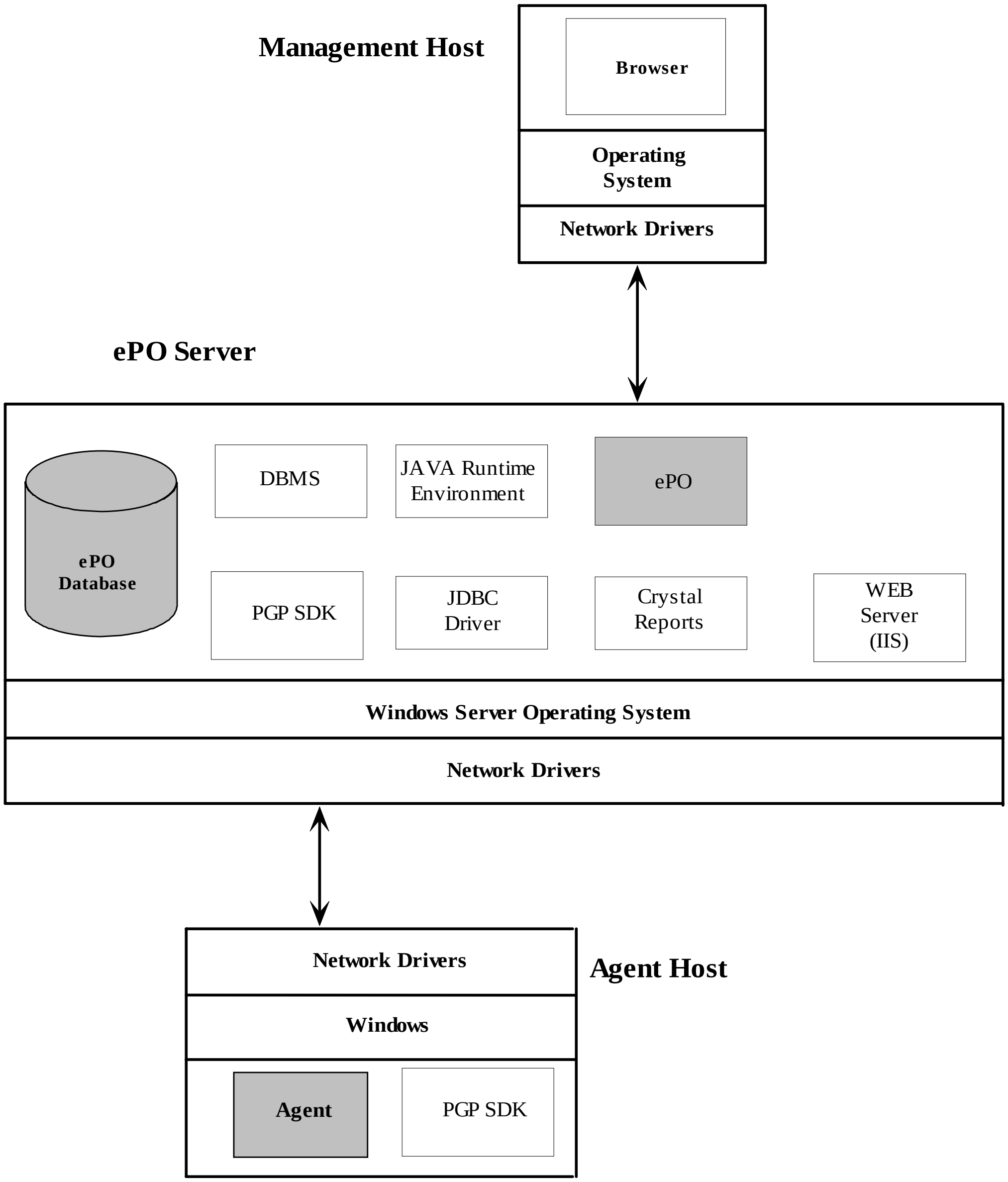
2.1.2 ePolicy Orchestrator (ePO)

In addition to the Agent, the TOE includes ePolicy Orchestrator (ePO) version 3.6.1 (Patch 1). ePO distributes and manages agents that reside on client systems. By using ePO you can manage a large enterprise network. A centralized but distributed architecture allows the Agent software to be centrally managed and yet decrease network traffic required to manage clients. ePO provides the management interface and functionality for the administrators of the TOE. It also provides centralized audit collection and review functionality.

2.2 Physical Boundary

The physical boundary of the TOE includes the Agent software and ePO software. Hardware is not included. The SQL Database and JAVA runtime library, JDBC Driver, HTTP Server and Crystal Reports software that are used by the Management Server are not included in the TOE. The PGP SDK software used on both the Management Server and Agent system for TLS is not included in the TOE. The following figure represents the physical boundary of the TOE. The TOE components are shaded.

Figure 2 - Physical 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 System Protection (SYSPROT)

The Agents are host based intrusion prevention systems designed to protect system resources and applications from attacks. The Agents accomplish this by intercepting operating system calls and comparing them to signatures symptomatic of known attacks and behavioral rules. The Agents also inspect network traffic by comparing packets to signatures symptomatic of known attacks. If a potential security violation is detected, the system call or network traffic may be allowed to proceed or be blocked. An audit event may also be generated.

2.3.2 Audit (AUDIT)

The TOE generates audit records upon detection of a potential security violation or system configuration events. The audit records can be viewed by an authorized user. The TOE audit functionality includes the ability to configure what auditable events actually generate audit records.

2.3.3 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.

2.3.4 Management (MGMT)

The TOE's Management Security Function provides administrator functionality that enables a human user to configure and manage TOE components. Configuration functionality includes enabling a user to modify TSF Data used by the TOE's Security Functional Policies (SFPs). Management functionality includes invocation of TOE functions that effect security functions and security function behavior.

2.4 HIP 6.0.2 Evaluated Configuration

2.4.1 Evaluated Configuration

The Agents are available in multiple variants, each running on a different operating system. However, only the Windows variant is included in this evaluation. The evaluated configuration includes one or more Agents (for one or more of the operating systems); an instance of the Management Server installed with both subsystems of the Management Server software and an additional instance of the Management System Console on a separate system. Specifically the items of the evaluated configuration are:

A) One or more HIP 6.0.2 Windows Agents

B) ePO Server – A single dedicated Windows workstation running ePO v3.6.1 (Patch 1)

2.4.2 ePO Configuration

ePO operates as a distribution system and management system for a client-server architecture offering components for the server part of the architecture (not the clients). The hardware and network components and configuration requirements for the ePO server (outside the scope of the TOE) are listed in the following table.

Table 1 - Hardware and Network Components Required for ePO Server

Hardware and Network Environment Requirements	
Free disk space	500MB
Processor	Intel Pentium II-class or higher; 450MHz or higher
Memory	512mb RAM

Hardware and Network Environment Requirements	
Monitor	1024 x 768; 256 color, VGA monitor
NIC	Network Interface Card with 100mb capacity
File system	NTFS partition
IP Address	Static IP Address

The ePO server also requires a DBMS that is part of the IT environment.

Software and operating system components (outside the scope of the TOE) that are required for the ePO server are listed in the following table.

Table 2 - Software Components and Requirements for the ePO Server

Software Components and Requirements of the Environment	
DBMS (one of the following is required)	Microsoft SQL Server 2000 Standard with SP 3
	Microsoft SQL Server 2000 Enterprise with SP 3
	Microsoft SQL Server 7 Standard with SP 3 or 4
	Microsoft SQL Server 7 Enterprise with SP 3 or 4
Browser	Microsoft Internet Explorer v6.0
Domain Controller	The server must have a trust relationship with the Primary Domain Controller (PDC) on the network.
JAVA Runtime Environment	JRE 1.4.2_09
JDBC Driver	jTDS driver 1.2
Crystal Reports	8.0/8.5
Agent-Server Communication	Apache 2.0.54
Web Server	Apache 2.0.54
Application Server	Tomcat 4.1.30
TLS	PGP SDK 3.5.3

In addition, the following configuration options must be selected for the evaluated configuration:

A) All user accounts defined in ePO must specify ePO authentication (rather than NT authentication)

2.4.3 HIP 6.0.2 Functionality Not Included in the Evaluation

The functionality of HIP 6.0.2 that is not included in the evaluation is described below:

A) Firewall functionality (some government users require firewall functionality to be disabled unless it has been evaluated against one of the firewall PPs at EAL4 or Medium Robustness). Application Blocking functionality is associated with the firewall functionality and is also excluded.

B) Custom signatures and policies.

C) Importing configurations.

D) HIP Solaris Agents.

E) HIP Linux Agents.

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 3 - TOE Data

Name	Description	AD	UA	GE
Application Protection Lists	List of processes that are explicitly enabled or disabled for performing user-level hooking			X
Console User Account Permissions	List of sites that Site Administrators and Site Reviewers may access		X	
Console User Account Type	Each user account defined in ePO must be defined as a Global Administrator, Global Reviewer, Site Administrator or Site Reviewer.		X	
Console User ID	Userid for a console user	X		
Console User Password	Password for a console user	X		
Exceptions	Mechanism to refine the signature matches to eliminate false positives			X
IPS Options	Per-Agent mode for operation of the IPS processing, may be ON for normal operation or configured for Adaptive mode			X
IPS Policies	Used to configure the reaction to signature matches			X
IPS Protection Policies	Per-Agent reaction specified for each of the severity levels that can be specified in signatures.			
Signatures	Collection of system call events or network traffic indicative of malicious code			X
Sites	Logical grouping of systems that Site Administrators and Site Reviewers may be granted permissions for			
System Event Audit Configuration	Configuration to determine which management actions create audit events			X
Trusted Applications	Mechanism to refine the signature matches to eliminate false positives			X

Legend: AD=Authentication data; UA=User attribute; GE=Generic Config. 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. HIP 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 direct the system calls and network packets to the TOE for examination.

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 workstation hardware provides virtual memory and process separation which the workstation 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 4 - 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 5 - 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 6 - 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.

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 7 - 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.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected.

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

Table 8 - 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.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

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 9 - 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 IDS data 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.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
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.

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 10 - 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.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.IDANLZ	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of the System functions.
O.INTEGR	The TOE must ensure the integrity of all audit and System data.

4.2 Security Objectives for the IT Environment

The TOEs operating environment must satisfy the following objectives.

Table 11 - Security Objectives of the IT 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.

Objective	Definition
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.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.AUDIT_SORT	The IT Environment will provide the capability to sort the audit information.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data.

.

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 2.1* 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 12 - TOE SFRs

Functional Components	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SEL.1	Selective audit
FAU_STG.4	Prevention of audit data loss
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_SMR.1	Security roles
FPT_ITT.1(1)	Basic Internal TSF Data Transfer Protection
IDS_SDC.1	System Data Collection
IDS_ANL.1	Analyzer analysis
IDS_RCT.1	Analyzer react
IDS_RDR.1	Restricted Data Review
IDS_STG.1(1)	Guarantee of System Data Availability

Functional Components	
IDS_STG.2	Prevention of System data loss

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*.

Table 13 - Auditable Events

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	*Object IDS, Requested access*
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FIA_UAU. 1	All use of the authentication mechanism	*User identity, location*
FIA_UID.1	All use of the user identification mechanism	*User identity, location*
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	*User identity*

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 additional information specified in the Details column of the table above.*

5.1.1.2 Security audit review (FAU_SAR)

FAU_SAR.1.1 The TSF shall provide *Global Administrator, Global Reviewer, Site Administrator or Site Reviewer* with the capability to read *all information* from the audit records.

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

5.1.1.3 FAU_SAR.2 Restricted Audit Review

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

5.1.1.4 FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type;

b) *no additional attributes*.

5.1.1.5 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall overwrite the oldest stored audit records and *send an alarm* if the audit trail is full.

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 Account Type*; and

b) *No other security attributes*.

5.1.2.2 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.2.3 User identification (FIA_UID)

FIA_UID.1.1 The TSF shall allow *no actions* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

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 *authorised System administrators*.

Application Note: Authorised System Administrators in this context are Site Administrators (limited to the sites they have permission for) and Global Administrators (all Agents).

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 and audit 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 14 - TSF Data Access Permissions

TSF Data	Global Administrator	Global Reviewer	Site Administrator	Site Reviewer
Application Protection Lists	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
Audit Data	Query	Query	Query all audit data	Query all audit data
Exceptions	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
IPS Options	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
IPS Policies	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
IPS Protection Policies	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
Signatures	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
System Data	Query, Modify	Query	Query all system data	Query all system data
System Event Audit Configuration	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
Trusted Applications	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)

TSF Data	Global Administrator	Global Reviewer	Site Administrator	Site Reviewer
User Account Permissions	Query, Modify	Query	n/a	n/a
User Account Type	Query, Modify	Query	n/a	n/a
User Accounts	Query, Modify	Query	Query	Query
User Passwords	Modify	n/a	n/a	n/a

5.1.3.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the **following** roles*: authorised administrator, authorised System administrators, Global Reviewers and Site Reviewers*.

Application Note: Authorised System Administrators in this context are Site Administrators (limited to the sites they have permission for) and Global Administrators (all Agents). Authorised administrators are Global Administrators.

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_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1(1) The TSF shall protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE.

Application Note: This iteration requires the TOE to use IT Environment-provided functionality to protect communication between TOE components. Having the functionality in the IT Environment is not sufficient since the TOE is not necessarily utilizing it.

5.1.5 IDS Component Requirements (IDS)

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) detected malicious code; 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 15 - System Data Collection Events and Details

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	None

Component	Event	Details
IDS_SDC.1	Detected malicious code	Location, identification of code

5.1.5.2 IDS_ANL.1 Analyser analysis

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

a) signature; and

b) *no other analytical functions*.

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. *Severity level*.

5.1.5.3 IDS_RCT.1 Analyser react

IDS_RCT.1.1 The System shall send an alarm to *the audit log* and take *optionally block the system call or network packet from proceeding (if configured to do so)* when an intrusion is detected.

5.1.5.4 IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1 The System shall provide *Global Administrators, Global Reviewers, Site Administrators, and Site Reviewers* with the capability to read *the system data listed in the table below* from the System data.

Table 16 - System Data Access

User Type	Access
Global Administrators, Global Reviewers	Full access
Site Administrators, Site Reviewers	System Data originating from Agents who are included in the sites the user has permissions for

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.

5.1.5.5 IDS_STG.1 Guarantee of System Data Availability

IDS_STG.1.1(1) The System shall protect the stored System data from unauthorised deletion **via interfaces within the TSC**.

IDS_ STG.1.2(1) The System shall protect the stored System data from modification **via interfaces within the TSC**.

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(1) The System shall ensure that *the full number of the currently stored* System data will be maintained when the following conditions occur: System data storage exhaustion.

Application Note: This iteration addresses access to the database from within the TSC.

5.1.5.6 IDS_STG.2 Prevention of System data loss

IDS_STG.2.1 The System shall ignore System data and send an alarm 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 17 - IT Environment SFRs

Functional Components	
FAU_SAR.3	Selectable audit review
FAU_STG.2	Guarantees of audit data availability
FPT_ITT.1(2)	Basic Internal TSF Data Transfer Protection
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
IDS_STG.1(2)	Guarantee of System Data Availability

5.2.1 Security audit (FAU)

5.2.1.1 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform sorting of audit data based on *date and time, subject identity, type of event, and success or failure of related event*.

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 unauthorised deletion.

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

FAU_STG.2.3 The TSF shall ensure that *the number corresponding to 80% of the configured audit log file size of* audit records will be maintained when the following conditions occur: audit storage exhaustion.

5.2.2 Protection of the TSF (FPT)

5.2.2.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1(2) The TSF shall protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE.

Application Note: This iteration requires the IT Environment to provide functionality to protect communication between TOE components. This functionality is invoked by the TOE.

5.2.2.2 FPT_RVM.1 Non-bypassability of the TSP

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

5.2.2.3 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

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

5.2.2.4 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.2.3 IDS Component Requirements (IDS)

5.2.3.1 IDS_STG.1 Guarantee of System Data Availability

IDS_STG.1.1(2) The System shall protect the stored System data from unauthorised deletion **via interfaces outside the TSC**.

IDS_ STG.1.2(2) The System shall protect the stored System data from modification **via interfaces outside the TSC**.

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(2) The System shall ensure that *the full number of the currently stored* System data will be maintained when the following conditions occur: System data storage exhaustion.

Application Note: This iteration addresses access to the database from outside the TSC.

5.3 Strength of Function for the TOE

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

5.4 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL3. These requirements are summarised in the following table:

Table 18 - TOE Security Assurance Requirements

Assurance Class	Component ID	Component Title
Configuration management	ACM_CAP.3	Authorisation controls
	ACM_SCP.1	TOE CM coverage
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification

Assurance Class	Component ID	Component Title
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

CHAPTER 6

6. TOE Summary Specification

6.1.1 System Protection (SYSPROT)

The Agents are host based intrusion detection/prevention systems designed to detect malicious code and protect system resources and applications from attacks. The Agents accomplish this by intercepting operating system calls and network packets (both incoming and outgoing) and comparing them to signatures symptomatic of malicious code.

The Agent software includes Policy rules that reference a list of Signatures. Signatures are system call and network packet patterns that are symptomatic of a potential security violation. The Agents compare system calls and network packets against the Signatures referenced by Policies enabled on that Agent. If the system call or network packet matches a signature, a potential security violation has been detected.

Each Signature in the Signature File is assigned a Severity Level (Information, Low, Medium or High). Each Severity Level defines the potential danger an occurrence of the Signature poses to a host. On a match of a Signature, the reaction taken by an Agent is defined by the Agent's Protection Policy. If a potential security violation is detected, the reactions configured by the administrator for that Agent are performed automatically by the TOE. Possible reactions are:

A) Generate an audit event

B) Block the system call or network packet

C) Allow the system call or network packet to proceed

If no signatures match, the call or packet is allowed to proceed. When multiple signatures match, the highest reaction is taken.

Exceptions and Trusted Applications may be defined for each Policy to override the Signatures. The exception feature enables administrators to weed out false positive alerts, minimize needless data flowing to the console, and ensures that the alerts are legitimate security threats. A trusted application is an application that is known to be safe in the end user environment, has no known vulnerabilities, and is allowed to perform operations that would otherwise be prevented. Application Protection may also be configured for Policies to control what applications are permitted to perform user-level process hooking. Explicit lists of permitted and blocked processes may be configured. If a process is not included in either list, then the hook is permitted if the process is a Windows service and blocked otherwise.

The Agent's IPS Options Policy defines the overall operation of the Agent. An Agent may be:

A) operating normally (On),

B) automatically generating client rules that permit all operations that would normally trigger an event (Adaptive).

An Agent is typically put into Adaptive or Learning mode when the Agent is first installed. This assists the Administrator in reviewing the activity on the system to customize the signatures and policies for that system. Once the customization is complete, the system is configured to operate normally.

Security audit events are generated on the Agent systems and communicated to ePO, where they are saved and reviewed via the same mechanism used for audit events (see AUDIT below). Each audit events includes a timestamp, the type of event, and Agent identity. For events involving signatures, the event also identifies the matching signature, user id (if applicable), process name (if applicable), severity level, and the reaction taken.

The transfer of information between the Agent systems and ePO must be protected from disclosure and modification in order to ensure the integrity of the information exchanged between those components. The TOE invokes functionality provided by the IT Environment to protect all communication between the components.

6.1.2 Audit (AUDIT)

The TOE generates audit records upon detection of a potential security violation or system configuration events. The audit records can be viewed by an authorized user using ePO. The TOE audit functionality includes the ability to define excluded auditable events.

The TOE's Audit Security Function includes the following functionality and each is described below.

A) Audit Record Generation

B) Viewing Audit Records

6.1.2.1 Audit Record Generation

The TOE monitors system activity and creates an Event upon detection of a potential security violation. The TOE also generates Events reporting TOE access and management activity. The table included with FAU_GEN.1 specifies the audit events related to management activities and the information included with each. Individual auditable events may be enabled or disabled by the administrator via the management interface.

Both audit records and system data records are saved in a database on ePO for later review (the DBMS is part of the IT Environment). Audit information is saved in the database in a table with a fixed number of rows (800,000) until the table space is exhausted, at which time the oldest 20% of the rows is discarded (ensuring that the most recent 80% is always maintained). Anytime the audit space is exhausted and the oldest records are discarded, an SNMP trap is generated as an alarm.

The number of rows reserved for the audit records is intended to store approximately one year's worth of audit records based upon the following assumptions:

A) Up to 20 administrators of any type

B) Each administrator performs up to 10 auditable management actions each day for each of 11 distinct auditable event types.

For system data, information is added to the database until disk space is exhausted. Administrators are provided guidance concerning backups of the database in order to avoid disk space exhaustion. However, if this situation does occur, any new system data records are discarded while the older system records are preserved within the database. If disk space is exhausted, an SNMP trap is generated as an alarm. The TOE does not provide any interface through which system data may be modified or deleted. The TOE does provide an interface to issue SQL queries to the DBMS; this interface prevents any SQL commands that could modify the system data.

6.1.2.2 Viewing Audit Records

ePO provides the functionality that enables Authorized Console Users to view audit records stored in the database. The TOE restricts access of audit records to users who have been properly configured with a User Account and who have successfully logged into ePO.

6.1.3 Identification and Authentication (I&A)

ePO provides a GUI application that allows an Authorised Console User to monitor TOE activity and modify TSF Data. 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 a Console User type associated with their user account that defines the functionality the user is allowed to perform. Site Administrator and Site Viewer types also have associated permissions to access specific sites.

Authentication is required (cannot be bypassed) and configured when the Console User Account is created. The TOE implements restrictions on the passwords. Guidance directs the Site Administrator to specify passwords that are a minimum of 10 characters and are not dictionary words. The TOE also protects the password from visual detection by echoing back asterisks (“*”) for the entered passwords.

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. Configuration functionality includes enabling a user to modify TSF Data used by the TOE’s Security Functional Policies (SFPs). Management functionality includes invocation of TOE functions that effect security functions and security function behavior.

The TOE provides the following management functions:

A) Management of console users,

B) Management of Policies,

C) Management of Exceptions,

D) Management of Application Protection Lists,

E) Management of Trusted Applications, and

F) Management of Agent Mode and operation.

Each Console User Account must be defined to the TOE. In addition to a login name and password, a Console User includes two security attributes: User Type and Permissions. A User Type defines one of four roles: Global Administrator, Site Administrator, Global Reviewer or Site Reviewer. Administrators may access and change configuration data and audit information while Reviewers may only read configuration data and audit information. Permissions apply to Site Administrator and Site Reviewer by explicitly specifying what sites (and systems within those sites) the roles may access.

Management capabilities for each role are described in the following table.

Table 19 - Management Capabilities

TSF Data	Global Administrator	Global Reviewer	Site Administrator	Site Reviewer
Application Protection Lists	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
Audit Data	Query	Query	Query all audit data	Query all audit data
Exceptions	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
IPS Options	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
IPS Policies	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
IPS Protection Policies	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
Signatures	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
System Data	Query, Modify	Query	Query all audit data	Query all audit data
System Event Audit Configuration	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)
Trusted Applications	Query, Modify	Query	Query, Modify (only the Agents the user account has permissions for)	Query (only the Agents the user account has permissions for)

TSF Data	Global Administrator	Global Reviewer	Site Administrator	Site Reviewer
User Account Permissions	Query, Modify	Query	n/a	n/a
User Account Type	Query, Modify	Query	n/a	n/a
User Accounts	Query, Modify	Query	Query	Query
User Passwords	Modify	n/a	n/a	n/a

Authorised System administrators (Global Administrators and Site Administrators) modify the behaviour of System data collection, analysis and reaction by installing the Agent on target systems, defining the mode of operation of the Agent (normal or adaptive) and configuring the policies.

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 20 - Assurance Measures

Assurance Component	Documentation Satisfying Component	Rationale
ACM_CAP.3	Configuration management documentation	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.
ACM_SCP.1	Configuration management documentation	McAfee includes all TOE components and relevant documents (including evidence generated for the CC evaluation) within their configuration management system.
ADO_DEL.1	Delivery process documentation	McAfee documents the delivery procedure for the TOE to include the procedure on how to download certain components of the TOE from the McAfee website and how certain components of the TOE are physically 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

Assurance Component	Documentation Satisfying Component	Rationale
		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 are documented by McAfee development evidence.
ADV_HLD.2	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.2.
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.
ALC_DVS.1	Development security documentation	McAfee implements processes and procedures for the development environment that provide security for the development process.
ATE_COV.2	Coverage analysis	McAfee demonstrates the external interfaces tested during functional testing using a coverage analysis.
ATE_DPT.1	Depth analysis	McAfee demonstrates the subsystem interfaces tested during functional testing using a depth 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	Test plan, procedures, and results	McAfee will help meet the independent testing by providing the TOE to the evaluation facility.
AVA_MSU.1	Administrator and user guidance	The administrative and user guidance referenced for AGD_ADM.1 and AGD_USR.1 satisfy the requirements for this component also.
AVA_SOF.1	Strength of function	McAfee documents the strength of function

Assurance Component	Documentation Satisfying Component	Rationale
	analysis	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 EAL3 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 claims conformance to the Intrusion Detection System System Protection Profile, Version 1.6, dated April 4, 2006.

7.2 Protection Profile Refinements

In accordance with the errata sheets of the PP, the following SFRs have been moved to the IT Environment:

A) FPT_STM.1

B) FPT_SEP.1

C) FPT_RVM.1

D) FAU_STG.2

E) FAU_SAR.3

In keeping with the rationale expressed in the errata sheets of the PP, IDS_STG.1 has been iterated and levied on both the TOE and the IT Environment.

In accordance with NIAP Precedent PD-0097, the following items have been deleted:

A) FIA_AFL.1

B) FPT_ITA.1

C) FPT_ITC.1

D) FPT_ITI.1

E) O.EXPORT

Also in accordance with NIAP Precedent PD-0097, iterations of FPT_ITT.1 have been added to the TOE and the IT Environment. The functionality to protect communication is provided by a third-party package (PGP SDK) that is not modified in any way by McAfee. PGP SDK executes as a DLL that is called from the TOE to protect communication between TOE components.

7.3 Protection Profile Additions

In accordance with the errata sheets of the PP, the following IT Environment objectives have been added to the ST:

A) OE.TIME

B) OE.PROTECT

C) OE.AUDIT_PROTECTION

D) OE.AUDIT_SORT

The mappings to threats, assumptions, and policies for these added objectives are also in accordance with the errata sheets of the PP.

OE.SD_PROTECTION has been added to the IT Environment objectives, corresponding to the iteration of IDS_STG.1 on the IT Environment.

The Evaluation Assurance Level has been changed to EAL3.

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 21 - Threats and Assumptions to Security Objectives Mapping

	O.PROTCT	O.IDSCAN	O,IDSENS	O.IDANLZ	O,RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	OE.TIME	OE.PROTECT	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.SD_PROTECTION
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							
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	X													
T.PRIVIL	X						X	X													
T.IMPCON						X	X	X				X									
T.INFLUX									X												X
T.FACCNT										X											

	O.PROTCT	O.IDSCAN	O,IDSENS	O.IDANLZ	O,RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	OE.TIME	OE.PROTECT	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.SD_PROTECTION
T.SCNCFG		X																			
T.SCNMLC		X																			
T.SCNVUL		X																			
T.FALACT					X																
T.FALREC				X																	
T.FALASC				X																	
T.MISUSE			X																		
T.INADVE			X																		
T.MISACT			X																		
P.DETECT		X	X							X							X				
P.ANALYZ				X																	
P.MANAGE	X					X	X	X				X		X	X						
P.ACCESS	X						X	X											X		X
P.ACCACT								X		X							X			X	
P.INTGTY											X										
P.PROTCT									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 22 - 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.

T.TYPE	Security Objectives Rationale
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.
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.

T.TYPE	Security Objectives Rationale
	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, O.IDSENS, 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 the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle. The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows. The OE.SD_PROTECTION objective counters this threat via IT Environment protections of the audit trail.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected. The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.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. The ST will state whether this threat must be addressed by a Scanner.
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. The ST will state whether this threat must be addressed by a Scanner.
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. The ST will state whether this threat must be addressed by a Scanner.

T.TYPE	Security Objectives Rationale
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity. The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS 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 IDS 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.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors. The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors. The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.MISACT	Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors. The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
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, O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, Sensor, and Scanner data. The OE.TIME objective supports this policy by providing a time stamp for insertion into the audit records.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken. The 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

T.TYPE	Security Objectives Rationale
	objective addresses this policy by providing TOE self-protection.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.AUDIT_PROTECTION and OE.SD_PROTECTION objectives counter this threat via IT Environment protections of the audit trail. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The OE.TIME objective supports this policy by providing a time stamp for insertion into the audit records. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The OE.AUDIT_SORT objective supports this policy by providing a mechanism for administrators to effectively review the audit logs.
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.
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.

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 23 - TOE SFRs to Security Objectives Mapping

	O.PROTCT	O.IDSCAN	O,IDSENS	O.IDANLZ	O,RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR
FAU_GEN.1										X	
FAU_SAR 1						X					
FAU_SAR.2							X	X			
FAU_SEL.1						X				X	
FAU_STG.4									X	X	
FIA_UAU.1							X	X			

	O.PROTCT	O.IDSCAN	O,IDSENS	O.IDANLZ	O,RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR
FIA_ATD.1								x			
FIA_UID.1							x	x			
FMT_MOF.1	x						x	x			
FMT_MTD.1	x						x	x			x
FMT_SMR.1								x			
FPT_ITT.1(1)											x
IDS_SDC.1		x	x								
IDS_ANL.1				x							
IDS_RCT.1					x						
IDS_RDR.1						x	x	x			
IDS_STG.1(1)	x						x	x	x		x
IDS_STG.2									x		

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

Table 24 - 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 and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The System 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(1)].
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.IDSENS	The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS. A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. These events must be defined in the ST [IDS_SDC.1].

Security Objective	SFR and Rationale
O.IDANLZ	The Analyzer must accept data from IDS Sensors or IDS 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.RESPON	The TOE must respond appropriately to analytical conclusions. The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SEL.1]. 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 TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. 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, 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 and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1(1)].
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The 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 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 and audit 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 System 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(1)].
O.OFLOWS	The TOE must appropriately handle potential audit and System data storage overflows. The TOE must prevent the loss of audit data in the event the its audit trail is full [FAU_STG.4]. The System must prevent the loss of audit data in the event the audit

Security Objective	SFR and Rationale
	trail is full [IDS_STG.2]. The System 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(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]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event the audit trail is full [FAU_STG.4].
O.INTEGR	The TOE must ensure the integrity of all audit and System data. Only authorized administrators of the System may query or add audit and System data [FMT_MTD.1]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1(1)]. The System must protect the collected data from modification and ensure its integrity when the data is transmitted between distributed TOE components [FPT_ITT.1(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 25 - IT Environment SFRs to Security Objectives Mapping

	OE.TIME	OE.PROTECT	OE.AUDIT_PROTECTION	OE.AUDIT_SORT	OE.SD_PROTECTION
FAU_SAR.3				X	
FAU_STG.2			X		
FPT_ITT.1(2)		X			
FPT_RVM.1		X			
FPT_SEP.1		X			
FPT_STM.1	X				
IDS_STG.1(2)					X

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

Table 26 - TOE Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
OE.TIME	Time stamps associated with an audit record 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.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.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(2)].
OE.AUDIT_PROTECTION	The IT Environment is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion [FAU_STG.2].
OE.AUDIT_SORT	The IT Environment is required to provide a mechanism for the administrator to sort audit logs so that they may be reviewed effectively [FPT_SAR.3].
OE.SD_PROTECTION	The IT Environment is required to protect the System data from any modification and unauthorized deletion via interfaces outside the TSC, as well as guarantee the availability of the data in the event of storage exhaustion [IDS_STG.1(2)].

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 27 - SFRs to TOE Security Functions Mapping

	AUDIT	I&A	MGMT	SYSPROT
FAU_GEN.1	X			
FAU_SAR.1	X			
FAU_SAR.2	X			
FAU_SEL.1	X			
FAU_STG.4	X			
FIA_UAU.1		X		
FIA_ATD.1		X		
FIA_UID.1		X		
FMT_MOF.1			X	

	AUDIT	I&A	MGMT	SYSPROT
FMT_MTD.1			X	
FMT_SMR.1			X	
FPT_ITT.1(1)				X
IDS_SDC.1				X
IDS_ANL.1				X
IDS_RCT.1				X
IDS_RDR.1	X			
IDS_STG.1(1)	X			
IDS_STG.2	X			

Table 28 - SFR to SF Rationale

SFR	SF and Rationale
FAU_GEN.1	**Audit** – As management events occur, the TOE generates audit records.
FAU_SAR.1	**Audit** - Authorized Console Users are given access to all the audit event records.
FAU_SAR.2	**Audit** – Audit review access is controlled by the TSF and limited to authorized users. Access is determined by the security attributes of the console user type and permissions.
FAU_SEL.1	**Audit** – Audit generation includes the ability to selectively audit based on audit event type. Auditing of specific security events is controlled by Exceptions and IPS Reactions.
FAU_STG.4	**Audit** – When the space for audit records is exhausted, the oldest 20% of the information is deleted and an SNMP trap is generated recording the fact that records were deleted.
FIA_ATD.1	**I&A** – User security attributes are associated with the user upon successful login.
FIA_UAU.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	**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.

SFR	SF and Rationale
FMT_MOF.1	**Mgmt** – The User Type identifies the privilege level of the console user. System administrators modify the behaviour of the IDS functions by determining the systems on which the TOE is installed and configuring the Agents on those systems.
FMT_MTD.1	**Mgmt** – The User Type identifies the privilege level of the console user. Appropriate privileges are provided to the various user types for management of Agents and Console Users. Note that the SFR describes management functionality in terms of querying and modifying all TOE data other than system data and audit data. Since this description does not explicitly address the ability to add or delete data (e.g., console users), the ST author interprets "modify" in this instance to include creation and deletion of TOE data where appropriate.
FMT_SMR.1	**Mgmt** – The TOE provides the roles specified in the SFR. When a Console User Account is created or modified, the user must specify the user type of the console user.
FPT_ITT.1(1)	**Sysprot** – Whenever information is communicated between distributed TOE components, the TOE invokes IT Environment-provided functionality to protect the information from modification and disclosure.
IDS_SDC.1	**Sysprot** – The Agents detect malicious code by examining system calls. Upon detection, and audit is generated. Agents also generate events when they are started or stopped.
IDS_ANL.1	**Sysprot** – The Agents detect malicious code by comparing system calls to signatures of known malicious attacks. Upon detection, and audit is generated.
IDS_RCT.1	**Sysprot** – The Agents detect malicious code by comparing system calls to signatures of known malicious attacks. Upon detection, and audit is generated and the system call may be blocked (as configured by the administrator).
IDS_RDR.1	**Audit** – Authorized Console Users are given access to all the system data records.
IDS_STG.1(1)	**Audit** – The TOE does not provide any mechanism to modify or delete saved system data. If storage space for system data is exhausted, the oldest records are maintained and new records are discarded.
IDS_STG.2	**Audit** – When the space for audit records is exhausted, the new system data is discarded and an SNMP trap is generated recording the fact.

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 29 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No Other Components	FPT_STM.1	Satisfied by the IT Environment
FAU_SAR.1	No Other Components	FAU_GEN.1	Satisfied
FAU_SAR.2	No Other Components	FAU_SAR.1	Satisfied
FAU_SEL.1	No Other Components	FAU_GEN.1 FMT_MTD.1	Satisfied Satisfied
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied by FAU_STG.2 in 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	See the note following the table Satisfied
FMT_MTD.1	No Other Components	FMT_SMF.1 FMT_SMR.1	See the note following the table Satisfied
FMT_SMR.1	No Other Components	FIA_UID.1	Satisfied
FPT_ITT.1	No Other Components	None	N/A
IDS_SDC.1	No Other Components	None	N/A
IDS_ANL.1	No Other Components	None	N/A
IDS_RCT.1	No Other Components	None	N/A
IDS_RDR.1	No Other Components	None	N/A
IDS_STG.1	No Other Components	None	N/A
IDS_STG.2	No Other Components	None	N/A

Note concerning FMT_SMF.1 - Prior to the publication and verification of the IDS System PP, International Interpretation #65 was finalized. This interpretation introduced a new family of Security Management requirements, Specification of Management Functions (FMT_SMF). While this should not normally affect dependency rationale, that interpretation introduces dependencies from FMT_MOF.1 and FMT_MTD.1, both contained in this Security Target. Hence, it seems as though some FMT_MSA security requirements should be added to this Security Target to fulfill those dependencies. However, while the IDS System PP is clearly intended to ensure that certain security management functions are controlled if they are made available, it is not evident from the IDS System PP which, if any, of those security management functions must be present in the first place. This Security Target identifies all applicable security management functions in the TOE and explains how they are appropriately controlled and it is effectively unnecessary to introduce a security functional requirement to demand that certain security management functions must be present.

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 30 - IT Environment SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_SAR.3	No other components.	FAU_SAR.1	Satisfied
FAU_STG.2	FAU_STG.1	FAU_GEN.1	Satisfied
FPT_ITT.1	No other components.	None	n/a
FPT_RVM.1	No other components.	None	n/a
FPT_SEP.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

The rationale for the Protection Profile conformance claims is defined in Chapter 7, Section 7.4 Protection Profile Rationale.

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.