Symantec Corporation
Symantec Critical System Protection v5.0.5

Security Target

Document Version 1.0

Prepared for:

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014-2132
Phone: (408) 517 8000
Fax: (408) 517 8186

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2/22/2006	Amy Nicewick	Initial draft.
0.2	2/27/2006	Amy Nicewick	Changes made to address pre-listing verdicts.
0.3	3/7/2006	Amy Nicewick	Changes made to address CSE comments.
0.4	5/19/2006	Amy Nicewick	Changes made to address verdicts.
0.5	8/2/2006	Amy Nicewick	Changes made to address verdicts of 7/19/2006.
0.6	8/15/2006	Amy Nicewick	Changes made to address verdicts of 8/11/2006.
1.0	10/31/2006	Amy Nicewick	Changes made to reflect final version.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the Symantec Critical System Protection v5.0.5. The Symantec Critical System Protection v5.0.5 is an intrusion detection and intrusion prevention system. It collects information about suspicious activity, and implements access control to prevent unauthorized access to system resources.

1.1 Purpose

This ST contains the following sections:

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- Security Environment (Section 3) – Describes the threats and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target, Target of Evaluation (TOE) and Common Criteria (CC) Identification and Conformance

Table 1 - ST, TOE, and CC Identification and Conformance

ST Title	Symantec Corporation Symantec Critical System Protection v5.0.5 Security Target
ST Version	Version 1.0, 10/31/2006
Author	Corsec Security, Inc. Amy Nicewick and Adam O'Brien
TOE Identification	Symantec Critical System Protection v5.0.5
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.3, [August 2005] (aligned with ISO/IEC 15408:2005); CC Part 2 extended; CC Part 3 augmented; PP claim (none); Parts 2 and 3 Interpretations from the Interpreted CEM as of 10/31/2006 were reviewed, and no interpretations apply to the claims made in this ST.
Protection Profile (PP) Identification	None
Evaluation Assurance Level (EAL)	EAL 2 Augmented with ALC_FLR.1
Keywords	Intrusion Detection, Intrusion Prevention, SCSP

1.3 Conventions, Acronyms, and Terminology

1.3.1 Conventions

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

The CC allows for several operations to be performed on security requirements: assignment, refinement, selection and iteration. All of these operations are used within this ST. These operations are presented in the same manner in which they appear in Parts 2 and 3 of the CC with the following exceptions:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [<u>*underlined italicized text within brackets*</u>].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parenthesis following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

1.3.2 Acronyms

The acronyms used within this ST are described in Section 9 – “Acronyms.”

1.3.3 Terminology

The term “operator” is defined in this document to include only those individuals who manage the TOE and manage the TOE Security Function (TSF) data.

The term “user” is defined in this document to include any individuals who access the host system on which the TOE is installed.

2 TOE Description

This section provides a general overview of the TOE as an aid to understanding the general capabilities and security requirements provided by the TOE. The TOE description provides a context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

Symantec Critical System Protection (SCSP) is a host-based Intrusion Detection and Intrusion Prevention (IDP) system. Intrusion detection capabilities allow suspicious activity to be identified and reported. Intrusion prevention capabilities mediate access to system resources, thereby preventing attacks from occurring. This class of product provides host-based intrusion detection and prevention on protected system devices and components. These products protect Information Technology (IT) components such as servers, local and remote workstations, and databases. Host-based IDPs are implemented as agent software running on these servers and workstations. These agents are managed from a central console through a management server. Figure 1 below shows the details of the deployment configuration of the Symantec Critical System Protection v5.0.5.

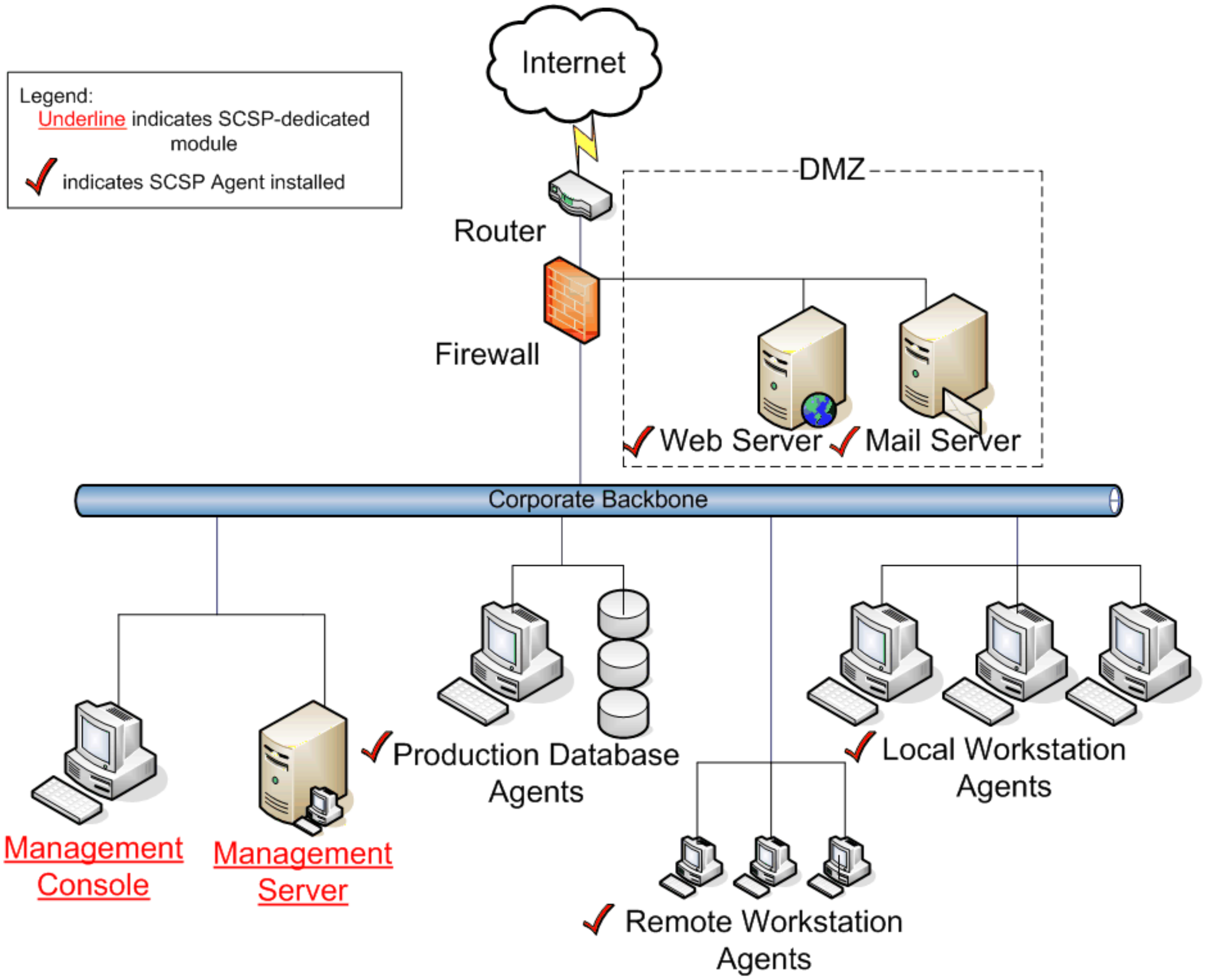
Legend:
Underline indicates SCSP-dedicated module
✓ indicates SCSP Agent installed
Internet
Router
Firewall
DMZ
✓ Web Server
✓ Mail Server
Corporate Backbone
Management Console
Management Server
✓ Production Database Agents
✓ Local Workstation Agents
✓ Remote Workstation Agents

Figure 1 - Deployment Configuration of the TOE

2.2 Product Description

The Symantec Critical System Protection product is a host-based intrusion detection and intrusion prevention system. The SCSP is a software-only implementation of an IDP. It is designed to protect an enterprise's internal network. The SCSP comprises three main components:

- SCSP Agents (Agents)
- SCSP Management Server (Server)
- SCSP Central Management Console (Console)

SCSP Agents (Agents):

SCSP Agents are software entities installed on various servers, workstations, and databases that are to be protected. The Agents apply Intrusion Protection System (IPS) and Intrusion Detection System (IDS) protection on processes and system resources on these machines. The policies which these agents apply are set though the SCSP Management Server.

The Intrusion Detection functionality monitors files, registry keys and system logs to determine if there has been any suspicious activity. One way it does this is by taking checksums of specified files periodically, and comparing them with previously calculated checksums to determine if there has been a change to the file. The Agent also captures operating system log events and determines whether those events are suspicious, based on the policies in place on the Agent. In addition, the IDS functionality will intercept registry system calls and apply a filter to them to determine whether a given key was changed. If any of these suspicious activities takes place, the IDS will generate an event. At specified polling intervals, the Agent passes selected IDS events to the Management Server to be stored in the database. The IDS functionality only records suspicious events; it does not prevent them.

The Intrusion Prevention functionality is a form of access control. It uses resource access control to protect the system from inappropriate use of system resources, such as registry keys, operating system files, important application files, and devices. Only the necessary resources for each running program are given read and write access privileges by the IPS. The IPS does this by using Application Programming Interface (API) hooks to capture system calls. It then applies behavior controls defined by policies to determine whether the calls should be allowed. If the calls are not appropriate for the processes initiating them, the IPS disallows them.

Agent software can be installed on a machine running the Windows XP Professional (with Service Pack 1 or later) or Windows Server 2003 Standard/Enterprise Operating System. The hardware requirements include the following: 256 Megabytes (MB) Random Access Memory (RAM), 1 Gigabyte (GB) hard disk, and a Pentium III 1.2 Gigahertz (GHz) CPU.

SCSP Management Server (Server):

The SCSP Management Server is the central management server for the SCSP system. The Server is implemented in Java and it provides functionality for storing, updating and distributing to the Console and Agents all enforcement policies, configuration settings, log events, and alerts. The Server is also responsible for registering Agents, authenticating the Console and Agents, and managing reporting, operators and roles. The Server also stores all data used and collected by the system, such as the policies and logs. All communication with the Server is initiated by the Agents and the Console via Secure Hyper-Text Transfer Protocol (HTTPS).

The Server is responsible for providing some of the management functionality for the SCSP system. For example, an operator creates policies via the Console Graphical User Interface (GUI). The Server receives these policies from the Console, and then makes them available to the various Agents in the system. The Agents perform the IDS and IPS functionality, and then send information back to the Server, usually in the form of event logs. This information is now made available in three possible forms: provided to the Console by the Server, stored in the database, or sent out by the Server as alerts via email or Simple Network Management Protocol (SNMP) traps. (Note: The Simple Mail Transfer Protocol (SMTP) and SNMP external interfaces are not security-relevant, but are included for completeness and understanding of the product.)

The Server software can be installed on a machine running the Windows Server 2003 Standard/Enterprise Operating System. The hardware requirements include the following: 1 GB RAM, 20 GB hard disk for production or 4 GB hard disk for evaluation, and a Pentium III 1.2 GHz CPU.

SCSP Management Console (Console):

The Console is a Java application that runs on a workstation that a system operator utilizes to manage the SCSP system. The Console provides a GUI through which the operator accesses the Server, and provides some of the management functionality for the SCSP system. The Console is responsible for initiating contact with the Server via HTTPS in order to perform management functions.

The Console software can be installed on a machine running Windows XP Professional (with Service Pack 1 or later) or Windows Server 2003 Standard/Enterprise Operating System. The hardware requirements are: 256 MB RAM, 1 GB hard disk, and a Pentium III 1.2 GHz CPU.

2.3 TOE Boundaries and Scope

This section will primarily address what physical and logical components of the SCSP are included in the TOE for this evaluation.

2.3.1 Physical Boundary

Figure 2 illustrates the physical scope and the physical boundary of the SCSP system and ties together all of the components of the TOE and the constituents of the TOE Environment. The Symantec Critical System Protection system version 5.0.5 will hereafter be referred to as the TOE throughout this document.

The TOE is an intrusion detection and intrusion prevention system which runs on the platform specified above. The TOE is installed as depicted in the figure below. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

- SCSP Management Console: The Console is the GUI utilized by the TOE operator to manage the TSF data, running on a Windows XP or Windows Server 2003, Java Swing, Java Runtime Environment (JRE) platform, with any number of User Interactive Programs and Third-party Applications installed and running. The hardware, Java Swing, JRE, operating system, User Interactive Programs, and Third-party Applications are excluded from the TOE Boundary.
- SCSP Management Server: The Server is the management software and the Microsoft SQL Server Desktop Engine (MSDE) database running on a dedicated Windows Server 2003, JRE, and Tomcat Server platform. The hardware, Windows, JRE, and Tomcat are excluded from the TOE Boundary.
- SCSP Agent: The Agent is the IDS/IPS functionality running on a Windows XP or Windows Server 2003 platform, with any number of User Interactive Programs and Third-party Applications installed and running. The hardware, operating system, User Interactive Programs, and Third-party Applications are excluded from the TOE.

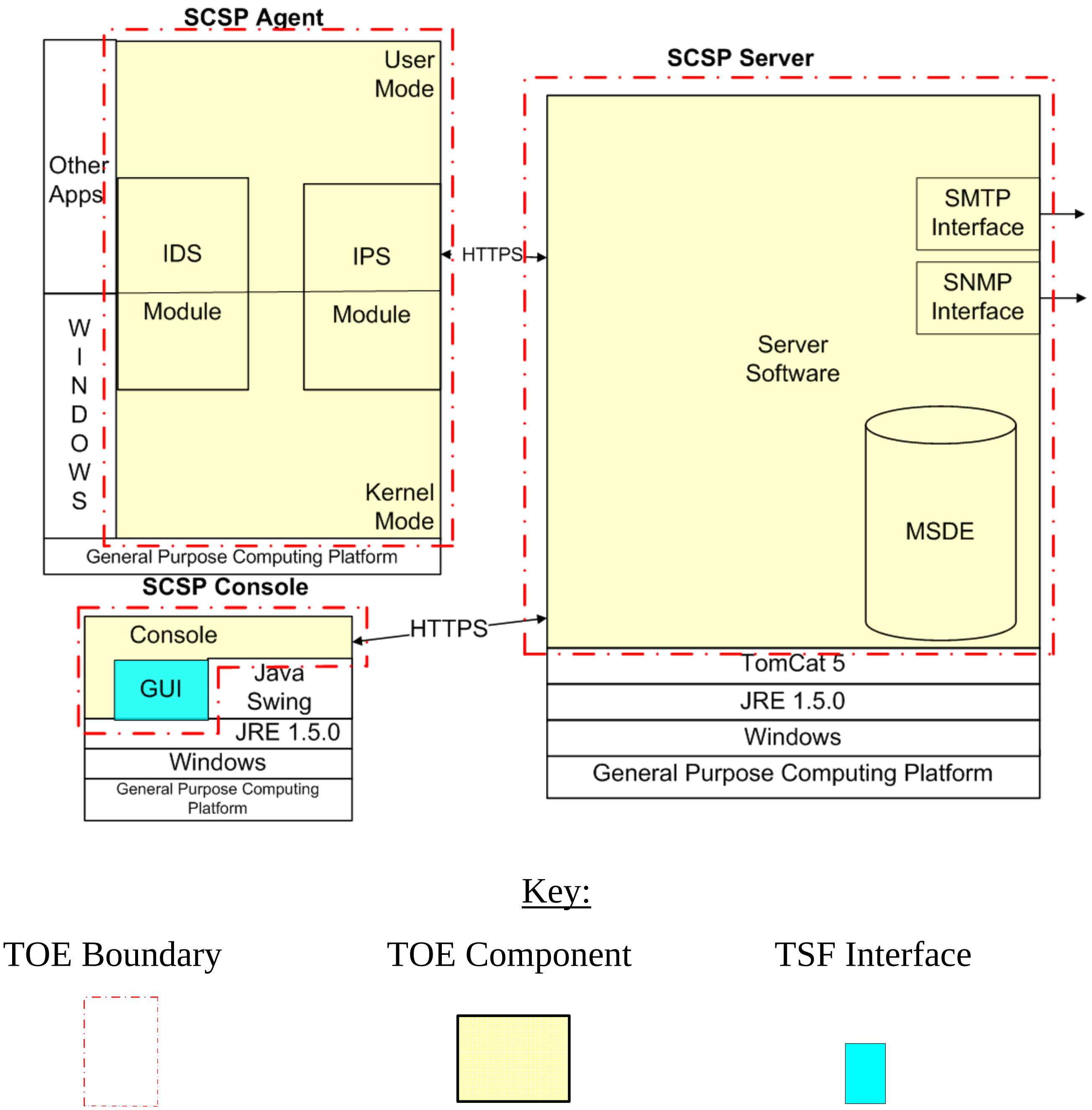

Figure 2 - Physical TOE Boundary

2.3.2 Logical Boundary

The TOE logical boundary is defined by the security functions that it implements. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection

- Identification and Authentication
- Security Management
- Protection of the TSF
- Intrusion Detection Functions

2.3.2.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation, storage and viewing of audit records. The TOE generates three types of logs: Audit logs, Management logs, and Enforcement logs. Audit logs contain information about operator logins and changes to configuration parameters and policies. Audit logs are generated by the Console. Management logs record the policies that are being applied to the Agents. Management logs are generated by the Agents. Enforcement logs record the IDS and IPS enforcement events. Enforcement logs are also generated by the Agents.

Audit logs are the primary focus of this security function. Some Management logs also contain security audit information. Enforcement logs are not addressed here, but are considered in the Intrusion Detection Functions security function.

2.3.2.2 User Data Protection

The User Data Protection function implements functionality for TOE security functions and TOE security function policies related to protecting user data. This functionality is the central behavior of the IPS Agent. Agents control access by interactive applications and services to Operating System resources. The paradigm of subjects accessing objects via operations is used to describe the rules enforced by the IPS Agent.

2.3.2.3 Identification and Authentication

The Identification and Authentication function provides functionality to establish and verify a claimed operator identity. This ensures that operators are associated with the proper security attributes, such as identity and roles. The TOE supports internally enforced operator username and password based authentication. Password strength rules are also enforced by the Console.

2.3.2.4 Security Management

The Security Management function specifies the management of several aspects of the TSF: security attributes, TSF data, and functionality in the TSF. The different management roles and their interaction will also be specified here.

2.3.2.5 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. The TOE protects information as it is transmitted between the components of the TOE (i.e., Agent and Server, or Console and Server) by transmitting via Hyper Text Transfer Protocol (HTTP) over Secure Sockets Layer (SSL). All other security functional requirements in this evaluation are impossible to bypass because the TOE is designed in such a way that no access is possible without passing through key security features, such as identification and authentication and role-based access control mediation. The TOE is separated from other processes by the operating system.

2.3.2.6 Intrusion Detection Functions

The Intrusion Detection Functions provides the IDS and the IPS enforcement events gathered by the Agents. These events record data accesses, service requests, network traffic, security configuration changes, and attempts to breach IPS policy. The data collected includes date and time of event, type of event, subject identity (e.g., username or source machine name), and the outcome of the event (e.g., success or failure).

2.3.3 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

Features and functionality that are not part of the evaluated configuration of the TOE are:

- Java Swing
- Java Runtime Environment
- Windows Operating System
- General Purpose Computing Platform (Hardware)
- Tomcat Web Server
- Other Applications running on the same host as the SCSP Agent

3 Security Environment

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

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

3.1 Assumptions

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

A.NOEVIL Operators are non-hostile, appropriately trained, and follow all operator guidance.

A.PHYSCL The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.2 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are unauthorized users of the TOE. Unauthorized users are assumed to:

- have public knowledge of how the TOE operates
- possess a low skill level
- have limited resources to alter TOE configuration settings
- have no physical access to the TOE
- possess a low level of motivation
- have a low attack potential

The IT assets requiring protection are the hosts on the protected network.

3.2.1 Threats Addressed by the TOE

The following threats are to be addressed by the TOE:

T.IDS An unauthorized user might gain unauthorized access to the resources of the host system which would not be detected.

T.IPS An unauthorized user might perform unauthorized actions (e.g., misuse, access, or malicious activity of IT System assets) on a host system which would compromise the security of the host system or make improper use of system resources.

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.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

3.3 Organizational Security Policies

There are no Organization Security Policies.

4 Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the TOE's security needs.

4.1 Security Objectives for the TOE

The specific security objectives are as follows:

O.AUDIT The TOE must gather audit records for data accesses and use of the System management functions.

O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE operators with the appropriate privileges, and only those TOE operators, can exercise such control.

O.IDAUTH The TOE must be able to identify and authenticate operators prior to allowing access to TOE administrative functions and data.

O.PROTECT The TOE must protect itself and the host system from unauthorized modifications and access to its functions and data.

O.ACCESS The TOE must allow authorized operators to access only appropriate TOE functions and data.

O.INTEGR The TOE must ensure the integrity of all audit and System data.

O.AGENT The TOE Agent 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 Agent.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives

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

OE.TIME The IT Environment will provide reliable timestamps to the TOE.

OE.SEP The IT Environment will protect the TOE from external interference or tampering.

4.2.2 Non-IT Security Objectives

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

NOE.NOEVIL Operators are non-hostile, appropriately trained, and follow all operator guidance.

NOE.PHYSCL The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

5 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE as well as Security Functional Requirements met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.1.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 2 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 2 - TOE Security Functional Requirements

SFR ID	Description	ST Operation			
		Selection	Assignment	Refinement	Iteration
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓	✓	
FAU_SAR.3(a)	Selectable audit review	✓	✓		✓
FAU_SAR.3(b)	Selectable audit review	✓	✓		✓
FAU_STG.1	Protected audit trail storage	✓			
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓	✓	
FIA_ATD.1	User attribute definition		✓	✓	
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.2	User authentication before any action			✓	
FIA_UID.2	User identification before any action			✓	
FMT_MOF.1	Management of security functions behavior	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		✓
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓	✓	
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
FPT_RVM.1	Non-bypassability of the TSP				
IDS_SDC.1	System data collection (EXP)				
IDS_RDR.1	Restricted data review (EXP)			✓	✓
IDS_STG.1	Guarantee of system data availability				

Section 5.1 contains the functional components from the CC Part 2 and three explicitly stated requirements with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.1.

5.1.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

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

b) All auditable events, for the *[not specified]* level of audit; and

c) [Set Policy, Create Policy, Update Settings, Login, Logout, Update Password, and Create Query].

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, *[no other audit relevant information]*.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide *[Administrators, Managers, and Guests]* with the capability to read *[all audit information]* from the audit records.

FAU_SAR.1.2

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3(a) Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1(a)

The TSF shall provide the ability to perform *[searches and sorting]* of audit data based on *[Date/Time, type of event, subject identity (Username), and the outcome (Disposition) of the event]*.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3(b) Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1(b)

The TSF shall provide the ability to perform *[ordering]* of audit data based on *[Host Machine, Date/Time, Object Name, Username, Operation, or Description]*.

Dependencies: FAU_SAR.1 Audit review

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1

The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2

The TSF shall be able to *[prevent]* unauthorised modifications to the audit records in the audit trail.

Dependencies: FAU_GEN.1 Audit data generation

5.1.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1

The TSF shall enforce the *[Access Control SFP]* on *[processes accessing files, network resources, registry keys, and devices]*.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

The TSF shall enforce the *[Access Control SFP]* to objects based on the following:

[SUBJECT (process) attributes:

1) Username of user launching process;

2) Full process path name;

OBJECT attributes:

Files:

1) Full file path name;

Network Resources:

1) Source Internet Protocol (IP) Address;

2) Destination IP Address;

3) Source Port;

4) Destination Port;

5) Protocol;

Registries:

1) Registry key name;

Devices:

1) Device Name].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *[a process is allowed to access a system resource as long as it is not explicitly blocked]*.

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *[If the IPS Policy is set to "Disable Prevention", then all processes are allowed to access all objects]*.

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the **following:** *[If the Limited Execution Policy is in force, a subject will be denied all access to all objects unless explicitly given access by the policy]*.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

5.1.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual ~~users~~ **operators**: *[Username, Password, and Role]*.

Dependencies: No dependencies

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet *[the requirement that passwords must be at least eight characters, and contain letters and at least two numbers or special characters]*.

Dependencies: No dependencies

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1

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

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2.1

The TSF shall require each ~~user~~ **operator** to identify itself before allowing any other TSF-mediated actions on behalf of that ~~user~~ **operator**.

Dependencies: No dependencies

5.1.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to *[determine the behaviour of, disable, enable, modify the behaviour of]* the functions *[IDS/IPS Functionality and administrative access defined in FMT_MTD.1]* to *[Administrators and Managers]*.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the *[Access Control SFP]* to restrict the ability to *[query]* the security attributes *[Username of user launching process, Full Process Path Name, Full File Path Name, Source IP Address, Destination IP Address, Source Port, Destination Port, Protocol, Registry Key Name, and Device Name]* to *[Administrator, Manager and Guest roles]*.

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to *[See* Table 3 *below]* the *[list of TSF data – See* Table 3 *below]* to *[the authorised identified roles – See* Table 3 *below]*.

Table 3 - Management of TSF Data

Roles TSF Data	Administrator	Manager	Guest
Audit Data	Query	Query	Query
Configuration Settings (of Management)	Change_default Query Modify Delete	Change_default Query Modify Delete	Query
Passwords	Modify Delete	Modify (*their own*)	None
Usernames	Query Modify Delete	Query Modify (*their own*)	Query

Roles TSF Data	Administrator	Manager	Guest
Roles	Query Modify Delete	Query	Query

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: *[security attribute management, TSF data management, and security function management]*.

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles *[Administrator, Manager, and Guest]*.

FMT_SMR.1.2

The TSF shall be able to associate ~~users~~ **operators** with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.5 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1

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

Dependencies: No dependencies

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

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.

Dependencies: No dependencies

5.1.6 Class Intrusion Detection Function

IDS_SDC.1 System Data Collection (EXP)

IDS_SDC.1.1

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

a) data accesses, service requests, network traffic, security configuration changes, attempts to breach IPS policy; 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.

IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1

The System shall provide Administrator, Manager, and Guest with the capability to read all data from the System data.

IDS_RDR.1.2

The system shall provide the System data in a manner suitable for the ~~user~~ **operator** to interpret the information.

IDS_STG.1 Guarantee of System Data Availability (EXP)

IDS_STG.1.1

The System shall protect the stored System data from unauthorized deletion.

IDS_STG.1.2

The System shall protect the stored System data from modification.

5.2 Security Requirements for the Environment

This section specifies the SFRs for the TOE environment by class. Table 4 identifies all SFRs implemented by the TOE environment and indicates the ST operations performed on each requirement.

Table 4 - TOE Environment Security Functional Requirements

SFR ID	Description	ST Operation			
		Selection	Assignment	Refinement	Iteration
FPT_SEP.1	TSF domain separation			✓	
FPT_STM.1	Reliable time stamps			✓	

Section 5.2 contains the functional components from the CC Part 2 with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.1.

5.2.1 Class FPT: Protection of the TOE Environment

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1

The ~~TSF~~ **TOE Environment** shall maintain a security domain for ~~its own~~ **the TOE's** execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2

The ~~TSF~~ **TOE Environment** shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1

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

Dependencies: No dependencies

5.3 Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.1. Table 5 summarizes the components.

Table 5 - Assurance Components

Assurance Requirements	
Class ACM: Configuration management	ACM_CAP.2 Configuration items
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Life Cycle	ALC_FLR.1 Basic Flaw Remediation
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing
Class AVA: Vulnerability assessment	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

6 TOE Summary Specification

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

6.1 TOE Security Functions

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

Table 6 - Mapping of Security Functions to TOE Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3(a)	Selectable audit review
	FAU_SAR.3(b)	Selectable audit review
	FAU_STG.1	Protected audit trail storage
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_RVM.1	Non-bypassability of the TSP
Intrusion Detection Functions	IDS_SDC.1	System data collection (EXP)
	IDS_RDR.1	Restricted data review (EXP)
	IDS_STG.1	Guarantee of system data availability (EXP)

6.1.1 Security Audit

The Security Audit function provides the TOE with the functionality for generation, storage, and viewing of audit records. As operators manage and configure the TOE, their activities are tracked by recording audit records into the logs. All security relevant configuration settings and changes are recorded to ensure accountability of the operator's actions. All logs contain the date, time, event type, subject identity, and the outcome of the event for each record.

The TOE generates three types of logs: Audit logs, Management logs, and Enforcement logs. Audit logs contain information about operator logins and changes to configuration parameters and policies. Audit logs are generated by the Console. Management logs record the policies that are being applied to the Agents. Management logs are generated by the Agents. Enforcement logs record the IDS and IPS enforcement events. Enforcement logs are also generated by the Agents.

All of the logs are stored in a MSDE database on the Server. TOE operators do not have direct access to the database and can only read audit records through the Console interface. A TOE operator is not granted access to the logs until they have been properly authenticated to the Server and database. TOE operators are never given write access to the logs and hence cannot modify or delete any audit records.

Only TOE operators assigned the appropriate roles can read the logs. The Administrator, Manager, and Guest roles can view the logs through the Monitors Page on the Console GUI or via queries and reports generated through the Console GUI. As a TOE operator requests a report or a page to view from the Console, the Server checks the operator's privileges to verify the TOE operator has permissions to view the requested data. The TOE audit interface allows the data to be searched, sorted, and ordered. When viewing the audit records through the Monitors Page on the Console, the records can be searched or sorted by date and time. The records can also be ordered by Host Machine, Date and Time, Object Name (Role), Username, Operation (e.g., Save, Update, Logout), or Description.

TOE Security Functional Requirements Satisfied: [FAU_GEN.1, FAU_SAR.1, FAU_SAR.3(a), FAU_SAR.3(b), and FAU_STG.1].

6.1.2 User Data Protection

The IPS Agent implements User Data Protection functionality via the Access Control Security Functional Policy. The Agent does this by controlling access by interactive applications and services to Operating System resources. Operators apply a prevention policy to define which subjects can perform which operations on which objects. The subjects that are regulated by this function are processes. The operation the subjects perform is access. The objects accessed are files, network resources, registry keys, and devices. The Access Control SFP defines how specific subjects can access specific objects and what operations they can perform on those objects. The subject and object attributes are used to determine the access of the subject to the object. The security function allows an operator to define a variety of rules to be enforced using the defined subject and objects.

Depending on the applied policy, each application or service is given access to certain resources, and/or restricted from accessing certain resources. The TOE accomplishes this access mediation by using "hooks" to various system calls. The Agent intercepts system calls and applies behavior controls to determine whether the calls are appropriate for the given application. If these calls are not appropriate, the Agent will disallow the calls. For example, a word processor application needs limited access to only a very few system resources in order to function normally, whereas an internet browser may require broader access to resources to perform its job normally.

The operator can disable the prevention enforcement dictated by the applied policy. This enables the operator to observe the impact of the prevention policy prior to its implementation.

TOE Security Functional Requirements Satisfied: [FDP_ACC.1, FDP_ACF.1].

6.1.3 Identification and Authentication

The Identification and Authentication function ensures that the TOE operator that is requesting a service has provided a valid username and password. For each operator, the TOE stores the following security attributes in the database: username, password, and role. When TOE operators enter their username and password at the Console interface, the information is passed to the Server, where it is verified against the username and password stored in the TOE. If the provided username and password match, the TOE operator is assigned the roles associated with that username.

The TOE supports internally enforced username and password-based authentication. Password strength rules are enforced by the Console. The TOE requires that passwords be at least eight characters long, and contain letters and at least two numbers or special characters. The first action that operators must take when attempting to interact with the TOE is to provide a username and password. Before identification and authentication, the TOE operator is not able to perform any TOE security functionality. The Strength of Function (SOF)-basic claim applies to the following security functions: I&A.

TOE Security Functional Requirements Satisfied: [FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2].

6.1.4 Security Management

Operators use the Console interface to perform all management of the TOE. The Security Management function implements and enforces the different management roles supported by the TOE: Administrator, Manager, and Guest. Each role enforced by this TSF has different privileges to configure the behavior of the TOE. For example, Administrators can change policies, and have the right to change security attributes.

The TOE enforces which roles have access to TSF data, such as audit data, IDS/IPS data, and configuration settings. Administrator, Manager and Guest roles all have the ability to query TSF Data. Only Administrators and Managers can modify or delete configuration settings. No role has the ability to modify or delete audit data or IDS/IPS data. The Administrator is the only role that can modify or delete other operators’ usernames, passwords , or roles.

Attempts by the operator to query, modify, or delete security attributes (such as Username, Password, or Role), TSF data (such as audit data, IDS/IPS data, and configuration settings), and security functions (such as user data protection and IDS/IPS functionality) are mediated by the TOE.

TOE Security Functional Requirements Satisfied: [FMT_MOF.1, FMT_MSA.1,FMT_MTD.1, FMT_SMF.1, FMT_SMR.1].

6.1.5 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that provide the TSF. Protection of the TOE from physical tampering is ensured by its environment. It is the responsibility of the administrator to assure that physical connections made to the TOE remain intact and unmodified. The TOE protects information as it is transmitted between components of the TOE (i.e., Agent and Server, or Console and Server) by transmitting via HTTPS. For example, when policy updates are sent from the Server to the Agent, they are transmitted over a secure line, using the HTTPS protocol. These updates are also tracked in audit logs to ensure operator accountability. For example, if an operator changes a policy, this action can be viewed in the audit records.

Non-bypassability of the TOE is provided by a combination of basic configuration and enforcement of security policy rules. Each subject’s and operator’s security privileges are separated. It is not possible to perform any actions on the system without successfully authenticating. Once an operator has been authenticated, they are bound to the appropriate roles and any privileges defined by the TOE access control. For any operator to perform a TOE operation an Administrator must have granted that operator the rights to perform that operation. These privileges are granted on a per operator basis. Since all access control rights are checked by the TOE’s mechanisms and the TOE uses unique attributes for each operator, then the TSF maintains separation between different operators. As an example, if an operator without explicit permission tries to edit a policy, the operator will not be able to save the changes.

TOE Security Functional Requirements Satisfied: [FPT_ITT.1, FPT_RVM.1].

6.1.6 Intrusion Detection Functions

The Intrusion Detection Functions implement the IDS and IPS functionality. These IDS and IPS events are generated by Agents installed on individual host machines. Enforcement events generated by the Agents record data accesses, service requests, network traffic, security configuration changes, and attempts to breach IPS policy on each host. Data collected includes date and time of the event, the type of event, subject identity (e.g., username or source machine name), and the outcome of the event (e.g., success or failure). Enforcement events are collected to provide the TOE operator with information concerning suspicious or malicious activity taking place on the Agent. The TOE operator can then take the appropriate corrective action.

When an operator authenticates to the Server, the TOE provides the operator with the capability to read the enforcement events, in a format that enables searching and ordering. The TOE protects this data from unauthorized modification or deletion with the mechanisms described in section 6.1.1. TOE operators are never given write access to enforcement records.

TOE Security Functional Requirements Satisfied: [IDS_SDC.1, IDS_RDR.1, IDS_STG.1].

6.2 TOE Security Assurance Measures

EAL2 Augmented with ALC_FLR.1 was chosen to provide a basic level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL2 Augmented with ALC_FLR.1 level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Table 7 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure Documents
ACM_CAP.2	Symantec Critical System Protection v5.0.5 – Configuration Management
ADO_DEL.1	Symantec Critical System Protection v5.0.5 – Delivery and Operation
ADO_IGS.1	Symantec Critical System Protection v5.0.5 Installation Guide Documentation v5.0.5 Symantec Critical System Protection v5.0.5 Installation Guide Supplement
ADV_FSP.1	Symantec Critical System Protection v5.0.5 - TOE Architecture: Informal Functional Specification
ADV_HLD.1	Symantec Critical System Protection v5.0.5 - TOE Architecture: High Level Design
ADV_RCR.1	Symantec Critical System Protection v5.0.5 - TOE Architecture: Representation Correspondence

Assurance Component	Assurance Measure Documents
AGD_ADM.1	Symantec Critical System Protection v5.0.5 Administration Guide Documentation v5.0.5 Symantec Critical System Protection v5.0.5 Prevention Policy Reference Guide Documentation v5.0.5 Symantec Critical System Protection v5.0.5 Detection Policy Reference Guide Documentation v5.0.5 Symantec Critical System Protection v5.0.5 Release Notes Documentation v5.0.5 Symantec Critical System Protection v5.0.5 Administration Guide Supplement
AGD_USR.1	n/a
ALC_FLR.1	Symantec Critical System Protection v5.0 – Flaw Remediation
ATE_COV.1	Symantec Critical System Protection v5.0.5 –Test Coverage Analysis
ATE_FUN.1	Symantec Critical System Protection v5.0.5 – Functional Testing
ATE_IND.2	Symantec Critical System Protection v5.0.5 – Independent Testing
AVA_SOF.1	Symantec Critical System Protection v5.0.5 – Strength of Function Analysis
AVA_VLA.1	Symantec Critical System Protection v5.0.5 - Vulnerability Analysis

6.2.1 ACM_CAP.2: Configuration Management Document

The Configuration Management document provides a description of the various tools used to control the configuration items and how they are used internally at Symantec. This document provides a complete configuration item list and a unique referencing scheme for each configuration item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

6.2.2 ADO_DEL.1: Delivery and Operation Document

The Delivery and Operation document provides a description of the secure delivery procedures implemented by Symantec to protect against TOE modification during product delivery. The Installation Documentation provided by Symantec details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the TOE operator(s) on configuring the TOE and how they affect the TSF.

6.2.3 ADO_IGS.1: Installation Guidance, AGD_ADM.1: Administrator Guidance, AGD_USR.1: User Guidance

The installation guidance document provides the procedures necessary for the secure installation, generation, and start-up of the TOE for operators of the TOE.

The administrator guidance documentation provides detailed procedures for the administration of the TOE and description of the security functions provided by the TOE.

The User Guidance documentation provided directs operators on how to operate the TOE in a secure manner. Additionally, User Guidance explains the operator-visible security functions and how they need to be exercised.

6.2.4 ADV_FSP.1: Informal Functional Specification, ADV_HLD.1: High Level Design, ADV_RCR.1: Representation Correspondence.

The Symantec design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and error messages for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Representation Correspondence demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the Security Target (ST) description to the High-Level Design.

6.2.5 ALC_FLR.1: Basic Flaw Remediation

The Flaw Remediation document outlines the steps taken at Symantec to capture, track and remove bugs. The documentation shows that all flaws are recorded and that the system tracks them to completion.

6.2.6 ATE_COV.1: Test Coverage Analysis, ATE_FUN.1: Functional Testing, ATE_IND.2: Independent Testing

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates that testing is performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided in order to meet the assurance requirement Functional Testing. Independent Testing will be performed by EWA in order to determine whether the TOE behaves as specified, and to gain confidence in the developer's test results by performing a sample of the developer's tests.

6.2.7 AVA_VLA.1: Vulnerability Analysis, AVA_SOF.1: Strength of Function Analysis

A Vulnerability Assessment is provided to demonstrate ways in which an entity could violate the TOE Security Policy (TSP) and provide a list of identified vulnerabilities. Additionally, this document provides evidence of how the TOE is resistant to obvious attacks.

The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

7 Protection Profile Claims

This section provides the identification and justification for any Protection Profile conformance claims.

7.1 Protection Profile Reference

There are no protection profile claims for this security target.

8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Security Target. Table 8 demonstrates the mapping between the assumptions, threats, and policies to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 8 - Relationship of Security Threats to Objectives

		Objectives	TOE Objectives							Environmental Objectives			
										IT		NON-IT	
Threats, Assumptions			O.ADMIN	O.AUDIT	O.IDAUTH	O.PROTECT	O.ACCESS	O.INTEGR	O.AGENT	OE.TIME	OE.SEP	NOE.NOEVIL	NOE.PHYSCL
Threats	TOE	T.IDS		✓					✓	✓	✓		
		T.IPS				✓		✓			✓		
		T.COMINT		✓	✓	✓	✓	✓	✓	✓	✓		
		T.PRIVIL	✓	✓	✓	✓	✓			✓	✓		
Assumptions		A.NOEVIL										✓	
		A.PHYSCL											✓

T.IDS **An unauthorized user might gain unauthorized access to the resources of the host system which would not be detected.**

This threat is primarily diminished by the O.AGENT objective, which requires that the TOE Agent 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 Agent. The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE. The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE. The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.

T.IPS **An unauthorized user might perform unauthorized actions (e.g., misuse, access, or malicious activity of IT System assets) on a host system which would compromise the security of the host system or make improper use of system resources.**

This threat is primarily diminished by the O.PROTECT objective, which requires that the TOE protect itself and the host system from unauthorized modifications and access to its functions and data. The OE.SEP objective supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.

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.**

This threat is primarily diminished by the O.INTEGR objective, which requires that the TOE ensure the integrity of all audit and System data. The O.PROTECT objective requires that the TOE protect itself and the host system from unauthorized modifications and access to its functions and data. The O.ACCESS and O.INTEGR objectives ensure that unauthorized modifications and access to functions and data is diminished. The O.IDAUTH objective requires that the TOE must be able to identify and authenticate operators prior to allowing access to TOE functions and data. The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE functions and data. The O.AGENT objective requires that the TOE Agent 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 Agent. The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE. The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE. The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.

T.PRIVIL **An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.**

This threat is primarily diminished by the O.IDAUTH objective, which requires that the TOE must be able to identify and authenticate operators prior to allowing access to TOE functions and data. The O.ADMIN, O.IDAUTH, and O.ACCESS objectives together ensure that policies won't be subverted or changed by unauthorized users. The O.ADMIN objective ensures that only TOE operators with appropriate privileges can manage the functions and data of the TOE. The O.ACCESS objective provides that the TOE must allow authorized operators to access only appropriate TOE functions and data. The O.PROTECT objective requires that the TOE protect itself and the host system from unauthorized modifications and access to its functions and data. The O.AUDIT objective provides defense in depth, by requiring the recording and availability of audit records for review by an authorized operator of the TOE. The OE.TIME objective supports these objectives by providing for reliable timestamps to be used by the TOE. The OE.SEP objective also supports these objectives by requiring that the IT environment protect the TOE from interference that would prevent it from performing its functions.

A.NOEVIL **Operators are non-hostile, appropriately trained, and follow all operator guidance.**

The NOE.NOEVIL objective ensures that operators are non-hostile, appropriately trained, and follow all operator guidance.

A.PHYSCL **The TOE will be located within controlled access facilities, which will prevent unauthorized physical access**.

The NOE.PHYSCL objective requires that the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

8.2 Security Functional Requirements Rationale

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

Table 9 - Relationship of Security Requirements to Objectives

	Objectives	TOE							Environment	
	Requirements	O.ADMIN	O.AUDIT	O.IDAUTH	O.PROTECT	O.ACCESS	O.INTEGR	O.AGENT	OE.TIME	OE.SEP
TOE	FAU_GEN.1		✓							
	FAU_SAR.1		✓							
	FAU_SAR.3(a)		✓							
	FAU_SAR.3(b)		✓							
	FAU_STG.1			✓	✓	✓	✓			
	FDP_ACC.1				✓					
	FDP_ACF.1				✓					
	FIA_ATD.1			✓						
	FIA_SOS.1			✓						
	FIA_UAU.2			✓		✓				
	FIA_UID.2			✓		✓				
	FMT_MOF.1	✓		✓	✓	✓				
	FMT_MSA.1	✓								
	FMT_MTD.1	✓		✓	✓	✓	✓			
	FMT_SMF.1	✓								
	FMT_SMR.1	✓								
	FPT_ITT.1						✓			
	FPT_RVM.1			✓	✓		✓			
	IDS_SDC.1							✓		
	IDS_RDR.1	✓		✓		✓				
	IDS_STG.1			✓	✓	✓	✓			
Environment	FPT_STM.1								✓	
	FPT_SEP.1									✓

O.AUDIT **The TOE must gather audit records for data accesses and use of the System management functions.**

Security-relevant events must be defined and auditable for the TOE (FAU_GEN.1). The TOE must provide the ability to review and manage the audit trail of the system (FAU_SAR.1, FAU_SAR.3). FAU_GEN.1, FAU_SAR.1, and FAU_SAR.3 together satisfy this objective.

O.ADMIN **The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE operators with the appropriate privileges, and only those TOE operators, can exercise such control.**

The System must provide the ability for authorized operators to view all System data collected and produced (IDS_RDR.1). The TOE defines a set of roles (FMT_SMR.1). Only those roles are given the right to control the behavior of the TSF (FMT_MOF.1) and to access TSF data (FMT_MTD.1). Mechanisms exist to enforce these rules (FMT_SMF.1). The security attributes used by the TOE are secure because they can only be changed by authorized operators (FMT_MSA.1). IDS_RDR.1, FMT_SMR.1, FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, and FMT_MSA.1 together satisfy this objective.

O.IDAUTH **The TOE must be able to identify and authenticate operators prior to allowing access to TOE functions and data.**

The System is required to restrict the review of System data to those granted explicit read-access (IDS_RDR.1). The TOE is required to protect the stored audit records from unauthorized deletion (FAU_STG.1). The System is required to protect the System data from any modification and unauthorized deletion (IDS_STG.1). Security attributes of subjects used to enforce the authentication policy of the TOE must be defined (FIA_ATD.1). The TOE will not give any access to an operator until the TOE has identified (FIA_UID.2) and authenticated (FIA_UAU.2) the operator. The System can have confidence in the competence of the identification and authentication because only strong passwords can be used (FIA_SOS.1). The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized operators of the TOE (FMT_MOF.1). Only authorized operators of the System may query and modify all other TOE data (FMT_MTD.1). The TOE must be able to recognize the different operator roles that exist for the TOE (FMT_SMR.1). The TOE must ensure that all functions are invoked and succeed before each function may proceed (FPT_RVM.1). IDS_RDR.1, FAU_STG.1, IDS_STG.1, FIA_ATD.1, FIA_UID.2, FIA_UAU.2, FIA_SOS.1, FMT_MOF.1, FMT_MTD.1, FMT_SMR.1, and FPT_RVM.1 together satisfy this objective.

O.PROTECT **The TOE must protect itself and the host system from unauthorized modifications and access to its functions and data.**

The TOE is required to protect the stored audit records from unauthorized deletion (FAU_STG.1). The TOE has an access control policy which ensures that only authorized entities gain access to the files, network resources, registry keys, and devices (FDP_ACC.1, FDP_ACF.1). The System is required to protect the System data from any modification and unauthorized deletion (IDS_STG.1). The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized operators of the TOE (FMT_MOF.1). Only authorized operators of the System may query and add System and audit data, and authorized operators of the TOE may query and modify all other data (FMT_MTD.1). The TOE must ensure that all functions are invoked and succeed before each function may proceed (FPT_RVM.1). FAU_STG.1, FDP_ACC.1, FDP_ACF.1, IDS_STG.1, FMT_MOF.1, and FMT_MTD.1 together satisfy this objective.

O.ACCESS **The TOE must allow authorized operators 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). The TOE is required to protect the audit data from unauthorized deletion (FAU_STG.1). The TOE will not give any access to an operator until the TOE has identified (FIA_UID.2) and authenticated (FIA_UAU.2) the operator. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized operators of the TOE (FMT_MOF.1). Only authorized operators of the System may query and add System and audit data, and authorized operators of the TOE may query and modify all other TOE data (FMT_MTD.1). IDS_RDR.1, FAU_STG.1, FIA_UID.2, FIA_UAU.2, FMT_MOF.1, and FMT_MTD.1 together satisfy this objective.

O.INTEGR **The TOE must ensure the integrity of all audit and System data.**

The TOE is required to protect the audit data from unauthorized deletion (FAU_STG.1). The System is required to protect the System data from any modification and unauthorized deletion (IDS_STG.1). Only authorized operators of the System may query or modify audit and System data (FMT_MTD.1). The System must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product (FPT_ITT.1). The TOE must ensure that all functions to protect the data are not bypassed (FPT_RVM.1). FAU_STG.1, IDS_STG.1, FMT_MTD.1, and FPT_ITT.1 together satisfy this objective.

O.AGENT **The TOE Agent 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 Agent.**

A System containing an Agent 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). IDS_SDC.1 satisfies this objective.

OE.TIME **The IT Environment will provide reliable timestamps to the TOE.**

The IT Environment is required to provide reliable timestamps to the TOE (FPT_STM.1).

OE.SEP **The IT Environment will protect the TOE from external interference or tampering.**

The IT Environment must protect the TOE from interference that would prevent it from performing its functions (FPT_SEP.1).

8.3 Security Assurance Requirements Rationale

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

The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.4 Rationale for Intrusion Detection Functions

A family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The IDS Protection Profile (PP) Version 1.5 was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS and IPS data (enforcement events, such as data accesses, service requests, network traffic, security configuration changes, and attempts to breach IPS policy), 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. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

8.5 Rationale for Refinements of Security Functional Requirements

The following refinements of Security Functional Requirements from CC version 2.3 have been made to clarify the content of the SFRs, and make them easier to read:

The title “Class FPT: Protection of the TSF” has been refined to “Class FPT: Protection of the TOE Environment” in Section 5.2.1.

The term “TSF” has been refined to “TOE Environment” in Section 5.2.1.

The term “its own” has been refined to “the TOE’s” in Section 5.2.1.

The term “user” has been refined to “operator” in several SFRs.

8.6 Dependency Rationale

Table 10 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. Where a dependency is not met, a rationale is given.

Table 10 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3(a)	FAU_SAR.1	✓	
FAU_SAR.3(b)	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
FDP_ACF.1	FMT_MSA.3		FMT_MSA.3 is not required because the security attributes used by the TOE are never given default attributes.
FIA_UAU.2	FIA_UID.1	✓	
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	✓	
FMT_MSA.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	✓	

FMT_SMR.1	FIA_UID.1	✓ (FIA_UID.2)	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency.

8.7 TOE Summary Specification Rationale

8.7.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Summary Specification (Section 6) describes a security function of the TOE. Each description is organized by set of requirements with rationale that indicates how these requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 11 demonstrates that the combination of the specified IT security functional requirements work together so as to satisfy the TOE security functions.

The only security mechanism that is realized by a probabilistic or permutational implementation is the password mechanism. For an analysis of the Strength of Function, refer to Strength of Function (SOF) Rationale section.

Table 11 - Mapping of Security Functional Requirements to TOE Security Functions

TOE Security Function	SFR	Rationale
Security Audit	FAU_GEN.1 FAU_SAR.1 FAU_SAR.3(a) FAU_SAR.3(b) FAU_STG.1	The TOE logs critical security functions related to security management. Audit records are generated by the TOE when operators login, logout, change configurations parameters or policies, and apply policies to Agents. Data related to the security functions, such as the date and time of the event, the type of event, subject identity, and the outcome of the event are written to the audit files by the TOE. (FAU_GEN.1) The TSF provides the operators with the capability to read the audit data via the Monitors Page, and the Reports Page on the Console GUI. (FAU_SAR.1) The Console GUI provides the capability for the operator to search, sort, and order the audit data. (FAU_SAR.3(a) and FAU_SAR.3(b)) The Console GUI prevents operators from modifying or deleting the audit records. (FAU_STG.1) Together these contribute to a coherent security audit function.
User Data Protection	FDP_ACC.1 FDP_ACF.1	The IPS functionality of the TOE enforces prevention policies on processes accessing files, network resources, registry keys, and devices. (FDP_ACC.1) The IPS functionality identifies subjects by Username of the launching process, and by the full process path name. Policies enforce the ability or inability of these subjects to access files (based on full file path name), network resources (based on source IP address, destination IP address, source port, destination port, and/or protocol), registries (based on registry key name), and devices (based on device name). (FDP_ACF.1) Together these contribute to a coherent user data protection function.

TOE Security Function	SFR	Rationale
Identification and Authentication	FIA_ATD.1 FIA_SOS.1 FIA_UAU.2 FIA_UID.2	The Administrator role sets up and maintains individual security attributes (Username, Password, and Role) for each operator. (FIA_ATD.1) The TOE requires that all passwords must be at least eight characters, and contain letters and at least two numbers or special characters, or the password will not be accepted. (FIA_SOS.1) Operators cannot perform any action on the TOE prior to being identified and authenticated by the TOE. (FIA_UID.2 and FIA_UAU.2) Together these contribute to a coherent identification and authentication function.
Security Management	FMT_MOF.1 FMT_MSA.1 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1	The TOE allows an operator who possesses the appropriate privileges to perform management functions. All management functionality is allowed only by authorized TOE operators. They must authenticate with the TOE before any access to the TSF is permitted. TOE operators can take three roles: ▪ Administrators can perform all security management functions on the TOE. They can query the audit data, IDS/IPS data, configuration settings, usernames and roles. They can modify configuration settings, passwords, usernames, and roles. And they can delete configuration settings, passwords, usernames, and roles. ▪ Managers can perform many security management functions on the TOE. They can query the audit data, IDS/IPS data, configuration settings, usernames, and roles. They can modify configuration settings, their own passwords, and their own usernames. They cannot delete any passwords, usernames, or roles, and they cannot modify any other operators' passwords or usernames. ▪ Guests can only query the security attributes and data, including audit data, IDS/IPS data, configuration settings, usernames and roles. They cannot modify or delete any security data on the TOE. Together these contribute to a coherent security management function.
Protection of the TSF	FPT_ITT.1 FPT_RVM.1	The functions that enforce the TSP must succeed first before any other function can proceed. No other administrator functions can be performed before identification and authentication of the operator is completed. (FPT_RVM.1) The TSF data is protected from disclosure or modification when it is transmitted between separate parts of the TOE, because it is transmitted via HTTPS. (FPT_ITT.1) Together these contribute to a coherent TOE protection function.
Intrusion Detection Functions	IDS_SDC.1 IDS_RDR.1 IDS_STG.1	The TOE collects intrusion detection events for policy-specified data accesses, service requests, network traffic, security configuration changes, and attempts to breach intrusion prevention policies. It collects the data and time of the event, the type of event, the subject identity, and the outcome of the event for each policy-specified access. (IDS_SDC.1) The TOE allows only authorized operators with the following roles to read the intrusion detection system data: Administrator, Manager, and Guest. The TSF provides the operators with the capability to read the IDS data via the Monitors Page and the Reports Page on the Console GUI. (IDS_RDR.1) The Console GUI prevents operators from modifying or deleting the IDS data. (IDS_STG.1) Together these contribute to a coherent intrusion detection function.

8.7.2 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL2 Augmented with ALC_FLR.1 was chosen to provide a basic level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment.

[While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment.] The chosen assurance level was also selected for conformance with the client's needs.

8.7.2.1 Configuration Management

The Configuration Management documentation provides a description of tools used to control the configuration items and how they are used at Symantec. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Configuration Items

8.7.2.2 Delivery and Operation

The Delivery and Operation documentation provides a description of the secure delivery procedures implemented by Symantec to protect against TOE modification during product delivery. The Installation Documentation provided by Symantec details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the operator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation and Start-Up Procedures

8.7.2.3 Development

The Symantec design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and error messages for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.
- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

Corresponding CC Assurance Components:

- Informal Functional Specification

- Descriptive High-Level Design
- Informal Representation Correspondence

8.7.2.4 Guidance Documentation

The Symantec Guidance documentation provides administrator and operator guidance on how to securely operate the TOE. The Administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally, it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. The User Guidance provided directs operators on how to operate the TOE in a secure manner. Additionally, User Guidance explains the operator-visible security functions and how they are to be used and explains the operator's role in maintaining the TOE's Security. Symantec provides single versions of documents which address the Administrator Guidance and User Guidance; there are not separate guidance documents specifically for non-administrator operators of the TOE.

Corresponding CC Assurance Components:

- Administrator Guidance
- User Guidance

8.7.2.5 Tests

There are a number of components that make up the Test documentation. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. Symantec Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided. Independent Testing will be performed by EWA-Canada in order to determine whether the TOE behaves as specified, and to gain confidence in the developer's test results by performing a sample of the developer's tests.

Corresponding CC Assurance Components:

- Evidence of Coverage
- Functional Testing
- Independent Testing

8.7.2.6 Vulnerability and TOE Strength of Function Analyses

A Vulnerability Assessment is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks. The Strength of TOE Security Function Analysis demonstrates the strength of the probabilistic or permutational mechanisms employed to provide security functions within the TOE and how they exceed the minimum SOF requirements.

Corresponding CC Assurance Components:

- Strength of TOE Security Function analysis
- Vulnerability Analysis

8.8 Strength of Function

Strength of function rating of SOF-basic was claimed for this TOE to meet the EAL2 Augmented with ALC_FLR.1 assurance requirements; this SOF is sufficient to resist the threats identified in Section 3. The SOF-basic claim applies to the following security functions: I&A. Section 4 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements. The evaluated TOE is intended to operate in commercial and DOD low robustness environments processing unclassified information.

The overall TOE SOF claim is SOF-basic because this SOF is sufficient to resist the threats identified in Section 3.2. Section 8.1 provides evidence that demonstrates that TOE threats are countered by the TOE security objectives. Section 8.2 demonstrates that the security objectives for the TOE and the TOE environment are satisfied by the security requirements.

The relevant security functions and security functional requirements which have probabilistic or permutational functions are FIA_UAU.2 and FIA_SOS.1.

9 Acronyms

Table 12 - Acronyms

Acronym	Definition
API	Application Programming Interface
CC	Common Criteria
DMZ	DeMilitarized Zone
EAL	Evaluation Assurance Level
GB	Gigabyte
GHz	Gigahertz
GUI	Graphical User Interface
HTTP	Hyper-Text Transfer Protocol
HTTPS	Secure Hyper-Text Transfer Protocol
I&A	Identification and Authentication
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
JRE	Java Runtime Environment
MB	Megabyte
MSDE	Microsoft SQL Server Desktop Engine
PP	Protection Profile
RAM	Random Access Memory
SCSP	Symantec Critical System Protection
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOF	Strength Of Function
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	Target of Evaluation (TOE) Security Function
TSP	Target of Evaluation (TOE) Security Policy