Security Target: Symantec™ Security Information Manager Version 4.5

ST Version 1.7

August 24, 2007

Prepared For:

Symantec Corporation

20330 Stevens Creek Blvd.

Cupertino, CA 95014

www.symantec.com

Prepared By:

Apex Assurance Group, LLC

5448 Apex Peakway Drive, Ste. 101

Apex, NC 27502

www.apexassurance.com

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Symantec™ Security Information Manager Version 4.5. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Document Revision History

REVISION	DATE	DESCRIPTION
1.0	January 1, 2007	Initial release to Symantec for review
1.1	January 7, 2007	Update with comments from Symantec, submit to lab for evaluation
1.2	January 15, 2007	Incorporate additional comments and revise TOE description
1.3	April 10, 2007	Address laboratory verdicts
1.4	June 6, 2007	Address laboratory verdicts
1.5	July 19, 2007	Include build number, application note
1.6	August 19, 2007	Close verdicts
1.7	August 24, 2007	Revise assumptions per AVA verdicts, refresh Assurance Measures table

Table of Contents

List of Tables

List of Figures

1 Introduction

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

1.1 Identification

This section provides information necessary to identify and control this ST and its Target of Evaluation.

ST Title:	Security Target for Common Criteria Evaluation: Symantec™ Security Information Manager Version 4.5
ST Revision:	1.7
ST Publication Date:	August 24, 2007
TOE Identification:	Symantec™ Security Information Manager Version 4.5
Vendor:	Symantec Corporation
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.3 August 2005 (ISO/IEC 15408:2005).
Author:	Apex Assurance Group
Keywords:	Symantec, SIM, information management, event management, incident management

1.2 Overview

The TOE is the Symantec™ Security Information Manager Version 4.5, providing real-time event correlation and data archiving to protect against security threats and to preserve critical security data. The TOE collects, analyzes, and archives information from security devices, critical applications, and services to help recognize and respond to threats in the enterprise.

Symantec™ Security Information Manager Version 4.5 may hereafter also be referred to as Security Information Manager, Information Manager or the TOE.

1.3 CC Conformance Claim

The TOE is Common Criteria Version 2.3 Part 2 extended and Part 3 conformant at EAL2.

1.4 Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the Security Target
2	TOE Description	Defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
3	TOE Security Environment	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE and the TOE environment
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE
6	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.
7	PP Claims	Specifies Protection Profile conformance claims of the TOE
8	Rationale	Provides a rationale to demonstrate that the security objectives satisfy the threats; provides justifications of dependency analysis and strength of function issues

Table 1 – ST Organization and Description

1.5 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 2.3 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in paragraph 2.1.4 of Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

Italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.6 Document Terminology

The following table provides a list of terms and acronyms used within this document:

TERM	DEFINITION
Administrator	An operator responsible for installation, configuration, and User management
AV	Antivirus
CC	Common Criteria version 2.3 (ISO/IEC 15408:2005)
EAL	Evaluation Assurance Level
FW	Firewall
IDS	Intrusion Detection System
NTP	Network Time Protocol
Operator	An individual utilizing the functions of the TOE as an Administrator or User
OS	Operating System
OSP	Organizational Security Policy
SIM	Security Information Manager
SFR	Security Functional Requirement
SFP	Security Function Policy
SOF	Strength Of Function
SSIM	Symantec Security Information Manager
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
User	An operator responsible for management of incidents, reports, and correlation rules
VPN	Virtual Private Network

Table 2 – Document Terms and Acronyms

2 TOE Description

This section describes the Target of Evaluation (TOE), the provided security functionality (logical boundaries), and the physical TOE boundaries.

2.1 Overview

Security information management provides the ability to analyze historical security events and generate reports on security metrics in support of satisfying security policy compliance needs. Symantec Security Information Manager provides real-time event correlation and data archiving to protect against security threats and to preserve critical security data. Information Manager collects, analyzes, and archives information from security devices, critical applications, and services, such as the following:

- Firewalls
- Routers, switches, and VPNs
- Enterprise Antivirus solutions
- Intrusion detection and intrusion prevention devices
- Vulnerability scanners
- Authentication servers
- Windows and UNIX system logs

Symantec Security Information Manager provides the following features to help recognize and respond to threats in the enterprise:

- Normalization and correlation of events from multiple vendors to recognize threats from all areas of the enterprise.
- Event archives to retain events in both their original and normalized formats.
- Distributed event filtering and aggregation to ensure that only relevant security events are correlated.
- Real-time security intelligence updates from Symantec™ Global Intelligence Network to keep the operator apprised of global threats and to allow correlation of internal security activity with external threats.
- Customizable event correlation rules to fine-tune threat recognition and incident creation for the environment.
- Security incident creation, ticketing, tracking, and remediation for quick response to security threats. Information Manager prioritizes incidents based upon the security policies associated with the affected assets.
- An event archive viewer that allows an operator to mine large amounts of event data and perform network operations on the machines that are associated with each event.
- A Management Console (also referred to as “the console”) to view all incidents and drill

down to the related event details, including affected targets, associated vulnerabilities, and recommended corrective actions.

- Pre-defined and customizable queries to help demonstrate compliance with the security and data retention policies in the enterprise.

The following sections describe events, conclusions, and incidents.

2.1.1 Events

Network-attached devices and operating systems generate several kinds of events. Some events are informational, such as a user logging on, and others may indicate a security threat, such as antivirus software being disabled. The Information Manager Event Collector captures events from various network-attached devices and forwards the information to the Correlation Engine, where the events are then compared against a correlation rule pattern.

2.1.2 Conclusions

A conclusion occurs when one or more events match a correlation rule pattern. Information Manager normalizes events from multiple products and looks for patterns that indicate potential threats.

2.1.3 Incidents

An incident is the result of one or more conclusions that are identified as a type of an attack, and there can be many conclusions mapped to a single incident. For example, if a single attacker causes a number of different patterns to be matched, those are grouped into a single incident. Similarly, if a vulnerability scan uncovers a machine that suffers from a number of different vulnerabilities, these are all grouped into a single incident. Or, if a number of different machines report the same virus, Information Manager creates a single outbreak incident.

2.2 TOE Boundaries and Components

The following sections describe the TOE boundaries and detail the components within the TOE.

2.2.1 Physical Boundaries

The TOE is a combined hardware/software TOE and is defined as the Symantec™ Security Information Manager Version 4.5. Figure 1 – TOE and IT Environment Boundary provides an illustration of the boundaries for the TOE and for the IT Environment:

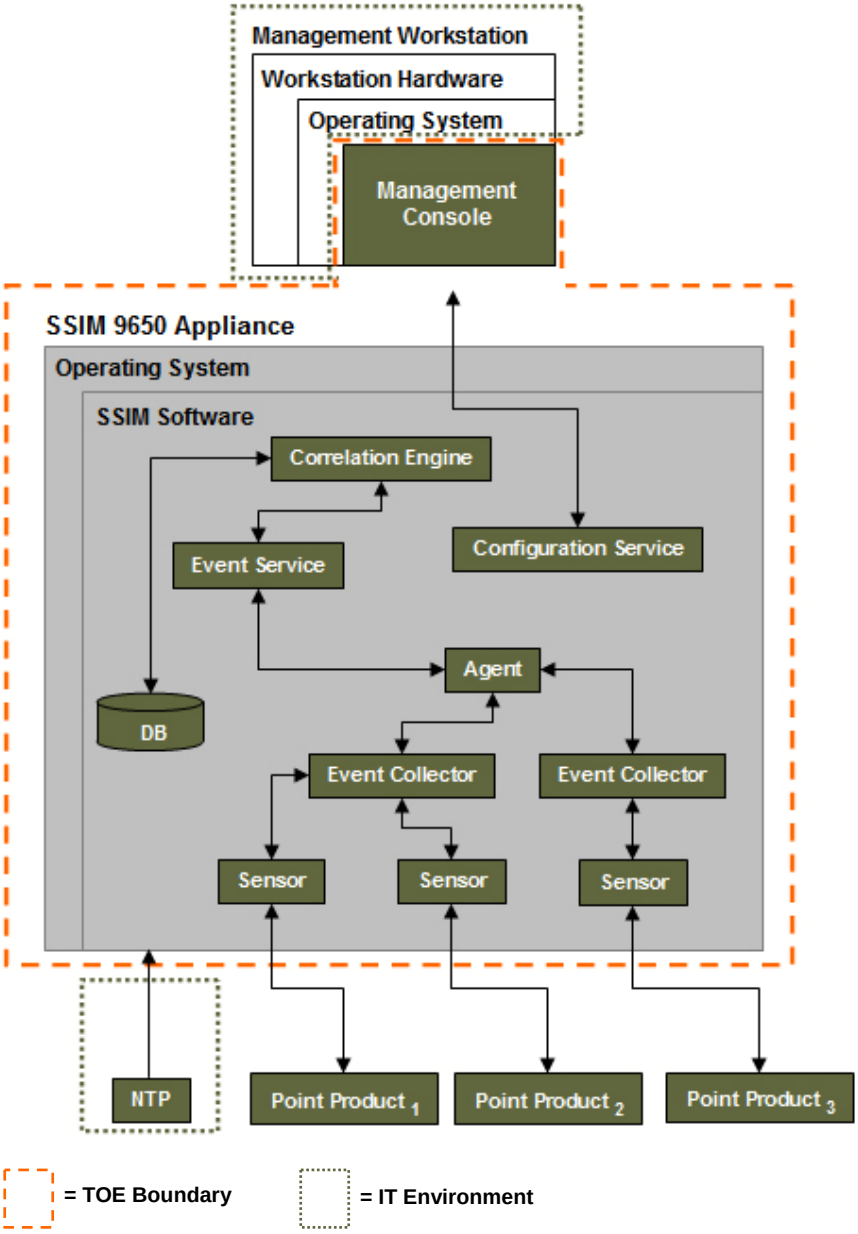

Figure 1 – TOE and IT Environment Boundary

Individual sensor components receive events from a Point Product deployed in the network. Each Event Collector is configured for a specific technology type and can receive information from multiple sensors. For example, in the figure above, *Point Product* $_1$ and *Point Product* $_2$ are similar devices (e.g., each is a firewall).

The table below provides a summary of each subcomponent in the TOE boundary as referenced in Figure 1 – TOE and IT Environment Boundary:

COMPONENT	DESCRIPTION
Agent	Facilitates communicating configuration information and event data between the Event Service and the Event Collector.
Configuration Service	Responsible for configuration for the TOE
Correlation Engine	Provides filters rules to generate correlations in multiple events and creates incidents when a rule is fired. This components also provides all incident management functions.
Database	Stores configuration information, event logs, and reports in addition to events, correlated events, conclusions, and incidents
Event Collector	Receives inbound events from sensors and forwards to the Agent for processing
Event Service	Communicates with Agent to push updated configurations and to receive events for processing and forwarding to the Correlation Engine
Management Console	Allows configuration as well as review of configuration settings and reports. There are two console management interfaces: one is web based and the other is Java-based. The Web-based console is used to configure local items specific to the appliance (such as network settings, date/time, etc.). The Java-based console is used to view incidents, tickets, events and is also used in user & role administration. This application is part of the Information Manager software and downloaded to a workstation via a Web-browser.
Sensor	Receives events from point products attached to the network and forwards to the Event Collector for aggregation.

Table 3 – Summary of Components within the TOE Boundary

In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	Version 4.5.0.113
TOE Hardware	Symantec Security Information Manager 9650

Table 4 – Evaluated Configuration for the TOE

The Linux-based Operating System (Red Hat Enterprise 4 running Kernel v2.6) for the appliance is included as part of the TOE software and is installed when the appliance is provisioned. As such, the Operating System on the TOE hardware is included in the evaluation.

The Management Console must run on a machine that meets the following requirements:

- Windows 2000 Pro SP4
- Windows XP SP2
- Windows 2003 Server SP1
- Windows 2000 Advanced Server SP4
- Minimum screen resolution setting of 1024 x 768 (1280 x 1024 recommended)

- 103 MB disk space
- 512 MB RAM (1 GB recommended)
- Connection to the same network as the appliance

2.2.2 Logical Boundaries

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

2.2.2.1 Security Audit

The TOE generates reports on the event analysis activities. Additionally, the TOE supports the provision of log data from each system component, such as user login/logout and incident/ticket management actions. It also records security events such as failed login attempts, etc. Audit trails can be stored for later review and analysis. Audit data is also collected by the Information Manger from the various devices that send event data, and the TOE analyzes this information against a set of correlation rules and filters.

2.2.2.2 Identification and Authentication

The TOE enforces individual I&A in conjunction with group/role based I&A mechanisms. Operators must successfully authenticate using a unique identifier and password prior to performing any actions on the TOE.

2.2.2.3 Security Management

The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to management of access control policies as well as management of incidents and tickets.

The TOE also allows the administrator to

- review/query audit data,
- modify the behavior of data collection, and
- restrict access to TOE data to the appropriate authorized user/authorized role.

Administrators configure the TOE with the Management Console via Web-based connection using port 443 and port 636.

The TOE normalizes events from multiple security products and looks for patterns that indicate potential threats. Incidents can be created and tracked to resolution.

2.2.2.4 TSF Protection

The TOE provides various protection mechanisms for its security functions, including authentication rules at the applicable interfaces. The TOE also ensures that the TSF is protected against interference and tampering by untrusted subjects.

2.2.3 TOE Security Functional Policies

The TOE supports the following Security Functional Policy:

2.2.3.1 Administrative Access Control SFP

The TOE implements an access control SFP named *Administrative Access Control SFP*. This SFP determines and enforces the privileges associated with operator roles. An authorized administrator can define specific services available to administrators and users via the Management Console.

3 TOE Security Environment

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used
- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply

3.1 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The assumptions are ordered into three groups: personnel, physical environment, and operational assumptions.

The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The operational environment must be managed in accordance with assurance requirements documentation for delivery, operation, and user/administrator guidance. The following specific conditions are assumed to exist in an environment where the TOE is employed.

3.1.1 Personnel Assumptions

A.MANAGE Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.

A.NOEVIL Administrators of the TOE and users on the local area network are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.1.2 Physical Environment Assumptions

A.LOCATE The processing platforms on which the TOE resides are assumed to be located within a facility that provides controlled access.

3.1.3 Operational Assumptions

A.CONFIG The TOE is configured to receive all events from network-attached devices.

A.TIMESOURCE The TOE has a trusted source for system time via NTP server.

3.2 Threats

The TOE and IT environment address the threats identified in the following sections.

3.2.1 Threats Addressed by the TOE and the IT Environment

The TOE addresses the following threats:

T.NO_AUTH	An unauthorized user may gain access to the TOE and alter the TOE configuration.
T.NO_PRIV	An authorized user of the TOE exceeds his/her assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data.

3.3 Organizational Security Policies

The organizational security policies relevant to the operation of the TOE are as follows:

P.EVENTS	All events from network-attached devices shall be monitored and reported.
P.INCIDENTS	Security events correlated and classified as incidents should be managed to resolution.

4 Security Objectives

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

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

O.CAPTURE_EVENT The TOE shall collect data (in the form of events) from security and non-security products and apply analytical processes to derive conclusions about events.

O.MANAGE_INCIDENT The TOE shall provide a workflow to manage incidents.

O.SEC_ACCESS The TOE shall ensure that only those authorized users and applications are granted access to security functions and associated data.

O.TOE_PROTECT The TOE operating system shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.

4.2 Security Objectives for the IT Environment

The IT security objectives for the IT environment are addressed below:

OE.TIME The TOE operating environment shall provide an accurate timestamp (via reliable NTP server).

OE.ENV_PROTECT The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.

4.3 Security Objectives for the Non-IT Environment

The non-IT security objectives listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

ON.PERSONNEL Authorized administrators are non-hostile and follow all administrator guidance and must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted not to disclose their

	authentication credentials to any individual not authorized for access to the TOE.
ON.PHYSEC	The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access into the facility.

5 IT Security Requirements

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

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table. These security requirements are defined in Sections 5.1 - 5.4.

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
User Data Protection	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security Attribute Based Access Control
	FDP_ITC.1	Import of User Data without Security Attributes
Identification and Authentication	FIA_UAU.2	User Authentication before Any Action
	FIA_UID.2	User Identification before Any Action
Security Management	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	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
	FPT_SEP.1	TSF Domain Separation
Incident Management	SIM_ANL.1 (EXP)	Event Analysis
	SIM_RES.1 (EXP)	Incident Resolution

Table 5 – TOE Security Functional Requirements

5.1 TOE Security Functional Requirements

The SFRs defined in this section are derived from Part 2 of the CC unless otherwise noted with "(EXP)" following the requirement description. Rationale for explicitly stated requirements can be found in Section 8.4 - Rationale for Explicitly Stated Security Requirements.

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 *not specified* level of audit; and

c) [Startup and shutdown of TOE services

d) Operator authentication attempts

e) Reports listed in Table 7 – Default Query Groups

f) Reports associated with management of incidents

g) System Status details listed in Table 10 – System Event Descriptions].

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 information].

5.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [the Administrator] with the capability to read [all audit data generated within the TOE] 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.

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [Administrative Access Control SFP] on [

Subjects: All operators

Objects: System reports[1], audit logs, appliance configurations, operator

[1] System reports that have been marked for distribution are not subject to access control

account attributes

Operations: all operator actions].

5.1.2.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [Administrative Access Control SFP] to objects based on the following: [

Subjects: All operators

Objects: System reports[2], audit logs, appliance configurations, operator account attributes

Operations: all operator actions].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [See Table 11 – Roles and Functions].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no additional rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [no additional explicit denial rules].

5.1.2.3 FDP_ITC.1 Import of User Data without Security Attributes

FDP_ITC.1.1 The TSF shall enforce the [Administrative Access Control SFP] when importing user data, controlled under the SFP, from outside the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [no additional importation control rules].

5.1.3 Identification and Authentication (FIA)

5.1.3.1 FIA_UAU.2 User Authentication before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.3.2 FIA_UID.2 User Identification before Any Action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other

[2] System reports that have been marked for distribution are not subject to access control

TSF-mediated actions on behalf of that user.

5.1.4 Security Management (FMT)

5.1.4.1 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [Administrative Access Control SFP] to restrict the ability to *modify and delete* the security attributes [Accounts, privileges] to [an authorized administrator].

5.1.4.2 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Administrative Access Control SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.4.3 FMT_SMF.1 Specification of Management Functions

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

- [Create accounts
- Modify accounts
- Define privilege levels
- Determine the behavior of the Administrative Access Control SFP
- Modify the behavior of the Administrative Access Control SFP
- Manage security incidents
- Manage rules

].

5.1.4.4 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Administrator, User].

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

5.1.5 Protection of the TSF (FPT)

5.1.5.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

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

5.1.5.2 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.

5.1.5.3 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.

5.1.6 Incident Management (SIM)

5.1.6.1 SIM_ANL.1 Event Analysis (EXP)

SIM_ANL.1.1 The TSF shall perform [filtering and correlation] analysis function(s) on data collected.

5.1.6.2 SIM_RES.1 Incident Resolution (EXP)

SIM_RES.1.1 The TSF shall provide a means to track work items that are necessary to resolve an incident.

5.2 Security Functional Requirements for the IT Environment

5.2.1 Protection of the TSF (FPT)

5.2.1.1 FPT_RVM_OS.1 Non-Bypassability of the TSP for OSs (EXP)

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_RVM by themselves. This explicitly stated SFR states the portion of FPT_RVM supplied by the OS and hardware in support of the overall FPT_RVM functionality. See FPT_RVM.1 (levied on the TOE) for the remaining functionality.

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

5.2.1.2 FPT_SEP_OS.1 TSF Domain Separation for OSs (EXP)

Rationale for explicitly stated SFR: Application TOEs are unable to fully satisfy FPT_SEP by themselves. This explicitly stated SFR states the portion of FPT_SEP supplied by the OS and hardware in support of the overall FPT_SEP functionality. See FPT_SEP.1 and (levied on the

TOE) for the remaining functionality.

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

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

5.2.1.3 FPT_STM.1 Reliable Time Stamps

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

5.3 Security Requirements for the Non-IT Environment

There are no security requirements for the non-IT environment.

5.4 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are derives from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2). The assurance components are summarized in the following table:

ASSURANCE CLASS	ASSURANCE COMPONENTS	
Configuration Management	ACM_CAP.2	Configuration items
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 6 – Security Assurance Requirements at EAL2

6 TOE Summary Specification

This section presents the Security Functions implemented by the TOE and the Assurance Measures applied to ensure their correct implementation.

6.1 TOE Security Functions

The security functions described in the following subsections fulfill the security requirements that are defined in Section 5.1 – TOE Security Functional Requirements. The security functions performed by the TOE are as follows:

- Security Audit
- Identification and Authentication
- Security Management
- TSF Protection

6.1.1 Security Audit

The TOE provides two types of audits:

1. Security events – aggregation and correlation of event data received from security products deployed in the network and
2. System events – audit data relating to the management and general function of the TOE.

The sections below describe each type of audit in more detail.

6.1.1.1 Security Events

Reports are available to operators (e.g., Administrators and Users) through the Dashboard, a function of the Management Console that provides an at-a-glance summary of the status of security products on the network. Operators can access canned reports or can create queries to generate custom reports using one or more queries.

The following table shows how queries are grouped in the Information Manager console and describes each query group:

QUERY GROUP	DESCRIPTION
All	This general category currently contains only one query: *Event Counts by Severity Last 7 Days*.
Compliance Templates	This group contains event queries to generate specific event views.
Product Queries	This group contains subgroups of queries, one subgroup for each collector that is installed, for example, Symantec Client Security.
SSIM	These queries are specific to Information Manager, and they are organized into product function subgroups.

QUERY GROUP	DESCRIPTION
Security Queries	This group contains event queries, which are grouped by device types that report the events, for example, intrusion devices.

Table 7 – Default Query Groups

Information Manager allows customization of the appearance of the output. Additionally, reports can remain private or can be published and distributed for use by other security analysts. When publishing a report, the operator can define whether the published report should be distributed immediately, or they can specify a time or recurring time interval for distribution.

6.1.1.1.1 Reviewing Events

Information Manager provides the following search templates, allowing basic queries on the event archives:

PARAMETER	RESULT
Recent Events	Displays a table that contains the most recent event information in table form.
IP Address Activity	Displays a search template to query for event records that include a specific IP address.
Host Activity	Displays a search template to query for event records that include a specific host name.
User Activity	Displays a search template to query for event records that include a specific user name.
Port Activity	Displays a search template to query for event records that include a specific port number.

Table 8 – Default Event Search Queries

Users also have the ability to create custom queries to search events.

The following table summarizes the event correlation rules supported by the TOE:

CATEGORY	DESCRIPTION
Rules List	Displays the list of default rules in the System Rules folder and custom rules in the User Rules folder. The User can use the checkboxes to turn rules on and off.
Conditions	Displays the event criteria that are used by rules to declare a security incident. When creating a custom rule, the User can add or remove event criteria from this pane.
Actions	Lets the User specify the follow-up actions that are required to resolve the incident. The User can also specify the user or team who will be assigned to investigate and resolve the incident.

CATEGORY	DESCRIPTION
Testing	Lets the User test rules with saved event data, so they can evaluate whether the rule declares incidents when it should. This tool helps fine-tune a rule to filter out events that cause false positives. The User can also debug errors that are preventing the rule from declaring incidents when it should.
History	Shows the date and time when a User last edited a rule.

Table 9 – Event Correlation Rules

6.1.1.2 System Events

The TOE also supports robust system logging capability; Users can monitor the health and performance of the TOE from the Management Console. The following table summarizes the system event data available:

CATEGORY	DESCRIPTION
System Status	Displays the appliance's memory and CPU utilization, the database statistics, and the status of any database jobs, such as backup or purge.
System	Displays processing rate statistics for system processes such as correlating events, declaring conclusions, and inserting incident data into the Information Manager database.
Filters	Displays filtering statistics for the correlation engine. Users can monitor the Filter tab to determine how many events are being excluded from the correlation engine.
Rules	Displays trigger statistics for each correlation rule. Users can monitor the Rules tab to confirm that rules are being triggered as expected.
Event Service	Displays rate statistics for the following event services: • Events received • Event relays • Event normalization • Event archiving • Event correlation forwarding
Administration	View and maintain administrative information, such as User accounts and roles, policies, and paging services.
Appliance Configurations	Manage event archiving options, such as determining how long to save events before purging the archive.
Product Configurations	Displays a list of all the security products that can be managed on the network.
Visualizer	Displays an illustration that represents the Information Manager network.

Table 10 – System Event Descriptions

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

- FAU_GEN.1
- FAU_SAR.1
- SIM_ANL.1 (EXP)

6.1.2 Identification and Authentication

The TOE enforces individual identification and authentication and provides a centralized authentication mechanism. Operators with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE (whether those actions are reviewing reports/component logs, managing operator accounts, or configuring TOE components). Identification and Authentication occurs via management GUI interfacing with the Appliance or via directly attached console port on the appliance.

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

- FIA_UAU.2
- FIA_UID.2

6.1.3 Security Management

6.1.3.1 Access Control

The TOE maintains the operator roles described in the following table. The individual roles are categorized into two main roles: the Administrator and the User.

ROLE	MANAGEMENT FUNCTIONS
Administrator	
SES Administrator	Maintains full authority over all of the domains in the environment
Domain Administrator	Maintains full authority over one specific domain in the environment
System Administrator	Manages Information Manager. Verifies that events are flowing into the system and that the system is functioning normally
User Administrator	• Creates correlation rules and collection filters • Performs user and device administration

ROLE	MANAGEMENT FUNCTIONS
User	
Incident Manager	Views all incidents, events, reports, and actions
Report Writer	• Views incidents, events, and reports for assigned devices • Reviews and validates incident response • Provides attestation of incident review and response by administrators to GAO and others
Report User	Views events and reports for assigned devices
Rule Editor	Creates, edits, and deploys rules

Table 11 – Roles and Functions

6.1.3.2 Incident Management

The TOE facilitates management of security incidents and alerting (non-security) incidents. An incident is derived from one or more events that are logged in the event database. For example, when a firewall-down event occurs, an alerting incident could be generated. A security incident might be created when an internal port sweep event occurs. The term "incidents" includes both security incidents and alerting incidents.

Incident management begins when an incident is created. Information Manager provides two methods of incident creation:

1. Automatic incident creation – the Correlation Engine creates incidents from events, and then the events are assigned according to automatic assignment rules.
2. Manual incident creation – the User determines which events are related and manually correlates the events by grouping them as a single incident.

After an event or group of events is selected and identified as an incident, the incident is assigned to an analyst for investigation and resolution. Information Manager provides the analyst with recommended actions to be completed. A history log tracks any changes to the incident and lets the analyst note important facts.

The following incident management activities are available to an authorized User:

- View incidents
- Create or modify incidents
- Filter incidents
- Create tickets from incidents
- Close incidents

As Users work through the incidents that are logged in the TOE, products affected by the incident may require specific tasks to resolve the incident or to prevent further incidents.

The TOE supports the import of user data without security attributes. Imported user data includes existing/emerging vulnerability, threat, and risk information that is downloaded from Symantec Global Intelligence Network, a comprehensive collection of vendor-neutral security data sources of information about known and emerging vulnerabilities, threats, risks and global attack activity. This user data is imported from Symantec Global Intelligence Network via SSL session to the Correlation Engine component of the TOE.

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

- FDP_ACC.1
- FDP_ACF.1
- FDP_ITC.1
- FMT_MSA.1
- FMT_MSA.3
- FMT_SMF.1
- FMT_SMR.1
- SIM_RES.1 (EXP)

6.1.4 TSF Protection

The TOE is integrated into a network, and only an approved, authenticated Administrator can install, configure, and modify the TOE components (and all TOE Security Functions), which provides a protected domain for the TSFs. The appliance subsystem is self-contained; therefore, it maintains its own execution domain and the device performs all intrinsic security functions. The Management Console subsystem[3] and its environment protects security functions via the host operating system, which maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects in the scope of control of the host OS.

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

- FPT_ITT.1
- FPT_RVM.1
- FPT_SEP.1

6.2 Strength of Function for the TOE

This security target includes a number of probabilistic or permutational functions. Relevant security functions and security functional requirements include:

[3] The Console Management Application is downloaded from a 9600 Console appliance to a management workstation via Web-browser

- Identification and Authentication
    - FIA_UAU.2 – User Authentication before Any Action
    - FIA_UID.2 – User Identification before Any Action

The SOF for these mechanisms is SOF-Basic.

6.3 Security Assurance Measures

This section identifies the Configuration Management, Delivery/Operation, Development, Guidance Documents, Test, and Vulnerability Assessment measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES	DESCRIPTION
ACM_CAP.2	CM_DOC	Configuration items: The implementation and documentation of procedures for the development of the TOE, including a configuration list of uniquely identified items. Evidence Title: *Configuration Management Processes and Procedures: Symantec™ Security Information Manager Version 4.5*
ADO_DEL.1	DEL_DOC	Delivery procedures: The implementation and documentation of procedures for delivering the TOE to a customer in a secure manner. Evidence Title: *Secure Delivery Processes and Procedures: Symantec™ Security Information Manager Version 4.5*
ADO_IGS.1	IGS_DOC	Installation, generation, and start-up procedures: Documentation provided to the end users instructing the end users how to install and configure the TOE in a secure manner. Evidence Titles: *Symantec™ Security Information Manager Version 4.5 Installation Guide* *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Security Information Manager Version 4.5*
ADV_FSP.1	FSP_DOC	Informal functional specification: Functional Specification for the TOE describing the TSF and the TOE's external interfaces. Evidence Title: *Functional Specification: Symantec™ Security Information Manager Version 4.5*
ADV_HLD.1	HLD_DOC	Descriptive high-level design: System Design for the TOE providing descriptions of the TSF structure in the form of subsystems and the functionality of each subsystem. Evidence Title: *High Level Design and Representation Correspondence Analysis: Symantec™ Security*

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES	DESCRIPTION
		Information Manager Version 4.5
ADV_RCR.1	RCR_DOC	Informal correspondence demonstration: The documentation of the correspondence between the TSS, FSP and HLD in specifically provided deliverables. Evidence Title: *High Level Design and Representation Correspondence Analysis: Symantec™ Security Information Manager Version 4.5*
AGD_ADM.1	ADMIN_GUIDE	Administrator guidance: Documentation provided to the customers instructing the customer how to configure the TOE in a secure manner. Evidence Titles: *Symantec™ Security Information Manager Version 4.5 Administrator's Guide* *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Security Information Manager Version 4.5*
AGD_USR.1	USER_GUIDE	User guidance: Documentation provided to the customers instructing the users how to use the TOE. Evidence Title: *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Security Information Manager Version 4.5*
ATE_COV.1	TEST_COV	Evidence of coverage: Documented correspondence between the security functions and tests. Evidence Title: *Test Plan and Coverage Analysis: Symantec™ Security Information Manager Version 4.5*
ATE_FUN.1	TEST_DOC	Functional testing: The implementation and documentation of the test procedures including expected and actual results. Evidence Title: *Test Plan and Coverage Analysis: Symantec™ Security Information Manager Version 4.5*

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES	DESCRIPTION
AVA_SOF.1	SOF_DOC	Strength of TOE security function evaluation: The documentation for the Strength of Function Assessment. Evidence Title: *Vulnerability Analysis and Strength of Function Claims: Symantec™ Security Information Manager Version 4.5*
AVA_VLA.1	VLA_DOC	Developer vulnerability analysis: Vulnerability Assessment of the TOE and its deliverables is performed and documented to ensure that identified security flaws are countered. Evidence Title: *Vulnerability Analysis and Strength of Function Claims: Symantec™ Security Information Manager Version 4.5*

Table 12 – Assurance Measures (EAL2)

7 Protection Profile Claims

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

8 Rationale

8.1 Rationale for Security Objectives of the TOE, IT Environment, and Non-IT Environment

8.1.1 Summary Mapping of Security Objectives

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

OBJECTIVE / THREATS/ ASSUMPTIONS	O.CAPTURE_EVENT	O.MANAGE_INCIDENT	O.SEC_ACCESS	O.TOE_PROTECT	OE.TIME	OE.ENV_PROTECT	ON.PERSONNEL	ON.PHYSEC
ASSUMPTIONS								
A.CONFIG	✓						✓	
A.MANAGE			✓				✓	
A.NOEVIL							✓	
A.LOCATE								✓
A.TIMESOURCE					✓			
THREATS								
T.NO_AUTH			✓	✓		✓	✓	✓
T.NO_PRIV			✓					
OSPs								
P.EVENTS	✓				✓		✓	
P.INCIDENTS		✓			✓		✓	

Table 13 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

8.1.2 Rationale for Security Objectives of the TOE

A.CONFIG — This assumption is addressed by O.CAPTURE_EVENT, which ensures that the TOE collects security events from security products and non-

	security products deployed within a network and applies analytical processes to derive conclusions about the events.
A.MANAGE	This assumption is addressed by O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications.
T.NO_AUTH	This threat is countered by the following: • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications and • O.TOE_PROTECT, which provides mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.
T.NO_PRIV	This threat is countered by O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications.
P.EVENTS	This organizational security policy is enforced by O.CAPTURE_EVENT, which ensures that the TOE collects security events from security products and non-security products deployed within a network and applies analytical processes to derive conclusions about the events.
P.INCIDENTS	This organizational security policy is enforced by O.MANAGE_INCIDENT, which ensures that the TOE will provide the capability to provide workflow functionality to manage the resolution of incidents.

8.1.3 Rationale for Security Objectives of the IT Environment

The IT security objectives for the IT environment are addressed below:

A.TIMESOURCE	This assumption is addressed by OE.TIME, which ensures the provision of an accurate time source.
T.NO_AUTH	This threat is countered by OE.ENV_PROTECT, which ensures that TSF components cannot be tampered with or bypassed.
P.EVENTS	OE.TIME provides support for enforcement of this policy by ensuring the provision of an accurate time source.

P.INCIDENTS	OE.TIME provides support for enforcement of this policy by ensuring the provision of an accurate time source.

8.1.4 Rationale for Security Objectives of the Non-IT Environment

The non-IT security objectives listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

A.MANAGE	This assumption is addressed by ON.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.
A.NOEVIL	This assumption is addressed by ON.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.
A.CONFIG	This assumption is addressed by ON.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.
A.LOCATE	This assumption is addressed by ON.PHYSEC, which ensures that the TOE is operated in an environment that will protect it from unauthorized access and physical threats and attacks that can disturb and corrupt the information generated.
T.NOAUTH	This threat is countered by the following: • ON.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.

- ON.PHYSEC, which ensures that the TOE is operated in an environment that will protect it from unauthorized access and physical threats and attacks that can disturb and corrupt the information generated.

P.EVENTS — ON.PERSONNEL provides support for the enforcement of this policy by ensuring that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.

P.INCIDENTS — ON.PERSONNEL provides support for the enforcement of this policy by ensuring that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner.

8.2 Security Requirements Rationale

8.2.1 Summary of TOE Security Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVE / SFR	O.CAPTURE_EVENT	O.MANAGE_INCIDENT	O.SEC_ACCESS	O.TOE_PROTECT	OE.ENV_PROTECT
FAU_GEN.1	✓	✓			
FAU_SAR.1	✓	✓			
FDP_ACC.1			✓		
FDP_ACF.1			✓		
FDP_ITC.1	✓	✓			
FIA_UAU.2			✓		

OBJECTIVE / SFR	O.CAPTURE_EVENT	O.MANAGE_INCIDENT	O.SEC_ACCESS	O.TOE_PROTECT	OE.ENV_PROTECT
FIA_UID.2			✓		
FMT_MSA.1			✓		
FMT_MSA.3			✓		
FMT_SMF.1		✓			
FMT_SMR.1		✓			
FPT_ITT.1				✓	✓
FPT_RVM.1				✓	
FPT_SEP.1				✓	
SIM_ANL.1 (EXP)	✓				
SIM_RES.1 (EXP)		✓			
FPT_RVM_OS.1					✓
FPT_SEP_OS.1					✓

Table 14 – Mapping of TOE Security Functional Requirements and Objectives

8.2.2 Sufficiency of Security Requirements

This section confirms that the security requirements are sufficient to satisfy the TOE security objectives, whether in a principal or supporting role.

OBJECTIVE	ARGUMENT TO SUPPORT SUFFICIENCY OF SECURITY REQUIREMENTS
O.CAPTURE_EVENT	The objective to ensure that the TOE will collect events from security products and non-security products deployed within a network and applies analytical processes to derive conclusions about the events is met by the following security requirements: • FAU_GEN.1 and FAU_SAR.1 define the auditing capability for events and administrative access control and requires that authorized users will have the capability to read and interpret

OBJECTIVE	ARGUMENT TO SUPPORT SUFFICIENCY OF SECURITY REQUIREMENTS
	data stored in the audit logs • FDP_ITC.1 allows the import of user data from outside the TSC (such as threat, vulnerability, and attack activity information provided by Symantec Global Intelligence Network) to help ensure the latest vulnerabilities and threats are reported. • SIM_ANL.1 (EXP) ensures that the TOE performs analysis on all security events received from network devices
O.MANAGE_INCIDENT	The objective to ensure that the TOE provides a workflow to manage incidents is met by the following security requirements: • FAU_GEN.1 and FAU_SAR.1 define the auditing capability for incidents and administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs • FDP_ITC.1 allows the import of user data from outside the TSC (such as threat, vulnerability, and attack activity information provided by Symantec Global Intelligence Network) to help ensure the latest vulnerabilities and threats are reported. • FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role • SIM_RES.1 (EXP) ensures that the TOE provides the capability to manage status and track action items in the resolution of incidents
O.SEC_ACCESS	This objective ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications. • FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions and configuration data are controlled • FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions, configuration data, audit logs, and account attributes is based on the user privilege level and their allowable actions • FIA_UAU.2 and FIA_UID.2 require the TOE to enforce identification and authentication of all users prior to configuration of the TOE • FMT_MSA.1 specifies that only privileged administrators can access the TOE security functions and related configuration data • FMT_MSA.3 ensures that the default values of security

OBJECTIVE	ARGUMENT TO SUPPORT SUFFICIENCY OF SECURITY REQUIREMENTS
	attributes are restrictive in nature as to enforce the access control policy for the TOE • FPT_SEP.1 ensures that a separate execution domain is maintained by the TOE to help prevent unauthorized access to the TOE
O.TOE_PROTECT	The objective to ensure that the TOE provides mechanisms to isolate the TOE Security Functions (TSF) and assures that TSF components cannot be tampered with or bypassed is met by the following: • FPT_ITT.1 ensures that communications between TOE components are protected via SSL tunnel. • FPT_SEP.1 ensures that the TOE is protected from untrusted processes that could attempt to tamper with or bypass the TOE. • FPT_RVM.1 ensures that the TOE is not bypassed (e.g., the TOE collects all security events)
OE.TIME	The objective to ensure that the TOE operating environment provides an accurate timestamp is met by the following: • FPT_STM.1 requires the provision of reliable time stamps that can be associated with security-relevant events
OE.ENV_PROTECT	The objective to ensure that the TOE Environment provides mechanisms to isolate the TOE Security Functions (TSF) and assures that TSF components cannot be tampered with or bypassed is met by the following: • FPT_ITT.1 ensures that communications between TOE components are protected via SSL tunnel. • FPT_SEP_OS.1 ensures that the Management Console portion of the TOE, which runs on a host machine in the IT Environment, is protected from untrusted processes that could attempt to tamper with or bypass the TOE • FPT_RVM_OS.1 levied on the environment ensures that the Management Console portion of the TOE, which runs on a host machine in the IT Environment, is not bypassed.
ON.PERSONNEL	The objective to ensure that authorized administrators are non-hostile and follow all administrator guidance and that the TOE is delivered, installed, managed, and operated in a secure manner is met by the following: • A.MANAGE assumes Administrators of the TOE are appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner. • A.NOEVIL assumes the Administrator is not careless, willfully

OBJECTIVE	ARGUMENT TO SUPPORT SUFFICIENCY OF SECURITY REQUIREMENTS
	negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation. • A.LOCATE assumes the processing platform on which the TOE resides is assumed to be located within a facility that provides controlled access.
ON.PHYSEC	The objective to ensure that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility is met by the following: • A.LOCATE assumes the processing platform on which the TOE resides is assumed to be located within a facility that provides controlled access.

Table 15 – Sufficiency of Security Requirements

8.3 TOE Summary Specification Rationale

The following table provides a mapping of Security Functional Requirements to IT Security Functions:

IT SECURITY FUNCTION / TOE SFR	SECURITY AUDIT	IDENTIFICATION AND AUTHENTICATION	SECURITY MANAGEMENT	TSF PROTECTION
FAU_GEN.1	✓			
FAU_SAR.1	✓			
FDP_ACC.1			✓	
FDP_ACF.1			✓	
FDP_ITC.1			✓	
FIA_UAU.2		✓		
FIA_UID.2		✓		
FMT_MSA.1			✓	
FMT_MSA.3			✓	

IT SECURITY FUNCTION / TOE SFR	SECURITY AUDIT	IDENTIFICATION AND AUTHENTICATION	SECURITY MANAGEMENT	TSF PROTECTION
FMT_SMF.1			✓	
FMT_SMR.1			✓	
FPT_ITT.1				✓
FPT_RVM.1				✓
FPT_SEP.1				✓
SIM_ANL.1 (EXP)	✓			
SIM_RES.1 (EXP)			✓	

Table 16 – Mapping of Security Functional Requirements to IT Security Functions

8.3.1 Sufficiency of IT Security Functions

This section provides appropriate justification that the IT Security Functions are suitable to meet the TOE Security Functional Requirement and that when implemented, contributes to meeting that requirement.

SFR	RATIONALE TO SUPPORT SUFFICIENCY OF SECURITY FUNCTION
FAU_GEN.1	This TOE SFR is satisfied by the Security Audit function, which generates audit logs and summary reports various security events.
FAU_SAR.1	This TOE SFR is satisfied by the Security Audit function by enabling only authorized users to review and query the audit logs and reports.
FDP_ACC.1	This TOE SFR is satisfied by the Security Management function, which permits each user to be assigned a privilege level and the respective privileges for that level and only allow access to event and incident management functions for which the user is authorized.
FDP_ACF.1	This TOE SFR is satisfied by the Security Management function by permitting TOE access based on the privileges assigned a specific privilege level.
FDP_ITC.1	This TOE SFR is satisfied by the Security Management function, which process the information entering the system. The TOE allows the import of user data from outside the TSC (in this case, information from Symantec Global Intelligence Network) to help ensure the latest threats and

	vulnerabilities are detected and recorded.
FIA_UAU.2	This TOE SFR is satisfied by the Identification and Authentication security function by requiring operators to successfully authenticate themselves using a unique identifier and password prior to performing any action on the TOE.
FIA_UID.2	This TOE SFR is satisfied by the Identification and Authentication security function by requiring operators to successfully identify themselves using a unique identifier.
FMT_MSA.1	This TOE SFR is satisfied by Security Management function, which provides the TOE Administrator with full authority and ability to define user groups and their privileges. These security functions also provide complete control (via configuration) over the security functions of the TOE.
FMT_MSA.3	This TOE SFR is satisfied by Security Management function, which allows the TOE Administrator to change default settings for each operator and privilege level.
FMT_SMF.1	This TOE SFR is satisfied by Security Management function by providing the TOE Administrator the capability for the administrator to select the type of information structure with respect to selected services to be monitored and processed, and the ability to install and configure the TOE services. The Security Management function also provides the capability to modify operator accounts and privilege levels.
FMT_SMR.1	This TOE SFR is satisfied by Security Management function, which assigns each operator to the role of Administrator or User, the latter of which has a subset of Administrator services. These subset services are defined by the Administrator at the time the account is created.
FPT_ITT.1	This TOE SFR is satisfied by the TSF Protection security functions by ensuring that communications between the Management Console and appliance are protected with SSL encryption.
FPT_RVM.1	This TOE SFR is satisfied by the TSF Protection security function by ensuring that all events are captured and analyzed by the TOE.
FPT_SEP.1	This TOE SFR is satisfied by the TSF Protection security function by ensuring the TOE provides protection mechanisms for its security functions, such as the restricted ability that only TOE Administrators can perform administrative actions on the TOE.
SIM_ANL.1 (EXP)	This TOE SFR is satisfied by the Security Audit security function, which provides mechanisms to collect, correlate, and view audit data from network-attached devices.
SIM_RES.1 (EXP)	This TOE SFR is satisfied by the Security Management security function, which provides mechanisms to report and manage incidents and track their resolution.

Table 17 – Sufficiency of IT Security Functions

8.4 Rationale for Explicitly Stated Security Requirements

A family of Security Information Management (SIM) requirements was created to specifically address the data collected, analyzed, and managed by a SIM solution. The purpose of this family is to address the unique nature of SIM solutions and provide requirements about collecting events and managing incidents. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

8.5 Rationale for IT Security Requirement Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FDP_ACC.1	No other components.	FDP_ACF.1	Satisfied
FDP_ACF.1	No other components.	FDP_ACC.1	Satisfied
		FMT_MSA.3	Satisfied
FDP_ITC.1	No other components	FDP_IFC.1 FMT_MSA.3	Satisfied
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1
FIA_UID.2	FIA_UID.1	None	Not applicable
FMT_MSA.1	No other components.	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	Satisfied
FMT_MSA.3	No other components.	FMT_SMR.1 FMT_MSA.1	Satisfied
FMT_SMF.1	No other components.	None	Not applicable
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1
FPT_ITT.1	No other components	None	Not applicable
FPT_RVM.1	No other components.	None	Not applicable

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FPT_SEP.1	No other components.	None	Not applicable
SIM_ANL.1 (EXP)	No other components.	None	Not applicable
SIM_RES.1 (EXP)	No other components.	None	Not applicable

Table 18 – TOE SFR Dependency Rationale

8.6 Rationale for Strength of Function Claim

The TOE is targeted at a generalized IT environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have a low attack potential. As such, minimum and explicit strength of function claims is “SOF-basic” which is appropriate for the intended environment. Note that the only applicable mechanisms (i.e., those that are probabilistic or permutational yet not cryptographic) are related to the identification and authentication security function and specifically to the following security functional requirements: FIA_UAU.2, FIA_UID.2.

8.7 Rationale for Security Assurance

The assurance documentation listed in Table 12 – Assurance Measures (EAL2) meets the developer action and content and presentation of evidence elements for each assurance requirement defined in the CC. 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.

8.8 Protection Profile Claims Rationale

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

