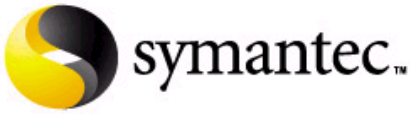
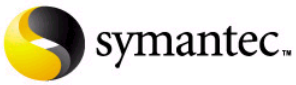


Security Target: Symantec™ Network Access Control Version 11.0

ST Version 1.6

June 19, 2008

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™ Network Access Control Version 11.0. 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	October 9, 2007	Initial release
1.1	November 12, 2007	Address initial comments from EWA-Canada
1.2	December 12, 2007	Address initial verdicts from EWA-Canada
1.3	March 13, 2008	Address additional verdicts from EWA-Canada
1.4	May 30, 2008	Revise role descriptions and minor updates to SFRs
1.5	June 5, 2008	Minor edits
1.6	June 19, 2008	Final edits and include OS detail in TOE Boundary section per new CSEC requirements

Table of Contents

1 INTRODUCTION 6

1.1 IDENTIFICATION 6
1.2 OVERVIEW 6
1.3 CC CONFORMANCE CLAIM 6
1.4 ORGANIZATION 6
1.5 DOCUMENT CONVENTIONS 7
1.6 DOCUMENT TERMINOLOGY 8

2 TOE DESCRIPTION 9

2.1 PRODUCT TYPE 9
2.2 FUNCTIONALITY OVERVIEW 9
2.3 PRODUCT DESCRIPTION 11
2.3.1 Symantec Network Access Control Client 11
2.3.2 Symantec Enforcer 6100 Series 12
2.3.3 Symantec Endpoint Protection Manager 12
2.4 TOE BOUNDARIES 13
2.4.1 Physical Boundary Configuration 13
2.4.2 Logical Boundaries 15
2.4.2.1 Audit 15
2.4.2.2 Information Flow Control 15
2.4.2.3 Management 16
2.4.3 TOE Security Functional Policies 16
2.4.3.1 NAC Information Flow Control SFP 16

3 TOE SECURITY ENVIRONMENT 17

3.1 SECURE USE ASSUMPTIONS 17
3.2 THREATS TO SECURITY 17
3.2.1 Threats Addressed by the TOE 17
3.2.2 Threats Addressed by Operating Environment 18
3.3 ORGANIZATIONAL SECURITY POLICIES 18

4 SECURITY OBJECTIVES 19

4.1 SECURITY OBJECTIVES FOR THE TOE 19
4.2 SECURITY OBJECTIVES FOR THE IT ENVIRONMENT 19
4.3 SECURITY OBJECTIVES FOR THE NON-IT ENVIRONMENT 20

5 IT SECURITY REQUIREMENTS 21

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 22
5.1.1 Security Audit (FAU) 22
5.1.1.1 FAU_GEN.1 Audit Data Generation 22
5.1.1.2 FAU_GEN.2 User Identity Association 23
5.1.1.3 FAU_SAR.1(1) Audit Review 23
5.1.1.4 FAU_SAR.1(2) Audit Review 23
5.1.1.5 FAU_SAR.2 Restricted Audit Review 23
5.1.1.6 FAU_SAR.3 Selectable Audit Review 24
5.1.1.7 FAU_STG.1 Protected Audit Trail Storage 24
5.1.1.8 FAU_STG.4 Prevention of Audit Loss 24
5.1.2 User Data Protection (FDP) 24
5.1.2.1 FDP_IFC.1 Subset Information Flow Control 24
5.1.2.2 FDP_IFF.1 Simple Security Attributes 24
5.1.3 Security Management (FMT) 25
5.1.3.1 FMT_MOF.1 Management of Security Functions Behavior 25
5.1.3.2 FMT_MSA.1 Management of security attributes 25

5.1.3.3 FMT_MSA.3 Static Attribute Initialization 26
5.1.3.4 FMT_MTD.1 Management of TSF Data 26
5.1.3.5 FMT_SMF.1 Specification of Management Functions 26
5.1.3.6 FMT_SMR.1 Security Roles 27
5.2 SECURITY FUNCTIONAL REQUIREMENTS FOR THE IT ENVIRONMENT 27
5.2.1 Security Audit (FAU) 27
5.2.1.1 FAU_STG.1 Protected Audit Trail Storage 27
5.2.2 User Data Protection (FDP) 27
5.2.2.1 FDP_RIP.1 Subset Residual Information Protection 27
5.2.3 Identification and Authentication (FIA) 27
5.2.3.1 FIA_AFL.1 Authentication Failure Handling 27
5.2.3.2 FIA_SOS.1 Verification of Secrets 27
5.2.3.3 FIA_UAU.2 User Authentication Before any Action 28
5.2.3.4 FIA_UAU.6 Re-Authenticating 28
5.2.3.5 FIA_UID.2 User Identification Before any Action 28
5.2.3.6 FIA_PLA_EXP.1 Performance and Log Alerts (EXP) 28
5.2.4 Protection of the TSF (FPT) 28
5.2.4.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection 28
5.2.4.2 FPT_RVM.1 Non-Bypassability of the TSP 28
5.2.4.3 FPT_SEP.1 TSF Domain Separation 28
5.2.4.4 FPT_STM.1 Reliable Time Stamps 28
5.2.5 TOE Access (FTA) 29
5.2.5.1 FTA_SSL.1 TSF-Initiated Session Locking 29
5.2.5.2 FTA_TAB.1 Default TOE Access Banners 29
5.3 SECURITY REQUIREMENTS FOR THE NON-IT ENVIRONMENT 29
5.4 TOE SECURITY ASSURANCE REQUIREMENTS 29
5.5 STRENGTH OF FUNCTION FOR THE TOE 30

6 TOE SUMMARY SPECIFICATION 31

6.1 TOE SECURITY FUNCTIONS 31
6.1.1 Audit 31
6.1.2 Information Flow Control 32
6.1.3 Management 34
6.1.3.1 Security Roles 34
6.1.3.2 Security Audit 35
6.1.3.3 Access Control 35
6.2 SECURITY ASSURANCE MEASURES 36

7 PROTECTION PROFILE CLAIMS 40

8 RATIONALE 41

8.1 RATIONALE FOR SECURITY OBJECTIVES OF THE TOE, IT ENVIRONMENT, AND NON-IT ENVIRONMENT 41
8.1.1 Summary Mapping of Security Objectives 41
8.1.2 Rationale for Security Objectives of the TOE 42
8.2 SECURITY REQUIREMENTS RATIONALE 47
8.2.1 Summary of TOE Security Requirements 47
8.2.2 Sufficiency of Security Requirements 48
8.2.3 Summary of IT Environment Security Requirements 51
8.2.4 Sufficiency of Security Requirements for the IT Environment 51
8.3 TOE SUMMARY SPECIFICATION RATIONALE 53
8.3.1 Sufficiency of IT Security Functions 54
8.4 RATIONALE FOR IT SECURITY REQUIREMENT DEPENDENCIES 56
8.5 RATIONALE FOR EXPLICITLY STATED REQUIREMENTS 57
8.6 RATIONALE FOR SECURITY ASSURANCE REQUIREMENTS 58
8.7 RATIONALE FOR STRENGTH OF FUNCTION CLAIM 58
8.8 RATIONALE FOR PROTECTION PROFILE CLAIMS 58

List of Tables

Table 1 – ST Organization and Description....7
Table 2 – Acronyms Used in Security Target....8
Table 3 – Evaluated Configuration for the TOE....14
Table 4 – TOE Security Functional Requirements....21
Table 5 – FAU_GEN.1 Events....23
Table 6 – Security Assurance Requirements....30
Table 7 – Available Reports....32
Table 8 – Description of Roles Supported in the TOE....35
Table 9 – Assurance Measures....39
Table 10 – Mapping of Assumptions, Threats, and OSPs to Security Objectives....42
Table 11 – Mapping of Threats, Policies, and Assumptions to Objective....47
Table 12 – Mapping of TOE Security Functional Requirements and Objectives....48
Table 13 – Rationale for TOE Objectives....50
Table 14 – Mapping of IT Environment Security Functional Requirements and Objectives....51
Table 15 – Rationale for IT Environment Objectives....53
Table 16 – Mapping of Security Functional Requirements to IT Security Functions....54
Table 17 – Sufficiency of IT Security Functions....56
Table 18 – TOE SFR Dependency Rationale....57

List of Figures

Figure 1 – Symantec Network Access Control Process....10
Figure 2 – Architecture Overview....11
Figure 3 – TOE Boundary....15

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: Symantec™ Network Access Control Version 11.0
ST Revision:	1.6
ST Publication Date:	June 19, 2008
TOE Identification:	Symantec™ Network Access Control Version 11.0
Vendor:	Symantec Corporation
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.3
Author:	Apex Assurance Group
Keywords:	Symantec™, network access control, endpoint protection

1.2 Overview

The TOE is Symantec™ Network Access Control Version 11.0, which validates and can enforce policy compliance for all types of endpoints on all types of networks. This validation and enforcement process begins prior to an endpoint's connection to the network and continues throughout the duration of the connection, with policy serving as the basis for all evaluations and actions.

Symantec™ Network Access Control Version 11.0 may hereafter also be referred to as the TOE in this document.

1.3 CC Conformance Claim

The TOE meets the following claims:

- Common Criteria Part 2 Extended and
- Common Criteria Part 3 EAL2 conformant with augmentation to include ALC_FLR.2 and AVA_MSU.1.

1.4 Organization

This Security Target is organized in 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.
- Application notes provide additional information for the reader, but do not specify

requirements. Application notes are denoted by *italicized* text within the functional requirements and are preceded with the text "*Application Note*"

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 acronyms used within this document:

TERM	DEFINITION
AVPP	U.S. Government Protection Profile for Anti-Virus Applications for Workstations in Basic Robustness Environments, Version 1.1, April 4, 2006
CC	Common Criteria
EAL	Evaluation Assurance Level
NAC	Network Access Control
NTP	Network Time Protocol
OSP	Organizational Security Policy
PP	Protection Profile
SEP	Symantec™ Endpoint Protection
SFR	Security Functional Requirement
SNAC	Symantec™ Network Access Control
SOF	Strength Of Function
ST	Security Target
TOE	Target Of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
UID	Unique Identifier

Table 2 – Acronyms Used in Security Target

2 TOE Description

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

2.1 Product Type

The product type of the Target of Evaluation (TOE) described in this Security Target (ST) is a network access control solution running on clients (e.g., desktops and laptops), an Enforcer to grant the endpoint network access, block network access, or remediate non-compliant computers, and a management component running on a central server to control and monitor execution of the network access control client application.

The primary purpose of Symantec Network Access Control is to ensure that the clients that run the software are compliant with an organization's security policies. Security policy compliance is enabled by using the Host Integrity policies created in the Symantec Endpoint Protection Manager component. Together, Host Integrity policies and hardware enforcement keep non-compliant computers off of the network. This software also can direct the clients that are not compliant to remediation servers, where software, patches, and virus updates can be downloaded.

Symantec Network Access Control is a companion product to Symantec Endpoint Protection, with which it shares the same management console. Symantec Endpoint Protection provides Symantec AntiVirus protection with advanced threat protection that protects endpoints (laptops, desktops, and servers) from both known threats and those threats that have not been seen before.

2.2 Functionality Overview

The Symantec Network Access Control client validates and enforces policy compliance for the computers that try to connect to the network. This validation and enforcement process begins before the computer connects to the network and continues throughout the duration of the connection. The Host Integrity Policy is the security policy that serves as the basis for all evaluations and actions.

This network access control process includes the following steps:

- The client continuously evaluates its compliance. When the client computer is powered on, the client runs a Host Integrity check that compares the computer's configuration with the Host Integrity Policy that was downloaded from the management server. The Host Integrity check evaluates your computer for compliance with the Host Integrity Policy for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check how recently its antivirus definitions have been updated, and which were the latest patches applied to the operating system.

- A Symantec Enforcer authenticates the client computer and either grants the computer network access, blocks, or isolates non-compliant computers to a confined area of the network for remediation. If the computer meets all the policy's requirements, the Host Integrity check passes. The Enforcer grants full network access to computers that pass the Host Integrity check. If the computer does not meet the policy's requirements, the Host Integrity check fails. When a Host Integrity check fails, the client or a Symantec Enforcer blocks or isolates the computer until it is remediated. Isolated computers have limited or no access to the network. The administrator may have set up the policy so that

a Host Integrity check passes even if a specific requirement fails. The client may display a notification every time the Host Integrity check passes.

- The client remediates non-compliant computers. If the client finds that a Host Integrity Policy requirement is not met, it installs or requests the user to install the required software. After your computer is remediated, it tries to access the network again. If the computer is fully compliant, the network grants the computer network access.
- The client proactively monitors compliance. The client actively monitors the compliance state for all client computers. If at any time the computer's compliance status changes, so do the network access privileges of the computer

The figure below illustrates the TOE functionality:

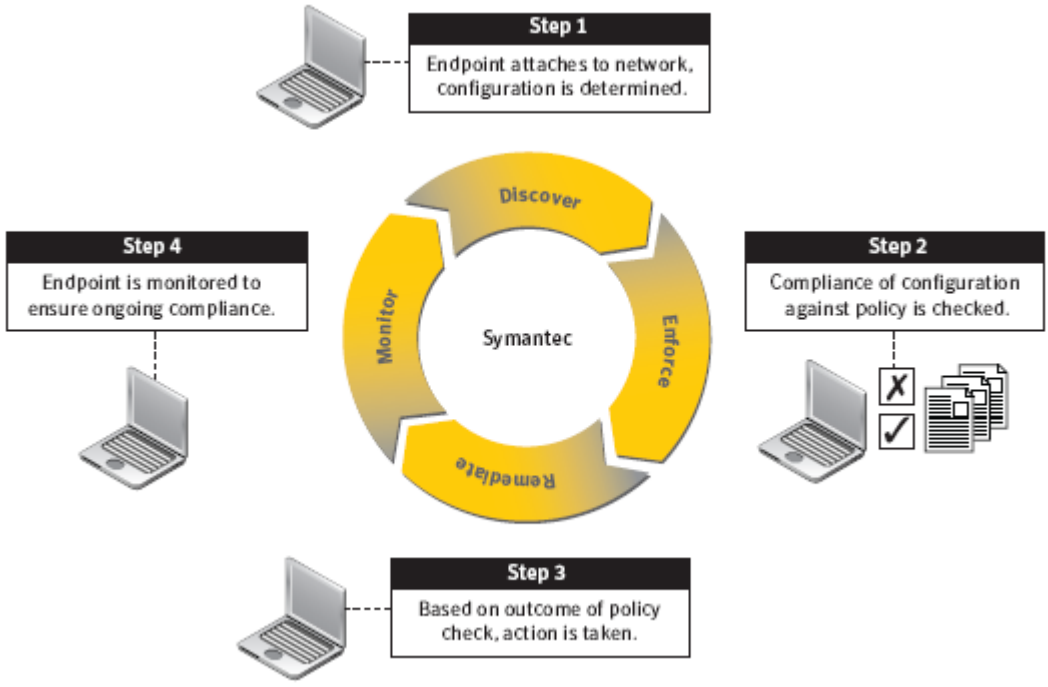


Figure 1 – Symantec Network Access Control Process

The figure below depicts a typical deployment of the TOE:

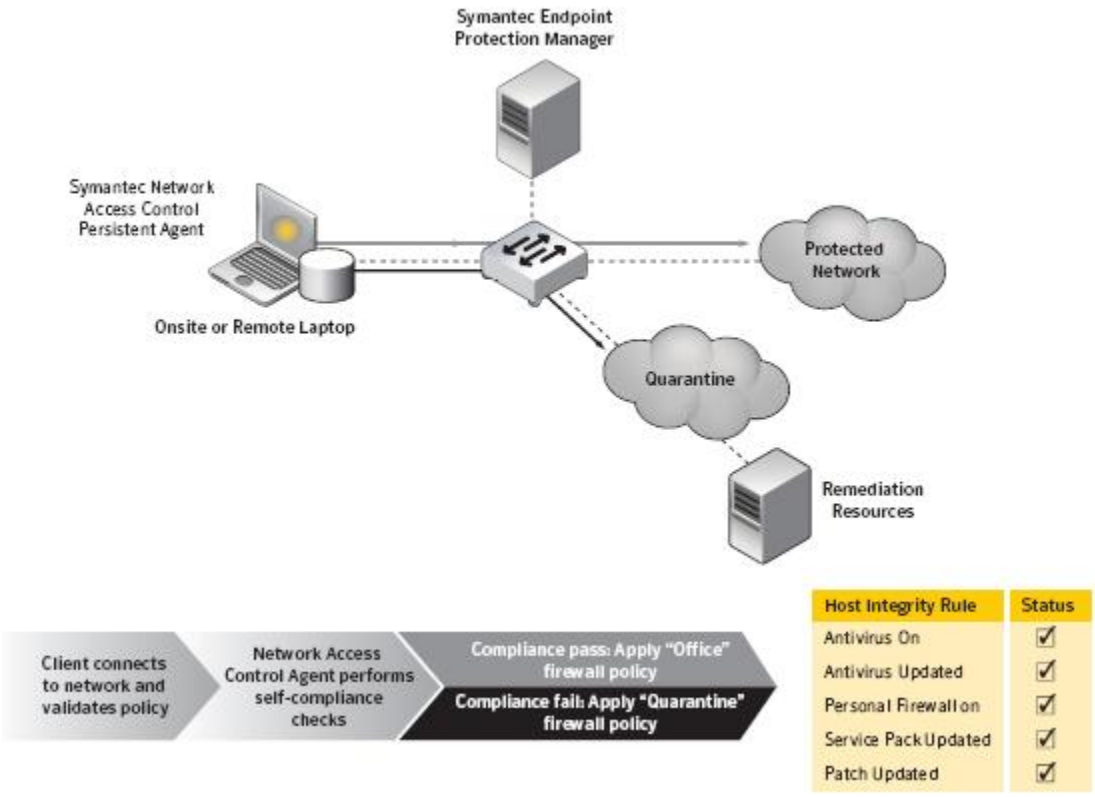


Figure 2 – Architecture Overview

2.3 Product Description

The evaluated features and components of Symantec™ Network Access Control are described in the following sections.

2.3.1 Symantec Network Access Control Client

The Symantec Network Access Control client is installed on the endpoints on which network access policies are to be enforced. The Symantec Network Access Control client includes Host Integrity checking and self-enforcement capabilities. The client is also designed to report its Host Integrity compliance status to a Symantec Enforcer.

The Symantec Network Access Control client evaluates whether a computer is properly protected and compliant before it is allowed to connect to the corporate network.

The client ensures that the computer complies with a security policy configured by the administrator. The security policy checks whether your computer runs the most recent security software, such as antivirus and firewall applications. If the computer does not run the required software, either the user or the client must update the software. If the security software is not up to date, the computer may be blocked from connecting to the network. The client runs periodic checks to verify that the computer continues to comply with the security policy.

The Symantec Network Access Control Client must be installed on an endpoint that meets the following minimum requirements:

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server
- Windows XP Home Edition or Professional
- Windows XP Tablet Edition
- Windows Server 2003 Standard or Enterprise

2.3.2 Symantec Enforcer 6100 Series

The Symantec Enforcer is an appliance that works with Symantec Network Access Control clients to help regulate their access to the network. The Enforcer ensures that all the computers that connect to the network it protects run the client software and have a correct security policy.

An Enforcer must authenticate the user or the client computer before it allows the client computer to access the network. Symantec Network Access Control works with several types of Enforcers to authenticate the client computer. The Symantec Enforcer is the network hardware appliance that verifies Host Integrity results and the client computer's identity before it allows the computer network access.

The Enforcer checks the following information before it allows a client to access the network:

- The Symantec Network Access Control client is running.
- The client has a unique identifier (UID).
- The client been updated with the latest Host Integrity Policy.
- The client computer passed the Host Integrity check.

2.3.3 Symantec Endpoint Protection Manager

Symantec Endpoint Protection Manager is installed on a computer to host the management server software. Symantec Endpoint Protection Manager communicates with the Symantec Network Access Control clients and is configured through the Symantec Endpoint Protection Manager Console.

The management functions of the System Administrator and Administrator may execute on a separate system from the portion of the TOE performing network access control compliance on workstations; this portion of the TOE is called Symantec Endpoint Protection Manager (SEPM). The SEPM communicates with the Enforcers or with individual workstations via an agent over HTTPS that is installed with the Symantec Network Access Control Client software.

The Symantec Endpoint Protection Manager must be installed on a workstation that meets the following minimum requirements:

- Microsoft® Windows® 2003 (32-bit and 64-bit)
- Microsoft Windows XP (32-bit)
- Microsoft Windows 2000—SP3 and later (32-bit)

The Symantec Endpoint Protection Manager Console lets you centrally manage the Symantec Network Access Control clients. The redesigned management console can be used to:

- Install clients
- Manage and deploy the Host Integrity policies that are applied to Symantec Network Access Control clients.
- Manage and deploy enforcement policies to the Enforcers in the network.
- Monitor and report on security threats and system response from a central point.

The console can be run from the computer hosting Symantec Endpoint Protection Manager or remotely through a Web-based interface. In case of the former, the console application to manage the SEPM must run on a workstation that meets the following minimum requirements:

- Microsoft Vista® (32-bit and 64-bit)
- Microsoft Windows 2003 (32-bit and 64-bit)
- Microsoft Windows XP (32-bit and 64-bit)
- Microsoft Windows 2000—SP3 and later (32-bit)

2.4 TOE Boundaries

2.4.1 Physical Boundary Configuration

The TOE is defined as Symantec™ Network Access Control Version 11.0. In order to comply with the evaluated configuration, the following components should be used:

COMPONENT	VERSION NUMBER
SEPM Software	Version 11.0.776.942
Client Software	Version 11.0.780.1109
Operating System for Symantec Network Access Control Client	• Windows 2000 Professional SP4 • Windows 2000 Server SP3 • Windows 2000 Advanced Server SP4

COMPONENT	VERSION NUMBER
	• Windows XP SP2[1] Professional Edition • Windows Server 2003 Standard or Enterprise
Operating System for Symantec Endpoint Protection Manager	• Windows 2003 R2 (32-bit and 64-bit) • Windows XP SP2[2] (32-bit) • Windows 2000 SP3 (32-bit)
Operating System for Symantec Endpoint Protection Manager Console	• Windows Vista® (32-bit and 64-bit) • Windows 2003 R2 (32-bit and 64-bit) • Windows XP SP2[3] (32-bit and 64-bit) • Windows 2000 SP4 (32-bit)
Symantec Enforcer Software	Version 11.0 Build 2038
Symantec Enforcer Hardware	Symantec Network Access Control Enforcer 6100 Series Appliance

Table 3 – Evaluated Configuration for the TOE

Figure 3 – TOE Boundary illustrates the physical scope and the physical boundary of the Symantec Endpoint Protection solution and details the TOE components and the elements of the TOE Environment.

[1] Tested on Service Pack 2 but compatible with previous versions of Windows XP

[2] Tested on Service Pack 2 but compatible with previous versions of Windows XP

[3] Tested on Service Pack 2 but compatible with previous versions of Windows XP

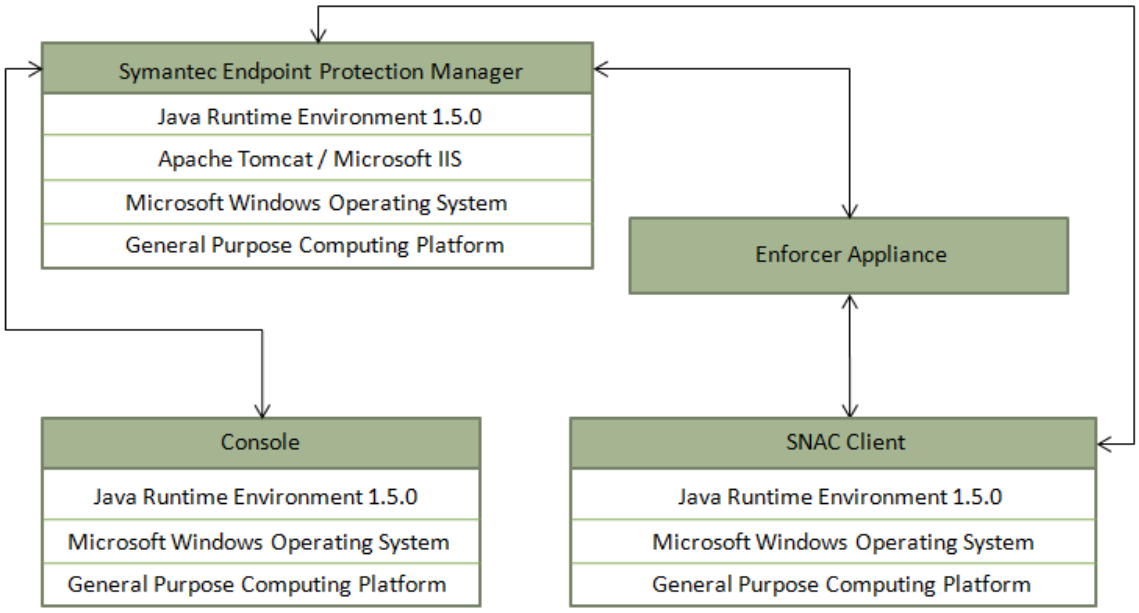


Figure 3 – TOE Boundary

2.4.2 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[4].

2.4.2.1 Audit

The audit services include details on actions taken when a non-compliant endpoint is detected as well as administrative actions performed while accessing the TOE. The TOE generates audits when security-relevant events occur, stores the audit information on the local system, transmits the audit information to a central management system, generates alarms for designated events, and provides a means for audit review.

Protection of audit data in the audit trail involves the TOE and the Operating System (OS). The TOE controls the insertion of audit events into the audit log and the deletion of audit events from the audit log. The OS provides basic file protection services for the audit log.

2.4.2.2 Information Flow Control

The TOE is designed to help prevent unwanted and non-compliant endpoints from gaining access to the local area network. The Client compares endpoint configuration with defined security policies; a non-compliant endpoint is not allowed full access to the network.

[4] Note that the logical boundaries include the core functionality of the TOE as well as supporting features detailed in the AVPP. This was done to perverse consistency between this and the evaluation of Symantec Endpoint Protection, as both are able to run under the same Symantec Endpoint Protection Manager management console.

2.4.2.3 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 Information Flow Control and Audit.

2.4.3 TOE Security Functional Policies

The TOE supports the following Security Functional Policy:

2.4.3.1 NAC Information Flow Control SFP

The TOE implements an information process flow policy named *NAC Information Flow Control SFP*. This SFP determines the procedures utilized to process information entering the TOE and the action taken upon the detection of an endpoint that is not compliant with the TOE's Host Integrity Policies. The actions taken at the occurrence of a violation is configurable by an authorized administrator via the Symantec Endpoint Protection Manager 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 Secure Use Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The secure use assumptions include assumptions for personnel, physical environment, and operational concerns.

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.

A.AUDIT_BACKUP	Administrators will back up the audit files and monitor disk usage to ensure audit information is not lost.
A.NOEVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PHYSICAL	It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
A.SECURE_COMMS	It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.

3.2 Threats to Security

The TOE or IT environment addresses the threats identified in the following sections.

3.2.1 Threats Addressed by the TOE

The TOE addresses the following threats:

T.AUDIT_COMPROMISE A user or process may gain unauthorized access to the audit trail and cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a security relevant event.

T.TSF_COMPROMISE A user or process may cause, through an unsophisticated attack, TSF data or executable code to be inappropriately accessed (viewed, modified, or deleted).

T.UNAUTH_ENDPOINT An unidentified or unsecure endpoint may attempt to access a network, resulting in malicious or unidentified activity on that network.

3.2.2 Threats Addressed by Operating Environment

The TOE Operating Environment addresses the following threats:

TE.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.

TE.RESIDUAL_DATA A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to verify compliance or process administrator requests.

3.3 Organizational Security Policies

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

P.ACCESS_BANNER The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.

P.ROLES The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

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.ADMIN_ROLE The TOE will provide an authorized administrator role to isolate administrative actions.

O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events.

O.AUDIT_PROTECTION The TOE will provide the capability to protect audit information.

O.AUDIT_REVIEW The TOE will provide the capability to selectively view audit information.

O.MANAGE The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE.

O.UNAUTH_ENDPOINT The TOE will detect unauthenticated, unauthorized, or non-compliant endpoints and deny access to the network until the endpoint is authenticated, authorized, and complaint to internal security policies.

4.2 Security Objectives for the IT Environment

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

OE.AUDIT_ALARM The IT Environment will provide the capability to produce an audit alarm before the audit log is full.

OE.AUDIT_BACKUP Audit log files are backed up and can be restored, and audit log files will not run out of disk space.

OE.AUDIT_STORAGE The IT environment will provide a means for secure storage of the TOE audit log files.

OE.DISPLAY_BANNER The IT environment will display an advisory warning regarding use of the system.

OE.DOMAIN_SEPARATION The IT environment will provide an isolated domain for the execution of the TOE.

OE.NO_BYPASS	The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.
OE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.PHYSICAL	Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.
OE.RESIDUAL_INFORMATION	The IT environment will ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated.
OE.SECURE_COMMS	The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.
OE.TIME_STAMPS	The IT environment will provide reliable time stamps.
OE.TOE_ACCESS	The IT Environment will provide mechanisms that control a user's logical access to the TOE.

4.3 Security Objectives for the Non-IT Environment

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

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_GEN.2	User Identity Association
	FAU_SAR.1(1)	Audit Review
	FAU_SAR.1(2)	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_SAR.3	Selectable Audit Review
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.4	Prevention of Audit Loss
Information Flow Control	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Security Management	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1(1)	Management of TSF Data
	FMT_MTD.1(2)	Management of TSF Data
	FMT_MTD.1(3)	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles

Table 4 – TOE Security Functional Requirements

5.1 TOE Security Functional 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 *minimum* level of audit; and

c) [The events identified in Table 5 – FAU_GEN.1 Events.

]

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 (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [the additional information identified in Table 5 – FAU_GEN.1 Events].

SFR	AUDITABLE EVENTS
FAU_GEN.1	None
FAU_GEN.2	None
FAU_SAR.1(1)	None
FAU_SAR.1(2)	None
FAU_SAR.2	None
FAU_SAR.3	None
FAU_STG.1	None
FAU_STG.4	Selection of an action
FDP_IFC.1	Action taken in response to detection of a non-compliant endpoint
FDP_IFF.1	Action taken in response to detection of a non-compliant endpoint

SFR	AUDITABLE EVENTS
FMT_MOF.1	None
FMT_MSA.1	None
FMT_MSA.3	None
FMT_MTD.1	None
FMT_SMF.1	None
FMT_SMR.1	None

Table 5 – FAU_GEN.1 Events

5.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 **For audit events resulting from actions of identified users, t**he TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3 FAU_SAR.1(1) Audit Review

FAU_SAR.1.1(1) The TSF shall provide [the System Administrator] with the capability to read [all audit information] from the audit records **on the central management system**.

FAU_SAR.1.2(1) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.4 FAU_SAR.1(2) Audit Review

FAU_SAR.1.1(2) The TSF shall provide [the System Administrator and Workstation Users] with the capability to read [all audit information] from the audit records **on the workstation being used**.

FAU_SAR.1.2(2) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application Note: The Workstation User is permitted to review all audit records saved on the workstation being used by that user. The System Administrator is permitted to review all logs on a specific workstation (which will only apply to that workstation) or on the central management system (which will apply to all workstations within that domain).

5.1.1.5 FAU_SAR.2 Restricted Audit Review

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

Application Note: This SFR applies to read access to the audit records through the TSFIs. The IT Environment (OS) is responsible for prohibiting read access to the audit file via OS interfaces.

5.1.1.6 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to perform *searches* and *sorting* of audit data based on

a) [Date and time of the event,

b) Type of event, and

c) Subject identity.

]

5.1.1.7 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion **via the TSFI**.

FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail **via the TSFI**.

Application Note: FAU_STG.1 applies to both the central management system and the individual workstations.

Application Note: This instance of FAU_STG.1 applies to protection of the audit records via the TSFI. The IT Environment (OS) is responsible for preventing deletion of the audit file via OS interfaces.

5.1.1.8 FAU_STG.4 Prevention of Audit Loss

FAU_STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [no other actions] if the audit trail is full.

5.1.2 User Data Protection (FDP)

5.1.2.1 FDP_IFC.1 Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [NAC Information Flow Control SFP] on [

Subjects: External IT entities attempting to send traffic through the TOE

Information: Host Integrity Policy

Operations: Block, Remediate, Allow]

5.1.2.2 FDP_IFF.1 Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [NAC Information Flow Control SFP] based on the following types of subject and information security attributes: [

Subject Security Attributes: Symantec Network Access Control client is running, the client has a unique identifier (UID), the client has been updated with the latest Host Integrity Policy, the client computer passed the Host

Integrity check.

Information Security Attributes: Antivirus On; Antivirus Updated; Personal Firewall On; Service Pack Updated; Patch Updated; Custom scripts containing “and/or” logic to allow or deny access based on file, process, or registry parameters]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[Monitoring option is enabled for the service and information structure type and:

1. The endpoint is compliant to the Host Integrity Policy or
2. The endpoint is remediated in an isolated area of the network to attain compliance with the Host Integrity Policy or
3. The endpoint MAC address is contained within an exception list configured in the Enforcer

].

FDP_IFF.1.3 The TSF shall enforce the [no additional NAC Information Flow Control SFP rules].

FDP_IFF.1.4 The TSF shall provide the following [no additional SFP capabilities].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [no explicit authorization rules].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [no explicit denial rules].

5.1.3 Security Management (FMT)

5.1.3.1 FMT_MOF.1 Management of Security Functions Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behavior of, disable, enable* the functions [

a) Auditing,

b) Configuring Host Integrity Policies

]

to [the System Administrator].

5.1.3.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [NAC Information Flow Control SFP] to restrict the ability to *query, modify, delete* the security attributes [TSF data] to [System Administrator].

5.1.3.3 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [NAC Information Flow 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 [System Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.1.3.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1(1) The TSF shall restrict the ability to *query, modify, delete* the [

a) Actions to be taken on workstations when a non-compliant endpoint is detected,

b) Information security attributes to be scanned automatically on workstations,

c) Processes authorized to transmit data over an internal network,

d) Audit logs on the central management system]

to [the System Administrator].

FMT_MTD.1.1(2) The TSF shall restrict the ability to *modify* the [

a) Host Integrity Policies

]

to [the System Administrator].

FMT_MTD.1.1(3) The TSF shall restrict the ability to *query* the [audit logs on the workstation being used] to [the System Administrator and Workstation Users].

5.1.3.5 FMT_SMF.1 Specification of Management Functions

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

a) Configure operation of the TOE on workstations,

b) Update Host Integrity Policies,

c) Acknowledge alert notifications from the central management system,

d) Review audit logs on the central management system,

e) Acknowledge alert notifications on the workstation being used, and

f) Review audit logs on the workstation being used

].

5.1.3.6 FMT_SMR.1 Security Roles

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

5.2 Security Functional Requirements for the IT Environment

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The **IT Environment** shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The **IT Environment** shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

Application Note: This instance of FAU_STG.1 applies to the audit trail file(s) as a whole, while the instance levied against the TOE applies to individual records within the files.

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1 The **IT Environment** shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from* the following objects: [all objects used by the TOE].

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The **IT Environment** shall detect when *[3]* unsuccessful authentication attempts occur related to [the unsuccessful authentication attempts since the last successful authentication for the System Administrator or Workstation User].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the **IT Environment** shall [lock the respective account and prevent future authentication attempts until reset by an administrator].

5.2.3.2 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The **IT Environment** shall provide a mechanism to verify that secrets meet [strong passwords **sufficient to satisfy SOF-basic requirements**].

5.2.3.3 FIA_UAU.2 User Authentication Before any Action

FIA_UAU.2.1 The **IT Environment** shall require each **System Administrator or Workstation User** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.3.4 FIA_UAU.6 Re-Authenticating

FIA_UAU.6.1 The **IT Environment** shall re-authenticate the **System Administrator or Workstation User** under the conditions [the session is locked due to inactivity].

5.2.3.5 FIA_UID.2 User Identification Before any Action

FIA_UID.2.1 The **IT Environment** shall require each **System Administrator or Workstation User** to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.3.6 FIA_PLA_EXP.1 Performance and Log Alerts (EXP)

FIA_PLA_EXP.1.1 The IT environment shall alert the administrator before audit storage reaches capacity.

5.2.4 Protection of the TSF (FPT)

5.2.4.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

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

5.2.4.2 FPT_RVM.1 Non-Bypassability of the TSP

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

5.2.4.3 FPT_SEP.1 TSF Domain Separation

FPT_SEP.1.1 The **IT Environment** shall maintain a security domain for **the TOE's** own execution that protects **the TOE** from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The **IT Environment** shall enforce separation between the security domains of subjects in the TSC.

5.2.4.4 FPT_STM.1 Reliable Time Stamps

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

5.2.5 TOE Access (FTA)

5.2.5.1 FTA_SSL.1 TSF-Initiated Session Locking

FTA_SSL.1.1 The **IT Environment** shall lock an interactive session **of the System Administrator or Workstation User** after [30 minutes] by:

a) Clearing or overwriting display devices, making the current contents unreadable;

b) Disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The **IT Environment** shall require the following events to occur prior to unlocking the **System Administrator or Workstation User** session: [re-authentication].

5.2.5.2 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Before establishing a user session, the **IT Environment** shall display an advisory warning message regarding unauthorized use of the **system**.

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 taken from Part 3 of the CC. The TOE assurance requirements are the Basic Robustness Assurance Package and are equivalent to EAL2 augmented by ALC_FLR.2 and AVA_MSU.1. 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

ASSURANCE CLASS	ASSURANCE COMPONENTS	
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Lifecycle Support	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 6 – Security Assurance Requirements

5.5 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:

- Identification and Authentication
    - FIA_SOS.1 – Verification of Secrets
    - FIA_UAU.2 – Authentication of administrators
    - FIA_UID.2 – Identification of administrators

The SOF for these mechanisms is SOF-Basic.

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:

- Audit
- Information Flow Control
- Management

6.1.1 Audit

The TOE provides robust reporting capabilities to provide the System Administrator with insight on the Server and Workstation Host Integrity Policy compliance activities. Additionally, the TOE supports the provision of log data from each system component.

The reporting functions give the up-to-date information to monitor and make informed decisions about the security of the network. The management console Home page displays the automatically generated charts that contain information about the important events that have happened recently in your network. You can use the filters on the Reports page to generate predefined or custom reports. You can use the Reports page to view graphical representations and statistics about the events that happen in your network. You can use the filters on the Monitors page to view more detailed, real-time information about your network from the logs.

Reporting runs as a Web application within the management console, and TOE reporting features include the following:

- Customizable Home page with your most important reports, overall security status, and links to Symantec Security Response
- Summary views of reports on compliance status and site status
- Predefined quick reports and customizable graphical reports with multiple filter options that you can configure
- The ability to schedule reports to be emailed to recipients at regular intervals
- Support for Microsoft SQL or an embedded database for storing event logs
- Configurable notifications that are based on security or compliance events

The TOE generates audit data for various events, and this audit data is aggregated into a series of pre-defined reports. An authorized administrator can view and filter the following reports:

REPORT TYPE	DESCRIPTION
Audit	Displays information about the policies that clients and locations use currently.
Compliance	Displays information about the compliance status of your network. These reports include information about Enforcer servers, Enforcer clients, Enforcer traffic, and host compliance.
Computer Status	Displays information about the operational status of the computers in your network, such as which computers are infected. These reports include information about versions, clients that have not checked in to the server, client inventory, and online status.
System	Displays information about event times, event types, sites, domains, servers, and severity levels.

Table 7 – Available Reports

Reports are available only to operators that have explicit access to reports, and this privilege is defined by the system administrator (i.e., System Administrator role). Only System Administrators can review reports on the SEPM, while System Administrators and Workstations users can review reports on the workstation. Operators with access to reports can search audit records and can sort records by date/time of event, the type of event recorded, and the affected host identity.

All system reports and audit logs are stored in an embedded Sybase database on the SEPM. If the database reaches storage capacity, the TOE will overwrite the oldest records.

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

- FAU_GEN.1
- FAU_GEN.2
- FAU_SAR.1(1)
- FAU_SAR.1(2)
- FAU_SAR.2
- FAU_SAR.3
- FAU_STG.1
- FAU_STG.4

6.1.2 Information Flow Control

Host Integrity Policies are configured to ensure that the client computers that connect to an enterprise network run the required applications and data files. The client that runs a Host Integrity check implements the Host Integrity Policy settings defined by the administrator.

During the Host Integrity check, the client follows the requirements that are set in the Host Integrity Policy. It examines the registry keys, active applications, date and size of a file, and

other possible parameters to determine the existence of the required software.

The client automatically generates an entry in the Security log whenever it finds that the required software is not installed on the computer. If user notification is enabled on the client, a message appears on the user's computer.

If the required software is not installed on the computer, the client can be set to silently connect to a remediation server. From there it can download and install the required software. The software can include a software patch, a hotfix, an update to virus definitions, and so on. The client can give the user a choice to download immediately or postpone a download. The computer cannot connect to the enterprise network until the software is installed.

The client can also detect whether or not an antivirus application is out of date. If an antivirus application is older than what a system administrator has specified, the client can be prevented from connecting to the enterprise network. Before it can connect, the client needs an up-to-date version of the antivirus application.

The Host Integrity Policy includes the settings that determine how often the client runs a Host Integrity check on the client computer. The client computer can connect to the network through a Symantec Enforcer. In this scenario, you can set up the Host Integrity Policy such that the client runs the Host Integrity check only when prompted by the Enforcer. The Enforcer can verify the following: the client is running, the client's policy is up to date, and the Host Integrity check is passed before it allows access to the network.

Every time a client receives a new security policy, it immediately runs a Host Integrity check. The client can be set up to automatically download and install the latest security policy. A security log entry is generated if the policy update fails. If user notification is enabled on the client, a message appears on the user's computer.

The following is an example of the kinds of requirements you need to consider when you set up Host Integrity enforcement. In this example, the Host Integrity Policy has been set up to require the following:

- The client runs up-to-date antivirus software
- The Host Integrity check is done only when the client tries to connect to the network through an Enforcer
- The check triggers the actions that takes place silently on the client

The Enforcer automatically does the following:

- Verifies that a client has been installed on a user's computer
- Prompts a client to retrieve updated security policies, if available

The Enforcer then prompts the client to run the Host Integrity check. The client first verifies that the latest antivirus software is installed and runs. If it has been installed but is not running, the client silently starts the antivirus application. If it is not installed, the client downloads the software from a URL that is specified in the Host Integrity requirement. Then the client installs and starts the software.

Next, the client verifies that the antivirus signature files are current. If the antivirus files are not current, the client silently retrieves and installs the updated antivirus files.

The client runs the Host Integrity check again and passes. The Enforcer receives the results and grants the client access to the enterprise network. In this example, the following requirements must be met:

- The file server that is used for Host Integrity updates has the latest files installed. The client obtains updated applications from the file server. You can set up one or more remediation servers that are connected to the enterprise network. From the remediation servers, users can copy or automatically download the required patches and hotfixes for any required application. If a remediation server fails, then Host Integrity remediation also fails. If the client tries to connect through an Enforcer, the Enforcer blocks the client if Host Integrity fails. You have the option to set up the Host Integrity Policy so that the client notifies the Enforcer that the Host Integrity check passed even though it failed. In this case, the Enforcer does not block the client. Information about the failed Host Integrity check is recorded in the client's Security log.
- The management server must be configured so that updates of the security policy are automatically sent to any computer that runs the client.

If the parameters that are defined for the Host Integrity Policies are not successful, then the Enforcer does not allow the client to connect to the enterprise network.

The following message appears on the client:

```
Symantec Enforcer has blocked all traffic from the client. rule: {name
of requirement} failed.
```

The client tries to recover. If the client's Host Integrity Policy is set up to update files before it allows the client to connect to the enterprise network, then the user is notified that an update needs to be provided. A progress indicator for the update follows the update. If the user disconnects from the enterprise network, the process starts again.

The Information Flow Control function is designed to satisfy the following security functional requirements:

- FDP_IFC.1
- FDP_IFF.1
- FMT_MSA.1
- FMT_MSA.3

6.1.3 Management

The functionality in the TOE requires management to ensure proper configuration control. These pieces of Management functionality are described in the following subsections:

6.1.3.1 Security Roles

The TOE maintains four roles: system administrator, administrator, limited administrator, and workstation user. The table below provides a brief description of each:

SNAC ROLE	DESCRIPTION
System Administrator	Domain management Administrator management

SNAC ROLE	DESCRIPTION
	Server management
Administrator	Create administrators in their domain Delete and modify the administrators that were created in their domain Change attributes for the administrators that are created in their domain. These attributes include notification, security, and permission settings.
Limited Administrator	Perform the work that is assigned to them by the system administrator or administrator Configure their own attributes including security settings and notification settings
Workstation User	Install patches and other software updates to bring the endpoint to compliance with policies Receive alert notifications for events on the workstation being used Acknowledge alert notifications for events on the workstation being used Review the TOE audit information on the workstation being used

Table 8 – Description of Roles Supported in the TOE

The System Administrator role in the TOE is responsible for all management functions of the TOE, including management of TOE security functions and review of TOE audit data.

6.1.3.2 Security Audit

A TOE Administrator can view system reports and specific component logs. The Administrator can further define lifespans for the storage of reports/logs and can view, print, save, schedule, and delete them as part of the Security Audit capabilities.

6.1.3.3 Access Control

The Administrator manages the creation and enforcement of different levels of access within the TOE, and each level of access has set of services available (as defined in Table 8 – Description of Roles Supported in the TOE). The Administrator can define services available to various privilege levels/roles without granting full System Administrator privileges.

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

- FMT_MSA.1
- FMT_MSA.3
- FMT_MOF.1
- FMT_MTD.1

- FMT_SMF.1
- FMT_SMR.1

6.2 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™ Endpoint Protection Version 11.0 and Symantec™ Network Access Control Version 11.0*
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™ Endpoint Protection Version 11.0 and Symantec™ Network Access Control Version 11.0*
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: *Installation Guide for Symantec Endpoint Protection and Symantec Network Access Control* *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Network Access Control Version 11.0*
ALC_FLR.2	ALC_DOC	Flaw reporting procedures: Describes how security flaws are tracked and reported.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES	DESCRIPTION
		Evidence Title: *Flaw Reporting Procedures: Symantec™ Endpoint Protection Version 11.0 and Symantec™ Network Access Control Version 11.0*
ADV_FSP.1	FUN_SPEC	Informal functional specification: Functional Specification for the TOE describing the TSF and the TOE's external interfaces. Evidence Title: *Functional Specification: Symantec™ Network Access Control Version 11.0*
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™ Network Access Control Version 11.0*
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™ Network Access Control Version 11.0*
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: *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control* *Client Guide for Symantec™ Endpoint Protection and Symantec Network Access Control* *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Network Access Control Version 11.0*

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES	DESCRIPTION
AGD_USR.1	USER_GUIDE	User guidance: Documentation provided to the customers instructing the users how to use the TOE. Evidence Titles: *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control* *Client Guide for Symantec™ Endpoint Protection and Symantec Network Access Control* *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Network Access Control Version 11.0*
ATE_COV.1	TEST_COV	Evidence of coverage: Documented correspondence between the security functions and tests. Evidence Title: *Test Plan and Coverage Analysis: Symantec™ Network Access Control Version 11.0*
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™ Network Access Control Version 11.0*
AVA_MSU.1	ADMIN_GUIDE USER_GUIDE	Examination of guidance: Misleading, unreasonable and conflicting guidance should be absent from the guidance documentation. Evidence Titles: *Administration Guide for Symantec Endpoint Protection and Symantec Network Access Control* *Client Guide for Symantec™ Endpoint Protection and Symantec Network Access Control* *Administrative Guidance and Installation, Generation, and Startup Procedures: Symantec™ Network Access Control Version 11.0*
AVA_SOF.1	SOF_DOC	Strength of TOE security function evaluation: The documentation for the Strength of Function Assessment.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES	DESCRIPTION
		Evidence Title: *Strength of Functional Analysis and Vulnerability Assessment: Symantec™ Network Access Control Version 11.0*
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: *Strength of Functional Analysis and Vulnerability Assessment: Symantec™ Network Access Control Version 11.0*

Table 9 – Assurance Measures

7 Protection Profile Claims

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

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.

THREATS/ ASSUMPTIONS / OBJECTIVES	A. AUDIT_BACKUP	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	T. AUDIT_COMPROMISE	TE.MASQUERADE	TE.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNAUTH_ENDPOINT	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.ROLES
O.ADMIN_ROLE												✓
O.AUDIT_ GENERATION											✓	
O.AUDIT_PROTECTION					✓							
O.AUDIT_REVIEW								✓				
O.MANAGE								✓				
O.UNAUTH_ENDPOINT									✓			
OE.AUDIT_ALARM					✓							
OE.AUDIT_BACKUP	✓											
OE.AUDIT_STORAGE					✓							
OE.DISPLAY_BANNER										✓		
OE.DOMAIN_ SEPARATION					✓			✓				
OE.NO_BYPASS					✓			✓				
OE.NO_EVIL		✓										
OE.PHYSICAL			✓									

THREATS/ ASSUMPTIONS / OBJECTIVES	A. AUDIT_BACKUP	A.NO_EVIL	A.PHYSICAL	A.SECURE_COMMS	T. AUDIT_COMPROMISE	TE.MASQUERADE	TE.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNAUTH_ENDPOINT	P.ACCESS_BANNER	P.ACCOUNTABILITY	P.ROLES
OE.RESIDUAL_ INFORMATION					✓		✓	✓				
OE.SECURE_COMMS				✓								
OE.TIME_STAMPS											✓	
OE.TOE_ACCESS						✓					✓	

Table 10 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

8.1.2 Rationale for Security Objectives of the TOE

.

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
T.AUDIT_ COMPROMISE: A user or process may cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.	**O.AUDIT_PROTECTION:** The TOE will provide the capability to protect audit information. **OE.AUDIT_ALARM:** The IT Environment will provide the capability to produce an audit alarm before the audit log is full. **OE.AUDIT_STORAGE:** The IT Environment will contain mechanisms to provide secure storage and management of the audit log. **OE.RESIDUAL_ INFORMATION:** The IT Environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.	**O.AUDIT_PROTECTION** contributes to mitigating this threat by controlling access to the individual audit log records. No one is allowed to modify audit records, the System Administrator is the only one allowed to delete audit records, and the TOE has the capability to overwrite the oldest stored audit records if the audit trail is full. **OE.AUDIT_ALARM** helps prevent the loss of audit records by sending an alarm if the available storage space for the audit log meets a certain threshold. **OE.AUDIT_STORAGE** contributes to mitigating this threat by restricting the ability of users in the IT Environment to access the audit log file.

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
	OE.DOMAIN_SEPARATION: The IT Environment will provide an isolated domain for the execution of the TOE. **OE.NO_BYPASS:** The IT Environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	**OE.RESIDUAL_INFORMATION** prevents a user not authorized to read the audit trail from access to audit information that might otherwise be persistent in a resource used by the TOE (e.g., memory). By preventing residual information in a resource, audit information will not become available to any user or process except those explicitly authorized for that data. **OE.DOMAIN_SEPARATION** contributes to countering this threat by ensuring that the TSF is protected from users through mechanisms other than its own interfaces. If the OS could not maintain and control a domain of execution for the TSF separate from other processes, the TSF could not be trusted to control access to the resources under its control, which includes the audit trail which are always invoked is also critical to the migration of this threat. **OE.NO_BYPASS** ensures audit compromise can not occur simply by bypassing the TSF.
TE.MASQUERADE: A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	**OE.TOE_ACCESS:** The IT Environment will provide mechanisms that control a user's logical access to the TOE.	**OE.TOE_ACCESS** mitigates this threat by requiring authorized administrators and workstation users to be identified and authenticated, a necessary step in controlling the logical access to the TOE and its resources by constraining how and when users can access the TOE. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
TE.RESIDUAL_DATA: A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to scan files or process administrator requests.	**OE.RESIDUAL_INFORMATION:** The IT Environment will ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated.	**OE.RESIDUAL_INFORMATION** counters this threat by ensuring that memory contents are not persistent when resources are released by the TOE and allocated to another user/process.
T.TSF_COMPROMISE: A user or process may gain unauthorized access to data through reallocation of memory used by the TOE to verify compliance or process administrator requests.	**OE.RESIDUAL_INFORMATION:** The IT Environment will ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated. **OE.DOMAIN_SEPARATION:** The IT environment will provide an isolated domain for the execution of the TOE. **O.AUDIT_REVIEW:** The TOE will provide the capability to selectively view audit information. **O.MANAGE:** The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE. **OE.NO_BYPASS:** The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	**OE.RESIDUAL_INFORMATION** is necessary to mitigate this threat, because even if the security mechanisms do not allow a user to explicitly view TSF data, if TSF data were to inappropriately reside in a resource that was made available to a user, that user would be able to inappropriately view the TSF data. **OE.DOMAIN_SEPARATION** is necessary so that the TSF is protected from other processes executing on the workstation. **O.MANAGE** is necessary because an access control policy is not specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions. **O.AUDIT_REVIEW** helps to mitigate this threat by providing the Security Administrator with a required minimum set of configurable audit events that could indicate a potential security violation. By configuring these auditable events, the TOE monitors the occurrences of these events (e.g. set number of authentication failures, set number of information policy flow failures, etc.).

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
		O.CORRECT_TSF_OPERATION provides assurance that the TSF continues to operate as expected in the field. **OE.NO_BYPASS** ensures TSF compromise cannot occur simply by bypassing the TSF.
T.UNAUTH_ENDPOINT: An unidentified or unsecure endpoint may attempt access a network, resulting in malicious or identified activity on that network.	**O. UNAUTH_ENDPOINT:** The TOE will detect unauthenticated, unauthorized, or non-compliant endpoints and deny access to the network until the endpoint is authenticated, authorized, and complaint to internal security policies.	**O. UNAUTH_ENDPOINT** mitigates this threat by providing mechanisms to prevent a non-compliant endpoint introduced onto a network.
P.ACCESS_BANNER: The system shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	**OE.DISPLAY_BANNER:** The IT Environment will display an advisory warning regarding use of the system.	**OE.DISPLAY_BANNER** satisfies this policy by ensuring that the system displays a banner that provides all authorized users with a warning about the unauthorized use of the system.
P.ACCOUNTABILITY: The authorized users of the TOE shall be held accountable for their actions within the TOE.	**O.AUDIT_GENERATION:** The TOE will provide the capability to detect and create records of security-relevant events associated with users. **OE.TIME_STAMPS:** The IT environment shall provide reliable time stamps and the capability for the administrator to set the time used for these time stamps. **OE.TOE_ACCESS:** The TOE will provide mechanisms that control a user's logical access to the TOE.	**O.AUDIT_GENERATION** addresses this policy by recording security-relevant events. The administrator's ID is recorded when any security relevant change is made to the TOE. **OE.TIME_STAMPS** plays a role in supporting this policy by requiring the IT environment to provide a reliable time stamp. The audit mechanism is required to include the current date and time in each audit record. **OE. TOE_ACCESS** supports this policy by requiring the IT environment to identify and

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
		authenticate all authorized administrators and workstation users prior to allowing any TOE access.
P.ROLES: The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.	**O.ADMIN_ROLE:** The TOE will provide an authorized administrator role to isolate administrative actions.	**O.ADMIN_ROLE** addresses this policy by requiring the TOE to support an administrator role, and restrict specific actions to that role.
A.AUDIT_BACKUP: Administrators will back up the audit files and monitor disk usage to ensure audit information is not lost.	**OE.AUDIT_BACKUP:** Audit log files are backed up and can be restored, and audit log files will not run out of disk space.	**OE.AUDIT_BACKUP** addresses the assumption by requiring the audit log files to be backed up, and by requiring monitoring of disk space usage to ensure space is available.
A.NO_EVIL: Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	**OE.NO_EVIL:** Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.	**OE.NO_EVIL** restates the assumption.
A.PHYSICAL: It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.	**OE.PHYSICAL:** Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information.	**OE.PHYSICAL** restates the assumption.

THREAT/POLICY/ ASSUMPTION	ADDRESSED BY	RATIONALE
A.SECURE_COMMS: It is assumed that the IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.	**OE.SECURE_COMMS:** The IT environment will provide a secure line of communications between distributed portions of the TOE and between the TOE and remote administrators.	**OE.SECURE_COMMS** restates the assumption. The workstation OS will provide a secure line of communication for the TOE.

Table 11 – Mapping of Threats, Policies, and Assumptions to Objective

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.

SFR \ OBJECTIVE	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.MANAGE	O.UNAUTH_ENDPOINT
FAU_GEN.1		✓				
FAU_GEN.2		✓				
FAU_SAR.1(1)				✓	✓	
FAU_SAR.1(2)				✓	✓	
FAU_SAR.2			✓			
FAU_SAR.3				✓	✓	

SFR \ OBJECTIVE	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AUDIT_REVIEW	O.MANAGE	O.UNAUTH_ENDPOINT
FAU_STG.1			✓			
FAU_STG.4			✓			
FDP_IFC.1						✓
FDP_IFF.1						✓
FMT_MOF.1	✓				✓	
FMT_MSA.1						✓
FMT_MSA.3						✓
FMT_MTD.1(1)	✓				✓	
FMT_MTD.1(2)	✓				✓	
FMT_MTD.1(3)	✓				✓	
FMT_SMF.1	✓				✓	
FMT_SMR.1	✓				✓	

Table 12 – Mapping of TOE Security Functional Requirements and Objectives

8.2.2 Sufficiency of Security Requirements

The following table presents a mapping of the TOE Objectives to TOE Security Requirements.

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
O.ADMIN_ROLE: The TOE will provide an authorized administrator role to isolate administrative actions.	FMT_MOF.1 FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3)	**FMT_SMR.1** requires that the TOE establish a System Administrator role and **FMT_SMF.1** provides the administrative actions available in the TOE. **FMT_MOF.1, FMT_MTD.1(1)** and

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
	FMT_SMF.1 FMT_SMR.1	**FMT_MTD.1(2)** specify the privileges that only the System Administrator may perform. **FMT_MTD.1(3)** specifies privileges for the System Administrator and Workstation Users.
O.AUDIT_GENERATION: The TOE will provide the capability to detect and create records of security relevant events.	FAU_GEN.1 FAU_GEN.2	**FAU_GEN.1** defines the set of events that the TOE must be capable of recording. This requirement ensures that the Administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. **FAU_GEN.2** ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the userid. In all other cases, the association is based on the source network identifier, which is presumed to be the correct identity, but cannot be confirmed since these subjects are not authenticated.
O.AUDIT_PROTECTION: The TOE will provide the capability to protect audit information.	FAU_SAR.2 FAU_STG.1 FAU_STG.4	**FAU_SAR.2** restricts the ability to read the audit trail to the System Administrator, thus preventing the disclosure of the audit data to any other user. However, the TOE is not expected to prevent the disclosure of audit data if it has been archived or saved in another form (e.g., moved or copied to an ordinary file). The FAU_STG family dictates how the audit trail is protected. **FAU_STG.1** restricts the ability to delete audit records to the System Administrator. **FAU_STG.4** defines the actions that must be available to the administrator, as well as the action to be taken if there is no response. This helps to ensure that audit records are kept until the System Administrator deems they

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
		are no longer necessary. This requirement also ensures that no one has the ability to modify audit records (e.g., edit any of the information contained in an audit record). This ensures the integrity of the audit trail is maintained.
O.AUDIT_REVIEW: The TOE will provide the capability to selectively view audit information.	FAU_SAR.1(1) FAU_SAR.1(2) FAU_SAR.3	**FAU_SAR.1(1)** and **FAUSAR.1(2)** and **FAU_SAR.3** provide the ability to review the audits in a user-friendly manner and the provide the ability to perform searches and sorting of audit data.
O.MANAGE: The TOE will provide all the functions and facilities necessary to support the authorized users in their management of the TOE.	FMT_MOF.1 FMT_MTD.1(1) FMT_MTD.1(2) FMT_MTD.1(3) FMT_SMF.1 FMT_SMR.1	Restricted privileges are defined for the System Administrator and Workstation Users. **FMT_MOF.1** defines particular TOE capabilities that may only be used by the System Administrator. **FMT_MTD.1(1)**, **FMT_MTD.1(2)**, and **FMT_MTD.1(3)** defines particular TOE data that may only be altered by users of the TOE. **FMT_SMF.1** and **FMT_SMR.1** define the administrative functions and roles provided by the TOE. **FAU_SAR.1** and **FAU_SAR.3** provide the ability to review the audits in a user-friendly manner.
O.UNAUTH_ENDPOINT: The TOE will detect unauthenticated, unauthorized, or non-compliant endpoints and deny access to the network until the endpoint is authenticated, authorized, and complaint to internal security policies	FDP_IFC.1 FDP_IFF.1 FMT_MSA.1 FMT_MSA.3	**FDP_IFC.1** defines the information flow control security function policy. **FDP_IFF.1** defines the parameters by which an endpoint can be allowed access to the network. **FMT_MSA.1** restricts the ability to filter traffic to an authorized administrator. **FMT_MSA.3** ensures that the default values of security attributes are restrictive in nature and enforce specification of initial configuration parameters to the Administrator

Table 13 – Rationale for TOE Objectives

8.2.3 Summary of IT Environment Security Requirements

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

IT ENVIRONMENT OBJECTIVE / SFR	OE_AUDIT_ALARM	OE.AUDIT_STORAGE	OE.DISPLAY_BANNER	OE.DOMAIN_SEPARATION	OE.NO_BYPASS	OE.RESIDUAL_INFORMATION	OE.SECURE_COMMS	OE.TIME_STAMPS	OE.TOE_ACCESS
FAU_STG.1		✓							
FDP_RIP.1						✓			
FIA_AFL.1									✓
FIA_SOS.1									✓
FIA_UAU.2									✓
FIA_UAU.6									✓
FIA_UID.2									✓
FIA_PLA_EXP.1	✓								
FPT_ITT.1							✓		
FPT_RVM.1					✓				
FPT_SEP.1				✓					
FPT_STM.1								✓	
FTA_SSL.1									✓
FTA_TAB.1			✓						

Table 14 – Mapping of IT Environment Security Functional Requirements and Objectives

8.2.4 Sufficiency of Security Requirements for the IT Environment

The following table presents a mapping of the IT Environment Objectives to IT Environment Security Functional Requirements.

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
OE.AUDIT_ALARM The IT Environment will provide the capability to produce an audit alarm before the audit log is full.	FIA_PLA_EXP.1	**FIA_PLA_EXP.1** requires the OS to send an alarm if the available storage space for the audit log meets a certain threshold.
OE.AUDIT_STORAGE: The IT environment will provide a means for secure storage of the TOE audit log files.	FAU_STG.1	**FAU_STG.1** requires the OS to protect the audit log file from unauthorized deletion.
OE.DISPLAY_BANNER: The system will display an advisory warning regarding use of the system.	FTA_TAB.1	**FTA_TAB.1** meets this objective by requiring the system to display a banner before a user can establish an authenticated session.
OE.DOMAIN_SEPARATION: The IT environment will provide an isolated domain for the execution of the TOE.	FPT_SEP.1	**FTP_SEP.1** requires the OS to provide an isolated domain for the TOE.
OE.NO_BYPASS: The IT environment shall ensure the TOE security mechanisms cannot be bypassed in order to gain access to the TOE resources.	FPT_RVM.1	**FPT_RVM.1** requires the OS to ensure that the TOE will not be bypassed.
OE.RESIDUAL_INFORMATION: The IT environment will ensure that any information contained in a protected resource within the TOE Scope of Control is not released when the resource is reallocated.	FPT_RIP.1	**FDP_RIP.1** is used to ensure the contents of resources are not available to subjects other than those explicitly granted access to the data.
OE.SECURE_COMMS: The IT environment will provide a secure line of communications between distributed portions of the TOE.	FPT_ITT.1	**FPT_ITT.1** ensures that secure communication between the central management system and the workstations will be available to the TOE.
OE.TIME_STAMPS: The IT environment will provide reliable time stamps.	FPT_STM.1	**FPT_STM.1** requires that the IT Environment provide time stamps for the TOE's use.

OBJECTIVE	REQUIREMENTS ADDRESSING THE OBJECTIVES	RATIONALES
OE.TOE_ACCESS: The IT Environment will provide mechanisms that control a user's logical access to the TOE.	FIA_AFL.1 FIA_SOS.1 FIA_UID.2 FIA_UAU.2 FIA_UAU.6 FTA_SSL.1	**FIA_AFL.1** provides a detection mechanism for unsuccessful authentication attempts by remote administrators, authenticated proxy users and authorized IT entities. The requirement enables a Security Administrator settable threshold that prevents unauthorized users from gaining access to authorized user's account by guessing authentication data by locking the targeted account. Thus, limiting an unauthorized user's ability to gain unauthorized access to the TOE. **FIA_SOS.1** ensures that the strength of the I&A mechanism will be adequate. **FIA_UID.2** requires that a user be identified to the TOE in order to access to the TOE. **FIA_UAU.2** requires that a user be authenticated by the TOE before accessing the TOE. **FIA_UAU.6** requires that a user be re-authenticated after a session is locked. **FTA_SSL.1** requires that sessions be locked after a period of inactivity. The combination of these SFRs ensures that users will successfully complete an I&A process of sufficient strength before they can gain access to the TOE.

Table 15 – Rationale for IT Environment Objectives

8.3 TOE Summary Specification Rationale

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

IT SECURITY FUNCTION / SFR	AUDIT	INFORMATION FLOW CONTROL	MANAGEMENT
FAU_GEN.1	✓		
FAU_GEN.2	✓		
FAU_SAR.1(1)	✓		
FAU_SAR.1(2)	✓		
FAU_SAR.2	✓		
FAU_SAR.3	✓		
FAU_STG.1	✓		
FAU_STG.4	✓		
FDP_IFC.1		✓	
FDP_IFF.1		✓	
FMT_MOF.1			✓
FMT_MSA.1		✓	✓
FMT_MSA.3		✓	✓
FMT_MTD.1(1)			✓
FMT_MTD.1(2)			✓
FMT_MTD.1(3)			✓
FMT_SMF.1			✓
FMT_SMR.1			✓

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

SFR	RATIONALE TO SUPPORT SUFFICIENCY OF SECURITY FUNCTION
FAU_GEN.1	This TOE SFR is satisfied by the Audit which generates audit logs from the audit of a variety of security events.
FAU_GEN.2	This TOE SFR is satisfied by the Audit function, which generates audit logs with details on the actions of identified users.
FAU_SAR.1(1)	This TOE SFR is satisfied by the Audit function, which provides the System Administrator with the capability to review all TOE audit records.
FAU_SAR.1(2)	This TOE SFR is satisfied by the Audit function, which provides the System Administrator and Workstation User with the capability to review all TOE audit records on the workstation.
FAU_SAR.2	This TOE SFR is satisfied by the Audit function by enabling only authorized users to review and query the audit logs based on the certain criteria.
FAU_SAR.3	This TOE SFR is satisfied by the Audit function, which allows users of the TOE to search and sort audit records.
FAU_STG.1	This TOE SFR is satisfied by the Audit function, which protects audit records from unauthorized deletion or modification.
FAU_STG.4	This TOE SFR is satisfied by the Audit function, which allows the administrator to define TOE actions if the audit records consume all available memory.
FDP_IFC.1	This TOE SFR is satisfied by the Information Flow Control function, which specifies policy parameters to allow endpoint access to the network.
FDP_IFF.1	This TOE SFR is satisfied by the Information Flow Control function, which specifies policy parameters to allow endpoint access to the network.
FMT_MOF.1	This TOE SFR is satisfied by the Management function, which specifies that only a System Administrator is authorized to configure the auditing and Host Integrity Policy scanning parameters of the TOE.
FMT_MSA.1	This TOE SFR is satisfied by Management and Information Flow Control functions, which provide the TOE Administrator with full authority to configure the TOE to uphold NAC information flow control policies.
FMT_MSA.3	This TOE SFR is satisfied by Management and Information Flow Control functions, which allow the TOE Administrator to change default settings for how the TOE enforces the NAC information flow controls.
FMT_MTD.1(1)	This TOE SFR is satisfied by the Management function, which specifies the configuration actions available to the System Administrator and Workstation Users.
FMT_MTD.1(2)	This TOE SFR is satisfied by the Management function, which specifies the configuration actions available to the System Administrator for Host Integrity Policies.
FMT_MTD.1(3)	This TOE SFR is satisfied by the Management function, which specifies the configuration actions available to the System Administrator and Workstation Users.

SFR	RATIONALE TO SUPPORT SUFFICIENCY OF SECURITY FUNCTION
FMT_SMF.1	This TOE SFR is satisfied by Management function, which specifies the management functions available in the TOE.
FMT_SMR.1	This TOE SFR is satisfied by Management function, which assigns each user to the role of System Administrator, Administrator, Limited Administrator, or Workstation User.

Table 17 – Sufficiency of IT Security Functions

8.4 Rationale for IT Security Requirement Dependencies

Each functional requirement, including explicit requirements was analyzed to determine that all dependencies were satisfied. All requirements were then analyzed to determine that no additional dependencies were introduced as a result of completing each operation. Table 18 – TOE SFR Dependency Rationale identifies the functional requirement and its correspondent dependency.

In Table 18 – TOE SFR Dependency Rationale, the “Component” column lists all of the components included in this ST; each one is assigned a unique ID number in the “ID” column. Each component’s dependencies (from the CC) are listed in the “Dependency” column. The “Satisfied” column indicates how the dependencies are satisfied, with the number referencing the ID number of the component included in the AVPP that satisfies the dependencies. “Not Applicable” is used when there are no dependencies for a component.

ID	COMPONENT	DEPENDENCY	SATISFIED
1	FAU_GEN.1	FPT_STM.1	23
2	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	1 15
3	FAU_SAR.1(1) and FAU_SAR.1(2)	FAU_GEN.1	1
4	FAU_SAR.2	FAU_SAR.1	3
5	FAU_SAR.3	FAU_SAR.1	3
6	FAU_STG.1	FAU_GEN.1	1
7	FAU_STG.4	FAU_GEN.1 FAU_STG.1	1 6
8	FDP_IFC.1	FDP_IFF.1	9
9	FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	8 27

ID	COMPONENT	DEPENDENCY	SATISFIED
10	FDP_RIP.1	None	Not Applicable
11	FIA_AFL.1	FIA_UAU.1	13
12	FIA_SOS.1	None	Not Applicable
13	FIA_UAU.2	FIA_UID.1	15
14	FIA_UAU.6	None	Not Applicable
15	FIA_UID.2	None	Not Applicable
16	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	18 19
17	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	18 19
18	FMT_SMF.1	None	Not Applicable
19	FMT_SMR.1	FIA_UID.1	15
20	FPT_ITT.1	None	Not Applicable
21	FPT_RVM.1	None	Not Applicable
22	FPT_SEP.1	None	Not Applicable
23	FPT_STM.1	None	Not Applicable
24	FTA_SSL.1	FIA_UAU.1	15
25	FTA_TAB.1	None	Not Applicable
26	FMT_MSA.1	FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	8 18 19
27	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	26 19

Table 18 – TOE SFR Dependency Rationale

8.5 Rationale for Explicitly Stated Requirements

The TOE includes *FIA_PLA_EXP.1 – Performance and Log Alerts* as an explicitly stated requirement. This requirement was included to comply with PD-0129 and to be consistent with the Symantec™ Endpoint Protection Version 11.0 evaluation.

8.6 Rationale for Security Assurance Requirements

The EAL definitions and assurance requirements in Part 3 of the CC were reviewed and the *Basic Robustness Assurance Package* as defined in Section 5.4 was believed to best achieve the goal of addressing circumstances where developers and users require a low level of independently assured security in commercial products. The assurance package was selected because the TOE is an application executing on a system outside the TOE boundary, and basic is the highest robustness level available to application TOEs.

8.7 Rationale for Strength of Function Claim

Part 1 of the CC defines “strength of function” in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels defined in Part 1: SOF-basic, SOF-medium and SOF-high. SOF-basic is the strength of function level chosen for this Security Target. SOF-basic states, “a level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.” The rationale for choosing SOF-basic was to be consistent with the Basic Robustness guidelines.

8.8 Rationale for Protection Profile Claims

This Security Target references the *U.S. Government Protection Profile for Anti-Virus Applications for Workstations in Basic Robustness Environments, Version 1.1, April 4, 2006* (AVPP). While direct compliance is not claimed, this evaluation does include all functional requirements related to audit and management functions as detailed in the AVPP. This was done to ensure consistency of evaluated configuration between this TOE and the Symantec Endpoint Protection Version 11.0 Common Criteria evaluation, which does claim compliance to the AVPP.