Retina Enterprise Suite
Security Target

Version 1.0

05/25/07

Prepared for:
eEye Digital Security Corporation
One Columbia
Aliso Viejo, CA 92656

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

1. SECURITY TARGET INTRODUCTION 1

1.1 SECURITY TARGET, TOE AND CC IDENTIFICATION 1
1.2 CONFORMANCE CLAIMS 2
1.3 CONVENTIONS, TERMINOLOGY, AND ABBREVIATIONS 2
1.3.1 Conventions 2
1.3.2 Terminology and Abbreviations 3

2. TOE DESCRIPTION 4

2.1 TOE ARCHITECTURE 5
2.1.1 Physical Boundaries 5
2.1.2 Logical Boundaries 5

3. SECURITY ENVIRONMENT 7

3.1 THREATS TO SECURITY 7
3.1.1 TOE Threats 7
3.1.2 IT System Threats 7
3.2 ORGANIZATION SECURITY POLICIES 8
3.3 SECURE USAGE ASSUMPTIONS 8
3.3.1 Intended Usage Assumptions 8
3.3.2 Physical Assumptions 8
3.3.3 Personnel Assumptions 8

4. SECURITY OBJECTIVES 9

4.1 IT SECURITY OBJECTIVES FOR THE TOE 9
4.2 SECURITY OBJECTIVES FOR THE NON-IT ENVIRONMENT 9
4.3 IT SECURITY OBJECTIVES FOR THE IT ENVIRONMENT 9

5. IT SECURITY REQUIREMENTS 11

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 11
5.1.1 Identification and authentication (FIA) 11
5.1.2 Security management (FMT) 12
5.1.3 Protection of the TOE security functions (FPT) 13
5.1.4 NSS Component Requirements (NSS) 13
5.2 IT ENVIRONMENT SECURITY FUNCTIONAL REQUIREMENTS 14
5.2.1 Identification and authentication (FIA) 14
5.2.2 Protection of the TSF (FPT) 15
5.2.3 NSS Component Requirements (NSS) 15
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 15
5.3.1 Configuration management (ACM) 16
5.3.2 Delivery and operation (ADO) 16
5.3.3 Development (ADV) 16
5.3.4 Guidance documents (AGD) 17
5.3.5 Tests (ATE) 18
5.3.6 Vulnerability assessment (AVA) 19

6. TOE SUMMARY SPECIFICATION 20

6.1 TOE SECURITY FUNCTIONS 20
6.1.1 Identification and Authentication 20
6.1.2 Security Management 20
6.1.3 Protection of TSF 21
6.1.4 Network Security System 21
6.2 TOE SECURITY ASSURANCE MEASURES 22
6.2.1 Process Assurance 22

6.2.2 Delivery and operation ... 22
6.2.3 Development ... 23
6.2.4 Guidance documents ... 23
6.2.5 Tests ... 24
6.2.6 Vulnerability Assessment ... 24

7. PROTECTION PROFILE CLAIMS ... 25

8. RATIONALE ... 26

8.1 SECURITY OBJECTIVES RATIONALE ... 26
8.1.2 Security Objectives for Non-IT Environment Rationale ... 31
8.2 SECURITY REQUIREMENTS RATIONALE ... 31
8.3 STRENGTH OF FUNCTION RATIONALE ... 33
8.4 REQUIREMENT DEPENDENCY RATIONALE ... 34
8.5 SECURITY ASSURANCE RATIONALE ... 34
8.6 EXPLICITLY STATED REQUIREMENTS RATIONALE ... 34
8.7 TOE SUMMARY SPECIFICATION RATIONALE ... 34
8.8 PP CLAIMS RATIONALE ... 35

LIST OF TABLES

Table 1 Security Functional Components ... 11
Table 2 IT System Events ... 13
Table 3 Security Functional Components for the IT Environment ... 14
Table 4 Security Assurance Components ... 16
Table 5 Security Environment vs. Objectives ... 27
Table 6 Objective to Requirement Correspondence ... 31
Table 7 Requirement Dependency Rationale ... 34
Table 8 Security Functions vs. Requirements Mapping ... 35

1. Security Target Introduction

This section identifies the Security Target, Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation (TOE) is the Retina Enterprise Suite, a non-disruptive network security scanner and management server – the TOE is not invasive and does not interfere with the operation of the IT system being monitored. eEye Digital Security Corporation, Inc provides the Retina Enterprise Suite.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description

  This section gives an overview of the TOE, describes the TOE in terms of physical and logical boundaries, and states the scope of the TOE.

- Section 3 – TOE Security Environment

  This section details the expectations of the environment, the threats that are countered by eEye Digital Retina Enterprise Suite and the environment and the organizational security policies that the eEye Digital Retina Enterprise Suite must fulfill.

- Section 4 – TOE Security Objectives

  This section details the security objectives of the eEye Digital Retina Enterprise Suite and the environment.

- Section 5 – IT Security Requirements

  This section presents the security functional requirements (SFR) for eEye Digital Retina Enterprise Suite and the IT Environment that supports the TOE, and details the assurance requirements for EAL2.

- Section 6 – TOE Summary Specification

  This section describes the security functions represented in the eEye Digital Retina Enterprise Suite that satisfy the security requirements.

- Section 7 – Protection Profile Claims

  This section presents any protection profile claims.

- Section 8 – Rationale

  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability

1.1 Security Target, TOE and CC Identification

ST Title –Retina Enterprise Suite Security Target

ST Version – Version 1.0

ST Date – 05/25/07

TOE Identification – Retina Enterprise Suite consists of the following eEye products:

Retina Network Security Scanner Version 5.4.21.53

REM version 3.0.2.571

REM Events Server version 2.2.0.194

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004, ISO/IEC 15408.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.2, January 2004, ISO/IEC 15408-2.
    - Part 2 Extended (with NSS_SCN.1, NSS_ANL.1, NSS_RDR.1, NSS_STG.1, and NSS_STG.2)
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.2, January 2004, ISO/IEC 15408-3.
    - Part 3 Conformant
    - Evaluation Assurance Level 2 (EAL2)
    - SOF-Basic

1.3 Conventions, Terminology, and Abbreviations

This section specifies the formatting convention used in the Security Target.

1.3.1 Conventions

The requirements in this document are divided into assurance requirements and two sets of functional requirements. The first set of functional requirements, which were drawn from the Common Criteria, is designed to address the core System requirements for self-protection. The second set of requirements, which were invented and categorized by the short name, NSS, is designed to address the requirements for the System's primary function, which is NSS collection of data and responses to conclusions based upon that data.

The CC permits four functional component operations—assignment, refinement, selection, and iteration—to be performed on functional requirements. This ST will highlight the four operations in the following manner:

- Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
- Refinement: allows the addition of details. Refinements are indicated using bold and italics, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Selection: allows the specification of one or more elements from a list. Selections are indicated using underline (e.g., selection).
- Iteration: allows a component to be used more than once with varying operations. Not used in this ST.
- Explicitly stated Security Functional Requirements (i.e., those not found in Part 2 of the CC) are identified with "(EXP)".
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology and Abbreviations

The following terminology and abbreviations may be used within this Security Target:

Abbreviation	Definition
AIS	Automated Information System
API	Application programming interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CCEVS	Common Criteria Evaluation and Validation Scheme
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HLD	High-level Design
NSS	Network Security System
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating system
PP	Protection Profile
REM	Retina Enterprise Manager
SAIC	Science Applications International Corporation
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

Term	Definition
Automated Information System	Any equipment of an interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes software, firmware, and hardware.
Security configuration settings	Settings that implement different levels of security on the IT system. For example, security aspects for the different services installed on a system, user rights, password policies, etc. If the configuration settings were improperly configured, the IT system could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Term	Definition
Vulnerability	Hardware, firmware, or software flow that leaves an AIS (defined above) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

2. TOE Description

The TOE is the Retina Enterprise Suite, which consists of Retina Network Security Scanner[1] Version 5.4.21.53, REM Events Manager version 3.0.2.571, and REM Events Server version 2.2.0.194. The TOE is a non-disruptive network security scanner – the TOE is not invasive and does not interfere with the operation of the IT system being monitored. The TOE does not scan network traffic anomalies reported by sensors, as do some other types of IDS product. Rather, the TOE scans hosts identified within a specific IP range. Ports on targeted hosts are monitored for specific activities and events identified in an audit policy.

The specific information for which the Retina Network Security Scanner searches within an IP range is controlled by audit policies. Architecturally, the Scanner is similar to a traditional IDS where the management function creates and modifies signature files that will be pulled down from a managing server to sensors or pushed to network sensors. However, the Scanner does not sense network traffic. Rather, the audit policies determine the events monitored by Scanners for a specific range of IP addresses.

The scanning engine contained within the Retina Network Security Scanner scans IP address ranges for specific information. One or more instances of the Scanner is supported in the evaluated configuration. The scanning process is multithreaded, that allows the Retina Network Security Scanner to handle different targeted hosts at the same time. The services provided are mapped to specific types of vulnerabilities identified in the audit policy for the specific IP range.

The process of scanning a host occurs in roughly the following manner:

- ICMP ping: This step establishes if the host is responding.
- Target setup: The specific details of the target are built, such as MAC addresses, reverse DNS hostnames and other details.
- Syn Scan: Using a series of TCP syn packets, Retina Network Security Scanner scans the host to determine which ports are responding.
- Protocol Detection: Whenever a port is found to be open, after the TOE establishes a connection with the port, it determines the protocol of the service offered by the port using the port number and any protocol-specific information that is initially returned by the target when the connection is established.
- OS Detection: Using a series of packets designed to "fingerprint" the target operating system, Retina matches the output against a database of known operating systems.
- Audit Phase: The audit phase is effectively the second half of the scan and encompasses the basic "vulnerability" scan portion of the audit.

It is the audit phase when the Retina Network Security Scanner applies the audit policy looking for specific services and protocols for the specific targeted host.

The REM application provides web-based interfaces that can be used to access and manage TOE services. One instance is supported in the evaluated configuration. It is also called simply “event manager”. The REM Events Server application supports communication between Retina Network Security Scanner and REM application TOE components. One instance is supported in the evaluated configuration. It is also called simply “event server”.

[1] *eEye also sells the Scanner as a standalone product, which has also been evaluated at EAL2.*

All Scanner audit records are stored in a relational DBMS. The data stored within the REM relational DBMS is protected by the underlying database system and by the underlying operating system of the database host. The REM relational DBMS uses MSSQL and is considered part of the environment.

2.1 TOE Architecture

The TOE physical boundaries encompass the scanner and management software. The TOE can be described in terms of both physical and logical boundaries.

2.1.1 Physical Boundaries

The TOE consists of the following components:

- Retina Network Security Scanner application
- REM application
- REM Events Server application

The TOE depends on the following components:

- Web browser, which may be Microsoft Internet Explorer 4.01, 5.5, or 6.0 SP1
- Web server, Microsoft Internet Information Server 6.0
- Microsoft .NET Framework 1.1
- Operating system, which may be any one of: Microsoft Windows NT 4.0 SP6a, 2000, 2003, and XP
- Database, Microsoft SQL Server 2000

2.1.2 Logical Boundaries

The security functions provided by the TOE include:

- Identification and authentication
- Security management
- TSF protection
- Network security system

The sections below summarize the security functions provided by the TOE.

2.1.2.1 Identification and Authentication

The TOE requires users to provide unique identification and authentication data (passwords) before any access to the system is granted. The only authentication mechanism supported by the TOE is passwords.

See the corresponding section in the TSS for more detailed information.

2.1.2.2 Security Management

The eEye Digital Retina Enterprise Suite provides the authorized administrator with graphical user interfaces that can be used to configure and modify the options of the TOE. There are several modules available to the authorized administrator, such as modify the behavior of the data collection and review, query Scanner audit data, and restrict access and/or the ability to query and modify all other TOE data to the appropriate authorized user.

See the corresponding section in the TSS for more detailed information.

2.1.2.3 TSF Protection

The TOE ensures that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

See the corresponding section in the TSS for more detailed information.

2.1.2.4 Network Security System

The TOE monitors network traffic against predefined audit policies (that are set at the granularity of a specific host or collection of hosts), to detect known potential vulnerabilities. The Retina Network Security Scanner performs the defined audits by accessing the specific ports on a target IP address to determine the services provided. The TOE protects the data it collects by restricting access to authorized users.

See the corresponding section in the TSS for more detailed information.

2.1.2.5 Security Functionality in the IT Environment

The TOE relies on the IT Environment to provide SSL that it uses to protect network communication from disclosure and modification between an administrator’s web browser and REM, and between the event server and the scanner. The TOE also relies on the IT Environment to protect its application components, configuration data, and collected data. The IT Environment is also relied on to provide reliable time stamps.

3. Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed.

The statement of the TOE security environment defines the following:

- Threats that the product is designed to counter,
- Assumptions made on the operational environment and the method of use intended for the product,
- Organizational security policies with which the product is designed to comply.

3.1 Threats to Security

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

3.1.1 TOE Threats

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

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

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential inappropriate activity to go undetected.

3.1.2 IT System Threats

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

T.SCNCFG An unauthorized user may exploit system privileges and gain unauthorized access to the IT System and its data due to improper security configuration settings that may exist in the IT System the TOE monitors.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL An unauthorized user may exploit system privileges and gain unauthorized access to the IT System and its data due to vulnerabilities that may exist in the IT System the TOE monitors.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on Scanner data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of Scanner data received from all data sources.

3.2 Organization Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

P.DETECT Static system configuration information that might be indicative of the potential for a future inappropriate activity or the occurrence of a past inappropriate activity of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

P.ANALYZ Analytical processes and information to derive conclusions about inappropriate activity (past, present, or future) must be applied to Scanner data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P.PROTECT The TOE shall be protected from unauthorized access, modification, and disruption to the TOE and its data and functions.

3.3 Secure Usage Assumptions

The following usage assumptions are made about the intended environment of the TOE.

3.3.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

3.3.2 Physical Assumptions

A.PROTECT The components of TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.

A.SYSPROTECT The operating environment will provide protection to the TOE and its related data.

A.TIME The TOE’s IT environment will provide a reliable time source to enable the TOE to timestamp Scanner audit records.

3.3.3 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

4. Security Objectives

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as IT Security Objectives for the TOE, IT Security Objectives for the Environment, or Non-IT Security Objectives for the Environment.

4.1 IT Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE.

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

O.NSSCAN The Scanner must be able to collect and store static system configuration information that might be indicative of the potential for a future inappropriate activity or the occurrence of a past inappropriate activity of an IT System.

O.NSSANLZ The TOE must be able to accept data from the Scanners and then apply analytical processes and information to derive conclusions about inappropriate activity (past, present, or future).

O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.

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

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

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

4.2 Security Objectives for the Non-IT Environment

The TOE's operating environment must satisfy the following objectives. These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

O.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner that is consistent with IT security.

O.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

O.INTROP The TOE is interoperable with the IT System it monitors.

O.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System. These users are not careless, negligent, or hostile and will follow the guidance provided

O.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

4.3 IT Security Objectives for the IT Environment

The following security objectives for the IT environment of the TOE must be satisfied in order for the TOE to fulfill its own security objectives.

OE.AUTH_ACCESS The TOE operating environment must ensure that only authorized users gain access to the TOE data collected and stored by the TOE in the IT environment by ensuring all users are identified and authenticated.

OE.IDAUTH The IT Environment must be able to identify and authenticate users prior to allowing access to scanner application’s functions and data.

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

OE.TIME The TOE’s IT environment must provide a reliable time source for the TOE to provide accurate timestamps for Scanner audit records.

5. IT Security Requirements

5.1 TOE Security Functional Requirements

This section of the ST details the security functional requirements (SFR) for the TOE and the IT Environment that will support the TOE. The SFR were drawn from the CC Part 2. In addition, that some explicitly stated (i.e., not defined in the Common Criteria) security functional requirements pertaining to host monitoring are defined within a new class Network Security System (NSS) and are identified with short name NSS.

Security Functional Class	Security Functional Components
Identification and authentication (FIA)	User attribute definition (FIA_ATD.1)
	Timing of authentication (FIA_UAU.1)
	Timing of identification (FIA_UID.1)
Security management (FMT)	Management of security functions behavior (FMT_MOF.1)
	Management of TSF data (FMT_MTD.1)
	Specification of management functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	Non-bypassability of the TSP (FPT_RVM.1)
Network Security System (NSS)	Scanner data collection (NSS_SCN.1)
	Scanner data analysis (NSS_ANL.1)
	Restricted data review (NSS_RDR.1)

Table 1 Security Functional Components

5.1.1 Identification and authentication (FIA)

5.1.1.1 User attribute definition (FIA_ATD.1)

5.1.1.1.1 FIA_ATD.1.1

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

a) [**User identity;**

b) **Passwords;**

c) **Group membership**].

5.1.1.2 Timing of authentication (FIA_UAU.1)

5.1.1.2.1 FIA_UAU.1.1

The TSF shall allow [**all of the functions of the Retina Network Security Scanner**] on behalf of the user to be performed before the user is authenticated.

Application note: *The scanner component of the TOE permits the use of functions before authentication given that the scanner component provides its own user interface that does not authenticate users.*

5.1.1.2.2 FIA_UAU.1.2

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

5.1.1.3 Timing of identification (FIA_UID.1)

5.1.1.3.1 FIA_UID.1.1

The TSF shall allow [**all of the functions of the Retina Network Security Scanner**] on behalf of the user to be performed before the user is identified.

Application note: *The scanner component of the TOE permits the use of functions before authentication given that the scanner component provides its own user interface that does not identify users.*

5.1.1.3.2 FIA_UID.1.2

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

5.1.2 Security management (FMT)

5.1.2.1 Management of security functions behavior (FMT_MOF.1)

5.1.2.1.1 FMT_MOF.1.1

The TSF shall restrict the ability to modify the behavior of the functions [**of Scanner data collection and review of Scanner audit data**] to [**the Administrator and users possessing administrator-defined roles that have been granted the necessary permission**].

5.1.2.2 Management of TSF data (FMT_MTD.1)

5.1.2.2.1 FMT_MTD.1.1

The TSF shall restrict the ability to query [**and add Scanner data and Scanner audit data and modify**] the [**all other TOE data**] to [**the Administrator and users possessing administrator-defined roles that have been granted the necessary permission**].

5.1.2.3 Specification of Management Functions (FMT_SMF.1)

5.1.2.3.1 FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [**Management of Scanner data collected and Management of Scanner audit policies**].

5.1.2.4 Security roles (FMT_SMR.1)

5.1.2.4.1 FMT_SMR.1.1

The TSF shall maintain the roles [**administrator, administrator-defined roles**].

Application note: *Administrator-defined roles are implemented using groups. Group membership implies possession of the administrator-defined role that corresponds to the administrator-defined group.*

5.1.2.4.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles.

5.1.3 Protection of the TOE security functions (FPT)

5.1.3.1 FPT_RVM.1 Non-bypassability of the TSP

5.1.3.1.1 FPT_RVM.1.1

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

5.1.4 NSS Component Requirements (NSS)

5.1.4.1 Scanner Data Collection (NSS_SCN.1) (EXP)

5.1.4.1.1 NSS_SCN.1.1

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

a) Security configuration changes, access control configuration, service configuration, authentication configuration, detected known vulnerabilities, accountability policy configuration and

b) No other events. (EXP)

5.1.4.1.2 NSS_SCN.1.2

At a minimum, the TSF shall collect and record the following information from the targeted IT System resource(s):

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) The additional information specified in the Details column of Table 2 IT System Events. (EXP)

Component	Event	Details
NSS_SCN.1	Security configuration changes	Destination address
NSS_SCN.1	Access control configuration	Location, access settings
NSS_SCN.1	Service configuration	Service identification (name or port), interface, protocols
NSS_SCN.1	Authentication configuration	Account names for cracked passwords, account policy parameters
NSS_SCN.1	Detected known vulnerabilities	Identification of the known vulnerability
NSS_SCN.1	Accountability policy configuration	Accountability policy configuration parameters

Table 2 IT System Events

5.1.4.2 Scanner data analysis (NSS_ANL.1) (EXP)

5.1.4.2.1 NSS_ANL.1.1

The TSF shall perform the following analysis function(s) on all Scanner data collected:

a) Statistical. (EXP)

5.1.4.2.2 NSS_ANL.1.2

The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of Scanner data source. (EXP)

5.1.4.3 Restricted Data Review (NSS_RDR.1) (EXP)

5.1.4.3.1 NSS_RDR.1.1

The TSF shall provide the authorized Administrator with the capability to read audit data, reports, and configuration information from the Scanner data collected. (EXP)

5.1.4.3.2 NSS_RDR.1.2

The TSF shall provide the Scanner data collected in a manner suitable for the user to interpret the information. (EXP)

5.1.4.3.3 NSS_RDR.1.3

The TSF shall prohibit all users read access to the Scanner data collected, except those users that have been granted explicit read-access. (EXP)

5.2 IT Environment Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the IT Environment. This section organizes the SFRs by CC class. Table 2 identifies all SFRs implemented by the IT Environment and indicates the ST operations performed on each requirement.

Security Functional Class	Security Functional Components
Identification and authentication (FIA)	User authentication before any action (FIA_UAU.2)
	User identification before any action (FIA_UID.2)
Protection of the TSF (FPT)	TSF domain separation (FPT_SEP.1)
	Reliable time stamps (FPT_STM.1)
	Basic internal TSF data transfer protection (FPT_ITT.1)
Network Security System (NSS)	Guarantee of scanner data availability (NSS_STG.1)

Table 3 Security Functional Components for the IT Environment

5.2.1 Identification and authentication (FIA)

5.2.1.1 User authentication before any action (FIA_UAU.2)

5.2.1.1.1 FIA_UAU.2.1

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

5.2.1.2 User identification before any action (FIA_UID.2)

5.2.1.2.1 FIA_UID.2.1

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

5.2.2 Protection of the TSF (FPT)

5.2.2.1 Basic internal TSF data transfer protection (FPT_ITT.1)

5.2.2.1.1 FPT_ITT.1.1

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

5.2.2.2 TSF domain separation (FPT_SEP.1)

5.2.2.2.1 FPT_SEP.1.1

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

5.2.2.2.2 FPT_SEP.1.2

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

5.2.2.3 Reliable time stamps (FPT_STM.1)

5.2.2.3.1 FPT_STM.1.1

The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for its own **and TOE** use.

5.2.3 NSS Component Requirements (NSS)

5.2.3.1 Guarantee of Scanner Data Availability (NSS_STG.1) (EXP)

5.2.3.1.1 NSS_STG.1.1

The ~~TSF~~ **IT Environment** shall protect the stored Scanner data collected from unauthorized deletion. (EXP)

5.2.3.1.2 NSS_ STG.1.2

The ~~TSF~~ **IT Environment** shall protect the stored Scanner data collected from unauthorized modification. (EXP)

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 2 (EAL2) components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance

Requirement Class	Requirement Component
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 4 Security Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1d The developer shall provide a reference for the TOE.
ACM_CAP.2.2d The developer shall use a CM system.
ACM_CAP.2.3d The developer shall provide CM documentation.
ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2c The TOE shall be labelled with its reference.
ACM_CAP.2.3c The CM documentation shall include a configuration list.
ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items.
ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user’s site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.
ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.
ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2c The functional specification shall be internally consistent.

ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4c The functional specification shall completely represent the TSF.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.1.1c The presentation of the high-level design shall be informal.

ADV_HLD.1.2c The high-level design shall be internally consistent.

ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.

AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Tests (ATE)

5.3.5.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.

ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.

ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.

ATE_IND.2.1c The TOE shall be suitable for testing.

ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.6 Vulnerability assessment (AVA)

5.3.6.1 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.6.2 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.

AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Identification and Authentication

FIA_UAU.1, FIA_UID.1 Enterprise Suite Components and Authentication

Access to the centralized reporting and remediation functions that the REM application provides that the Retina scanner application does not is restricted. Administrators are required to log into the REM application using a REM-defined username and password. Access to Retina scanner application's interfaces (compared to REM interfaces that may be used to initiate a scan after logging into REM) is not restricted by any of the Retina Enterprise Suite components. If a user can log into the operating system on the machine where the Retina scanner application is installed, that user may access Retina scanner functions.

FIA_ATD.1 REM Users and Authentication

REM defines users in terms of user identity, password, and group membership information. REM implements its own username/password mechanism. There is a single pre-defined "administrator" account that can be used to create additional user accounts as well as groups. The administrator account can create users and groups, and assign users and permissions to groups. Permissions that can be assigned to groups[2] include:

- scope type permissions – the range of IP addresses that members of a group may examine using the TOE.
- reporting/remediation type permissions – the TOE management interfaces that that members of a group may access

All users must present a username and password before the event manager GUI will allow access to its functions.

6.1.2 Security Management

FMT_SMR.1 Security Roles

The TOE supports both administrator and administrator-defined roles. The single pre-defined administrator account that can be used to create users and groups, and assign users and permissions to groups. The TOE checks that the user is an administrator, or that the user possesses the necessary permissions, or that the user is a member of a group that possesses the requested permissions before allowing access to a requested management interface.

FMT_SMF.1, FMT_MOF.1, FMT_MTD.1 Security Management

The TOE is managed using a GUI provided by REM Events Manager. REM Events Manager is a state-of-the-art graphical navigation tool that offers users extensive control over the complete life cycle of vulnerabilities--from the management of assets, to the discovery of vulnerabilities, to their remediation. REM Events Manager, through the REM Security Management Console, offers users a graphical view of the risk level of a single machine or an entire group of machines collectively and simultaneously.

REM Events Manager uses industry-standard Computer Vulnerabilities and Exposures (CVE) terms and concepts where available and appropriate. REM Events Manager enables users to view the network's current state of vulnerability and to examine the status and nature of network attacks--all from a graphical vantage point that facilitates exploration and analysis of the available data.

For example, REM Events Manager can enable a user to view the number and nature of network or system vulnerabilities, attempted attacks, and open ports for a single asset or for a group of assets. This type of information

[2] *Permissions cannot be assigned to individual users. Permissions can only be assigned to groups.*

can be extremely valuable to an effort to proactively and pre-emptively protect the security of your organization's network.

REM Events Manager enables network security managers to:

- Create an inventory of all assets
- Audit the assets and evaluate the results of the audit
- Delegate tasks and, if necessary, remediate vulnerabilities
- Generate reports
- Perform risk analyses

6.1.3 Protection of TSF

FPT_RVM.1 Non-bypassability

The TSF requires that all users be successfully authenticate before any TSF functions (other than entering identification and authentication data) can be performed. Once a user is identified and authenticated, they are associated with a role that determines which function interfaces the TOE will offer to the user. Each interface is defined to offer specific capabilities, all controlled by the TSF. The TSF does not offer general programming capabilities that might offer the opportunity to attempt to bypass the TSP.

6.1.4 Network Security System

NSS_SCN.1 Scanner Data Collection

By default, all of the auditable categories are enabled. Collected audit data is written to files in the IT Environment. The audit policies govern the collection of data regarding inappropriate activities on the IT systems it monitors. [3]

The TOE collects and records data related to the following events:

- Destination address of security configuration changes
- Location of access control configuration and the settings
- Service configuration, such as the name and/or port, the interface, and the protocol
- Authentication configuration, the user accounts of cracked passwords[4] and the account policy parameters
- Detection of known vulnerabilities, therefore the identification of the vulnerabilities
- Accountability policy configuration

Following is a list of additional information recorded in each audit records:

- Date and time
- Type of event
- Subject identity
- Outcome of the events

This Scanner data is presented in such a manner that the authorized user can read and interpret the content of the information; hence the information is presented in a manner suitable for human interpretation

[3] *Product features that are described in the administrative guidance that are part of the intended operation of the TOE but were not evaluated include: use of the Audit Wizard, use of Retina Plug-ins, use of Auto-Update (which will take the TOE out of its evaluated configuration), and using a DSN to store session data.*

[4] *References to "cracked passwords" when describing how the TOE collects data is not meant to imply that for example dictionary attacks are attempted, rather it is an informal description of the nature of the checks related to accounts. Known vulnerabilities are in general checked as described/applicable for each audit module.*

NSS_ANL.1 Scanner Data Analysis

The TOE uses statistical analysis to identify deviations from normal patterns of behavior that includes frequency analysis. Audit policies created at the REM Event Manager determine the events monitored by Scanners for a specific range of IP addresses. Audit events are typically monitored by accessing specific ports on a target IP address to determine the services provided that are applicable to the events to monitor. The information that is included in the audit records contains at least the date and time of the result, the type of result, and the identification of the Scanner data source.

NSS_RDR.1 Restricted Data Review

In the TOE environment, only successfully identified and authenticated users can access the TOE, and then only users who hold the appropriate authorization can view the data that is collected. Authorized Administrators can view the overall health of the TOE as well as the data colleted. All data is presented in such a manner that the it can be read and the contents of the data can be interpreted; thus the reader, the authorized Administrator can understand the content of the information presented as it is presented in a manner suitable for human interpretation.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL2 assurance requirements:

- Process Assurance;
- Delivery and Operation;
- Design Documentation;
- Guidance;
- Tests; and
- Vulnerability Assessment.

6.2.1 Process Assurance

6.2.1.1 Configuration Management

The CM documentation describes the processes and procedure that are followed and utilized in the tracking and monitoring the changes to the CM items and the generation of the TOE. The configuration management measures applied by eEye ensure that configuration items are uniquely identified. eEye ensures changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled. eEye performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, vulnerability analysis documentation, and configuration management documentation and all of these items are identified in the Configuration Management Plan as configuration items. These activities are documented in:

- eEye Retina Configuration Management Plan, version 0.21, 01/26/07.

The Configuration Management assurance measure satisfies the following assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and operation

eEye provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. eEye's delivery procedures describe all applicable procedures to be used to prevent inappropriate access to the TOE. eEye also provides documentation that describes the steps necessary to install eEye Retina Enterprise Suite in accordance with the evaluated configuration.

These activities are documented in:

- REM Security Management Console Administration Guide, v3.02, 2005
- REM Users Manual, REM-M-032803, 2003
- REM Manual Addendum, REM-EU-M-030305, v2.2.0, 2005
- Retina Network Security Scanner Users Manual, 5-3-1, 2005
- Release Notes for REM Events Manager version 3.0.2
- Release Notes for REM Events Server version 2.2.0
- Release Notes for Retina Network Security Scanner version 5.4.21.

The Delivery and operation assurance measure satisfies the following EAL 2 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

eEye has set of manuals describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces, a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces, and correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the actual implementation of the TOE.

These activities are documented in:

- eEye Retina Enterprise Suite Design, version 2, 01/30/07.

The Development assurance measure satisfies the following EAL2 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 Guidance documents

eEye provides administrator guidance documents that describe the administrative functions and the administrative interface available to authorized administrators of eEye Retina Enterprise Suite. These documents are consistent with other supplied documentation and describe how to administer eEye Retina Enterprise Suite in a secure manner. The guidance documents describe the assumptions regarding user behavior that is relevant to the secure operation of the TOE, and describes the parameters that are under the control of the authorized administrators.

These activities are documented in:

- REM Security Management Console Management Guide, v3.02, 2005
- REM Security Management Console Operations Guide, v3.02, 2005
- REM Security Management Console Administration Guide, v3.02, 2005.
- Retina Network Security Scanner Users Manual, 2005.

The Guidance documents assurance measure satisfies the following EAL2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Tests

eEye has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. eEye has documented each test as well as an analysis of test coverage demonstrating that the security aspects of the design evident from the functional specification is appropriately tested. Actual test results are provided that demonstrate that the tests have been applied and that the TOE operates as designed. The test documentation consist of the following documents:

- eEye Retina Enterprise Suite Test Document (COV and FUN), version 3, 04/27/07.

The Tests assurance measure satisfies the following EAL2 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.6 Vulnerability Assessment

eEye has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-basic.

eEye performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- eEye Retina Scanner and Enterprise Suite Vulnerability Analysis, version 5, 03/20/07.

The Vulnerability assessment assurance measure satisfies the following EAL2 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

The TOE does not claim compliance to any Protection Profile.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Strength of Function;
- Security Functional Requirement Dependencies;
- Explicitly Stated Requirements; and
- TOE Summary Specification.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and organizational security policy statement. The following table demonstrates that the mapping between the assumptions, threats, and organizational security polices to the security objectives is complete. The discussion following provides the rationale of coverage for each assumption, threat, and organizational security policy.

	O.PROTECT	O.NSSCAN	O.NSSANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.INTEGR	O.INSTAL	O.INTROP	O.PHYCAL	O.CREDEN	O.PERSON	OE.AUTH_ACCESS	OE.IDAUTH	OE.SEP	OE.TIME
A.ACCESS									X							
A.ASCOPE									X							
A.DYNMIC									X			X				
A.MANAGE												X				
A.NOEVIL								X		X	X	X				
A.NOTRST										X	X					
A.PROTECT										X						
A.SYSPROTECT															X	
A.TIME																X
T.COMINT	X				X	X	X						X	X		
T.COMDIS	X				X	X	X						X	X		
T.FALASC			X													
T.FALREC			X													
T.IMPCON				X	X	X		X						X		
T.LOSSOF	X				X	X	X						X	X		
T.PRIVIL	X				X	X								X		
T.SCNCFG		X														
T.SCNMLC		X														
T.SCNVUL		X														
P.ACCESS	X	X	X		X	X								X		
P.ANALYZ		X	X													

	O.PROTECT	O.NSSCAN	O.NSSANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.INTEGR	O.INSTAL	O.INTROP	O.PHYCAL	O.CREDEN	O.PERSON	OE.AUTH_ACCESS	OE.IDAUTH	OE.SEP	OE.TIME
P.DETECT		X														
P.INTGTY							X						X			
P.MANAGE	X			X	X	X		X			X	X		X		
P.PROTECT					X	X				X			X	X		

Table 5 Security Environment vs. Objectives

8.1.1.1 A.ACCESS

The TOE has access to all the IT System data it needs to perform its functions.

The O.INTROP objective ensures the TOE has the needed access.

8.1.1.2 A.ASCOPE

The TOE is appropriately scalable to the IT System the TOE monitors.

The O.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

8.1.1.3 A.DYNMIC

The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

The O.INTROP objective ensures the TOE has the proper access to the IT System. The O.PERSON objective ensures that the TOE will be managed appropriately.

8.1.1.4 A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

The O.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

8.1.1.5 A.NOEVIL

The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

The O.INSTAL objective ensures that the TOE is properly installed and O.PERSON ensures that the authorized administrators are trained, not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The O.PHYCAL objective provides for physical protection of the TOE. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.

8.1.1.6 A.NOTRST

The TOE can only be accessed by authorized users.

The O.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.

8.1.1.7 A.PROTECT

> The components of TOE critical to security policy enforcement must be located within controlled access facilities that will be protected from unauthorized physical access and modification.

The O.PHYCAL provides for the physical protection of the TOE hardware and software.

8.1.1.8 A.SYSPROTECT

> The operating environment will provide protection to the TOE and its related data.

The OE.SEP objective ensures the operating environment provides the mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed.

8.1.1.9 A.TIME

> The TOE's IT environment will provide a reliable time source to enable the TOE to timestamp Scanner audit records.

The objective, OE.TIME ensures the IT environment provides a reliable time source for the TOE to provide an accurate timestamp for all Scanner audit records.

8.1.1.10 T.COMDIS

> An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH AND OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH AND OE.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTECT objective addresses this threat by protecting itself from unauthorized modifications and access to its functions and data. The OE.AUTH_ACCESS objective ensures that only authorized administrators have access to the TOE data that is collected and stored in the IT environment.

8.1.1.11 T.COMINT

> An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH AND OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH AND OE.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTECT objective addresses this threat by protecting itself from unauthorized modifications and access to its functions and data. The OE.AUTH_ACCESS objective ensures that only authorized administrators have access to the TOE data that is collected and stored in the IT environment.

8.1.1.12 T.FALASC

> The TOE may fail to identify vulnerabilities or inappropriate activity based on association of Scanner data received from all data sources.

The O.NSSANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

8.1.1.13 T.FALREC

> The TOE may fail to recognize vulnerabilities or inappropriate activity based on Scanner data received from each data source.

The O.NSSANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

8.1.1.14 T.IMPCON

An unauthorized user may inappropriately change the configuration of the TOE causing potential inappropriate activity to go undetected.

The O.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH AND OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH AND OE.IDAUTH objective by only permitting authorized users to access TOE functions.

8.1.1.15 T.LOSSOF

An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

The O.IDAUTH AND OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH AND OE.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTECT objective addresses this threat by protecting itself from unauthorized modifications and access to its functions and data. The OE.AUTH_ACCESS objective ensures that only authorized administrators have access to the TOE data that is collected and stored in the IT environment.

8.1.1.16 T.PRIVIL

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

The O.IDAUTH AND OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH AND OE.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTECT objective addresses this threat by protecting itself from unauthorized modifications and access to its functions and data.

8.1.1.17 T.SCNCFG

An unauthorized user may exploit system privileges and gain unauthorized access to the IT System and its data due to improper security configuration settings that may exist in the IT System the TOE monitors.

The O.NSSCAN objective counters this threat by requiring the Scanner to collect and store static system configuration information that might be indicative of a configuration setting change.

8.1.1.18 T.SCNMLC

Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

The O.NSSCAN objective counters this threat by requiring the Scanner to collect and store static system configuration information that might be indicative of malicious code.

8.1.1.19 T.SCNVUL

An unauthorized user may exploit system privileges and gain unauthorized access to the IT System and its data due to vulnerabilities that may exist in the IT System the TOE monitors.

The O.NSSCAN objective counters this threat by requiring the Scanner to collect and store static system configuration information that might be indicative of a vulnerability.

8.1.1.20 P.ACCESS

All data collected and produced by the TOE shall only be used for authorized purposes.

The O.IDAUTH AND OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH AND OE.IDAUTH objective by only permitting authorized users to access TOE functions and data. The O.PROTECT objective addresses this policy by ensuring the TOE protects itself from unauthorized modifications and access to its functions and data. O.NSSCAN objective ensures that the Scanner is able to collect and store information and O.NSSANLZ objective ensures the data collected by the Scanner is received and then analytical processes are applied to the information to derive conclusions about inappropriate activity (past, present, or future).

8.1.1.21 P.ANALYZ

Analytical processes and information to derive conclusions about inappropriate activity (past, present, or future) must be applied to Scanner data and appropriate response actions taken.

O.NSSCAN objective ensures that the Scanner is able to collect and store information and O.NSSANLZ objective ensures the data collected by the Scanner is received and then analytical processes are applied to the information to derive conclusions about inappropriate activity (past, present, or future).

8.1.1.22 P.DETECT

Static system configuration information that might be indicative of the potential for a future inappropriate activity or the occurrence of a past inappropriate activity of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

The O.NSSCAN objective addresses this threat by requiring a TOE to collect Scanner data.

8.1.1.23 P.INTGTY

Data collected and produced by the TOE shall be protected from modification.

The O.INTEGR objective ensures the protection of data from modification. The OE.AUTH_ACCESS objective ensures that only authorized administrators have access to the TOE data that is collected and stored in the IT environment.

8.1.1.24 P.MANAGE

The TOE shall only be managed by authorized users.

The O.PERSON objective ensures carefully selected and trained administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH AND OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH AND OE.IDAUTH objective by only permitting authorized users to access TOE functions. The O.CREDEN objective requires administrators to protect all authentication data. The O.PROTECT objective addresses this threat by protecting itself from unauthorized modifications and access to its functions and data.

8.1.1.25 P.PROTECT

The TOE shall be protected from unauthorized access, modification, and disruption to the TOE and its data and functions.

The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The O.PHYCAL objective protects the TOE from unauthorized physical modifications to the TOE. The O.IDAUTH AND OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH AND OE.IDAUTH objective by only permitting authorized users to access TOE data. The OE.AUTH_ACCESS objective ensures that only authorized administrators have access to the TOE data that is collected and stored in the IT environment.

8.1.2 Security Objectives for Non-IT Environment Rationale

The purpose for the Non-IT Environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

8.2 Security Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.PROTECT	O.NSSCAN	O.NSSANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.INTEGR	OE.AUTH_ACCES	OE.IDAUTH	OE.SEP	OE.TIME
FIA_ATD.1						X					
FIA_UAU.1					X	X					
FIA_UAU.2									X		
FIA_UID.1					X	X					
FIA_UID.2									X		
FMT_MOF.1	X				X						
FMT_MTD.1	X				X		X				
FMT_SMF.1				X							
FMT_SMR.1											
FPT_ITT.1								X			
FPT_RVM.1	X			X		X	X				
FPT_SEP.1										X	
FPT_STM.1											X
NSS_SCN.1		X									
NSS_ANL.1			X								
NSS_RDR.1				X	X						
NSS_STG.1	X				X		X	X			

Table 6 Objective to Requirement Correspondence

8.2.1.1 O.PROTECT

The TOE must protect itself from unauthorized modifications and access to its functions and data.

FMT_MOF.1 restricts the ability to manage the Scanner data collected and review of Scanner audit data to the administrator.

FMT_MTD.1 provides the ability for the administrator to query Scanner audit data and add Scanner data as well as manage all other TSF data.

FPT_RVM.1 The TOE is required to ensure that its functions cannot be bypassed.

8.2.1.2 O.NSSCAN

The Scanner must collect and store static system configuration information that might be indicative of the potential for a future inappropriate activity or the occurrence of a past inappropriate activity of an IT System.

NSS_SCN.1 requires the TOE to collect information from the targeted IT system as defined in the audit policy.

8.2.1.3 O.NSSANLZ

The TOE must accept data from the Scanners and then apply analytical processes and information to derive conclusions about inappropriate activity (past, present, or future).

NSS_ANL.1 ensures that statistical analysis is used to identify deviations from normal patterns of behavior on the collected Scanner data

8.2.1.4 O.EADMIN

The TOE must include a set of functions that allow effective management of its functions and data.

NSS_RDR.1 provides the ability for authorized administrator to view the Scanner data collected.

FMT_SMF.1 The TOE also provides a set of tools that are accessible to the administrator to review the Scanner audit data.

FPT_RVM.1: The TOE is required to ensure that its functions cannot be bypassed.

8.2.1.5 O.ACCESS

The TOE must allow authorized users to access only appropriate TOE functions and data.

NSS_RDR.1 provides the ability for authorized administrator to view the Scanner data collected.

NSS_STG.1a-b ensures Scanner data is protected from unauthorized deletion.

FIA_UAU.2a The TOE is required to authentication users before allowing access to protected TSF functions and data.

FIA_UID.2a The TOE is required to identify users before allowing access to protected TSF functions and data.

FMT_MOF.1 restricts the ability to manage the Scanner data collected and review of Scanner audit data to the administrator.

FMT_MTD.1 provides the ability for the administrator to query Scanner audit data and add Scanner data as well as manage all other TSF data.

8.2.1.6 O.IDAUTH

The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

FIA_ATD.1 The TOE is required to manage user security attributes that are used to enforce the authentication policy.

FIA_UAU.1 The REM application authenticates users. The Retina scanner application does not.

FIA_UID.1 The REM application identifies users. The Retina scanner application does not.

FPT_RVM.1: The TOE is required to ensure that its functions cannot be bypassed.

8.2.1.7 O.INTEGR

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

FMT_MTD.1 provides the ability for the administrator to query Scanner audit data and add Scanner data as well as manage all other TSF data.

FPT_RVM.1: The TOE is required to ensure that its functions cannot be bypassed.

8.2.1.8 OE.AUTH_ACCESS

The TOE operating environment must ensure that only authorized users gain access to the TOE data collected and stored by the TOE in the IT environment.

FPT_ITT.1 ensures the TOE protects TSF data from modification when it is transmitted between separate parts of the TOE by utilizing SSL provided by the environment.

NSS_STG.1 ensures Scanner data is protected from unauthorized deletion and modification.

8.2.1.9 OE.IDAUTH

The IT Environment must be able to identify and authenticate users prior to allowing access to scanner application's functions and data.

FIA_UAU.2 The Retina scanner application does not authenticate users, the operating system in the IT Environment is relied on to restrict access to the scanner.

FIA_UID.2 The Retina scanner application does not identify users, the operating system in the IT Environment is relied on to restrict access to the scanner.

8.2.1.10 OE.SEP

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

FPT_SEP.1 requires the IT Environment to protect the TOE from untrusted process that could attempt to tamper with or bypass the TOE satisfies this objective.

8.2.1.11 OE.TIME

The TOE's IT environment must provide a reliable time source for the TOE to provide accurate timestamps for Scanner audit records.

FPT_STM.1 requires the IT Environment to provide accurate and reliable time mechanism to be utilized by the TOE for the date/time stamp in the [Scanner] audit record.

8.3 Strength of Function Rationale

The TOE strength of function is SOF-basic. While the TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information, its password mechanism can resist even persistent more sophisticated attackers. The password mechanism in the REM component with its minimum password length of six characters together with a failed login mechanism that locks users out after three failed attempts (requiring the account be unlocked by an authorized administrator) effectively guarantees SOF-basic for FIA_UAU.1.

8.4 Requirement Dependency Rationale

The ST satisfies all the requirement dependencies of the Common Criteria, except as noted below. Table 7 Requirement Dependency Rationale lists each requirement from Section 5, IT Security Requirements with a dependency and indicates which requirement was included to satisfy the dependency, if any. For each dependency not included, a justification is provided in Section 8.6 Explicitly Stated Requirements Rationale.

Functional Component	Dependency	Included
FIA_ATD.1	None	
FIA_UAU.1	FIA_UID.1	YES (FIA_UID.1)
FIA_UAU.2	FIA_UID.1	YES (FIA_UID.2)
FIA_UID.1	None	
FIA_UID.2	None	
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	YES
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	YES
FMT_SMF.1	None	
FMT_SMR.1	FIA_UID.1	YES (FIA_UID.1)
FPT_ITT.1	None	
FPT_RVM.1	None	
FPT_SEP.1	None	
FPT_STM.1	None	

Table 7 Requirement Dependency Rationale

8.5 Security Assurance Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position.

The chosen assurance level is appropriate with the statement of the security environment (threats, organizational policies, assumptions) and the security objectives defined in this ST. For instance, EAL2 is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE. The administrative staff is carefully selected and trained (O.PERSON). The administrative staff is also conscientious and not hostile and will follow the TOE documentation (A.NOEVIL). The TOE is physically protected (O.PHYCAL), and properly and securely configured (O.INSTAL).

Within such environments, it is assumed that attackers will have little attack potential. As such, given the amount of assurance deemed necessary to meet the security environment and objectives of the TOE, EAL2 is an appropriate level of assurance for the TOE described in this ST.

8.6 Explicitly Stated Requirements Rationale

A family of NSS requirements was created to specifically address the data collected and analyzed by an NSS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of NSS data and provide requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. Working together, this set of security functions satisfies all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The security functions work together to provide all of the security requirements. The security functions described in the TOE Summary Specification are all necessary for the required security functionality in the TSF. The following table, Table 8 Security Functions vs. Requirements Mapping, demonstrates the relationship between security requirements and security functions.

	IDENTIFICATION & AUTHENTICATION	SECURITY MANAGEMENT	PROTECTION OF TSF	SYSTEM DATA COLLECTION	SYSTEM DATA ANALYSIS
FIA_UAU.2a	X				
FIA_ATD.1	X				
FIA_UAU.1	X				
FIA_UID.1	X				
FMT_MOF.1		X			
FMT_MTD.1		X			
FMT_SMF.1		X			
FMT_SMR.1		X			
FPT_RVM.1			X		
NSS_SCN.1				X	
NSS_ANL.1					X
NSS_RDR.1					X

Table 8 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See section 7, Protection Profile Claims.