NetIQ Security Manager 5.5
Security Target

Version 0.9

07/09/07

Prepared for:
NetIQ, Incorporated
1233 West Loop South, Suite 1800
Houston, Texas 77027

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

LIST OF TABLES

1. Security Target Introduction

This section provides the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is the NetIQ Security Manager Version 5.5 provided by NetIQ, Inc. NetIQ Security Manager is an application that can act as an intrusion detection system for intrusion detection systems, as well as for operating systems, firewalls, and antivirus applications.

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 its 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 the TOE and IT environment, and the organizational policy that the TOE must fulfill.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the TOE and IT environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for the TOE and IT Environment that supports the TOE, and details the assurance requirements for EAL2.
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the TOE 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 – NetIQ Security Manager 5.5 Security Target

ST Version – Version 0.9

ST Date – 07/09/07

TOE Identification –NetIQ Security Manager Version 5.5

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

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 2.3, August 2005.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
  - Part 3 Conformant
  - Evaluation Assurance Level 2 (EAL2)
  - Strength of Function Claim: SOF-basic

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Explicitly stated Security Functional Requirements (i.e., those not found in Part 2 of the CC) are identified with "**(EX)**".
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2. TOE Description

The Target of Evaluation (TOE) is NetIQ Security Manager version 5.5.

NetIQ Security Manager is an application that can act as an intrusion detection system for intrusion detection systems, as well as for operating systems, firewalls, and antivirus applications. Intrusion detection systems (IDS) monitor IT systems for activities that may inappropriately affect the IT systems' assets and react appropriately. The TOE, instead of performing statistical, signature, and/or integrity analysis on event data that the TOE collects from monitored systems, provides the ability to correlate events from otherwise disparate monitored systems, which as noted may include monitoring systems. NetIQ Security Manager event data collection is depicted in the figure below.

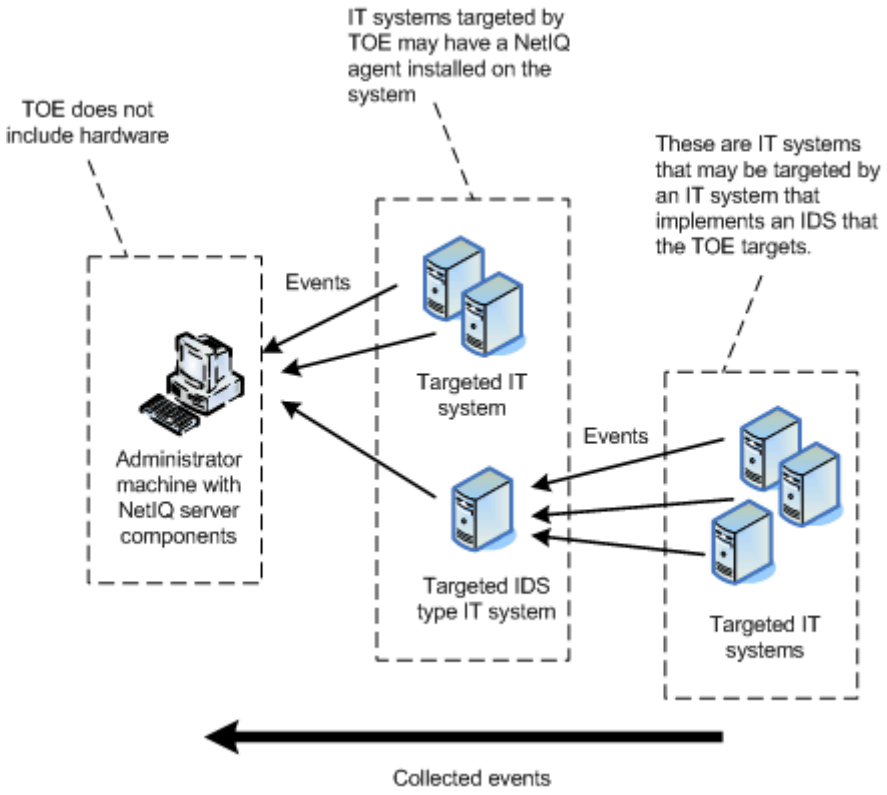

Figure 1: NetIQ Security Manager event data collection

The remainder of this section summarizes the TOE architecture.

2.1 TOE Overview

The TOE provides the ability to collect and react to event data from targeted IT systems using administrator configurable rules. The TOE provides the ability to collect, standardize, and archive collected data from targeted IT systems and provides the ability to generate reports to review collected data. NetIQ server components and/or agents (depending if an agent-based or an agent-less configuration is used to collect event data from a given targeted IT system) evaluate data collection rules in what is called an event workflow to determine if a rule matches. In an agent-based configuration, there is a NetIQ client application called an agent running on the same machine as the targeted IT system. In an agent-less configuration, there is no TOE software running on the targeted IT system. The TOE in an agent-less configuration uses targeted IT system-specific interfaces (e.g. application-specific network interfaces, e.g. reading from a database where a targeted IT system writes event data, etc.) to collect event data. In the event of a rule match the agent applies the corresponding response action associated with that rule. The NetIQ server components and/or agents generate a alerts and in the case of agent-based configurations, send alert data to

the NetIQ server components, along with the events that occurred on the targeted IT system that triggered the alert. NetIQ agents check for new rules or updates to existing rules by initiating connections with NetIQ server components at regular intervals.

The TOE provides the ability to administratively configure the following types of rules:

- *Event rules* – this type of rule can be used to monitor for a certain real-time event, and then send an alert to NetIQ server component user interfaces or trigger a response, such as running a script or paging a response team
- *Filtering rules* – this type of rule can be used to manage the large number of real-time events that TOE collects. Filtering rules can specify whether Security Manager processes events or stores them in the database in the IT environment
- *Missing event rules* – this type of rule can be used to monitor for a real-time event that one expects to occur within a specified time interval, but does not. For example, if one performs or automates routine tasks such as system backups, the TOE can generate alerts and responses if these tasks do not occur as planned
- *Consolidation rules* – this type of rule can be used to group similar real-time events from an agent into one summary event. Event consolidation provides a combined event to replace many similar events generated in a short time to reduce event noise
- *Collection rules* – this type of rule can be used to identify events to collect from specified sources to monitor in real-time. Collection rules do not generate alerts or provide other responses
- *Correlation rules* – this type of rule can be used to monitor and analyze a stream of real-time events to look for patterns that indicate a security breach. Rather than detecting a single event, a correlation rule detects multiple events and identifies patterns using the elapsed time, the number of events, the event identification, matching event parameters, or the order in which the event occurred
- *Log collection rules* – this type of rule can be used collect targeted IT system logs for archival and reporting. Log collection rules are similar to collection rules because they also do not generate alerts or respond to events. However, events that match a log collection rule are not further evaluated for other real-time processing rule matches
- *Log filter rules* – this type of rule can be used to filter collected log data and prevent the TOE from storing it in the database. Administrators can create log filter rules to filter archival events that they have determined are too noisy or unimportant
- *Performance measuring rules* - this type of rule can be used to provide real-time monitoring of Windows computers for system resource usage and performance thresholds. Also called performance processing rules.
- *Threshold rules* – this type of rule can be used to compare sampled values, average values, or changes in values to a threshold that administrators supply. The TOE can use comparative performance data to initiate standard responses, such as running a script or batch file, issuing an SNMP trap, notifying a specified notification group, or updating state variables
- *Alert processing rules* – this type of rule differs in purpose from event and performance processing rules. Event and performance processing rules act on events or threshold data. Alert rules process the alerts that event and performance processing rules generate, including generating SMTP messages, SNMP messages, and running administrator-defined scripts. Alert processing rules define the real-time response the TOE takes when another rule issues a specified level of alert

2.2 TOE Architecture

NetIQ Security Manager and IT environment components are depicted below.

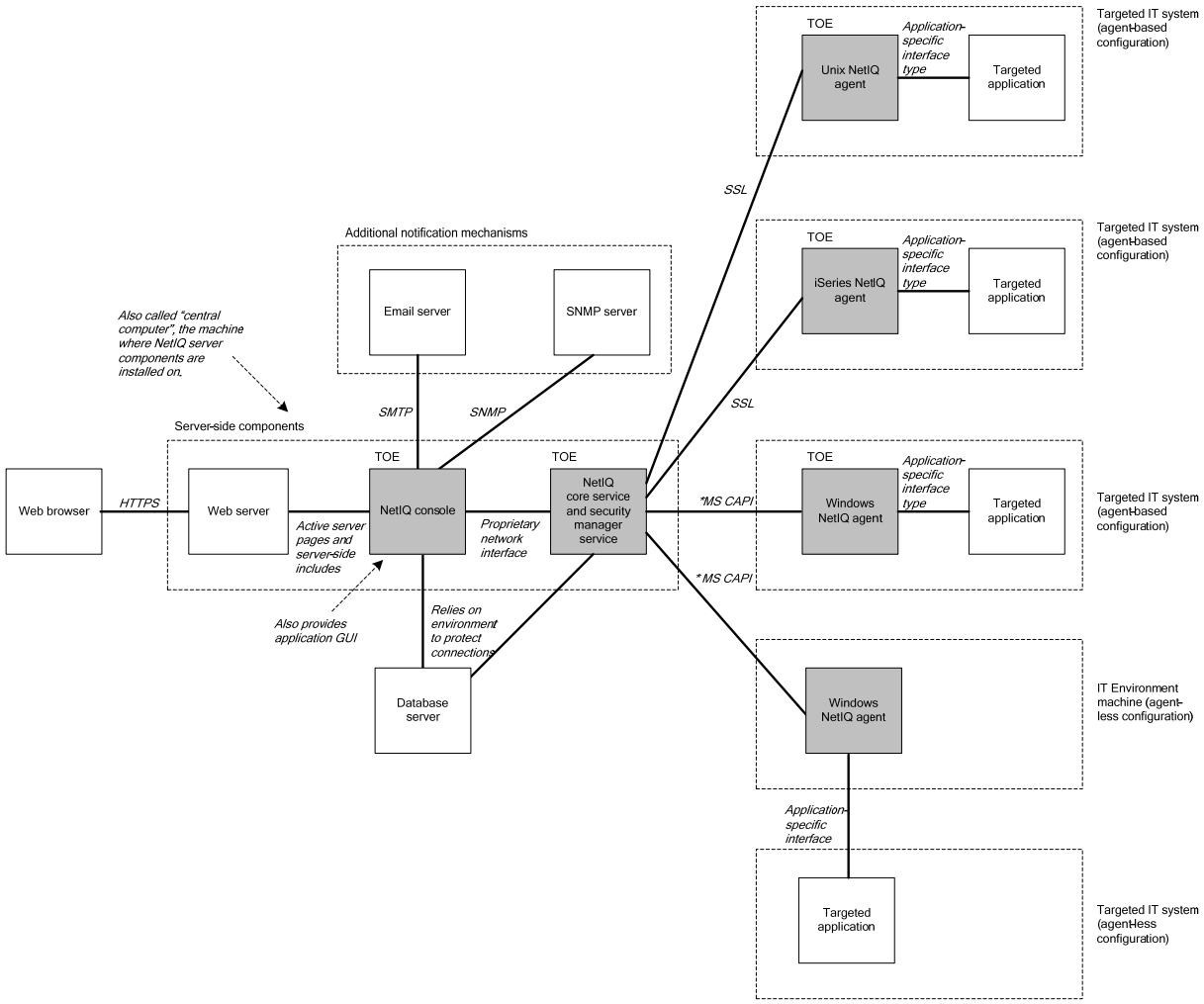

Figure 2: NetIQ Security Manager and IT environment components[1]

The NetIQ Security Manager *central computer* applications receive data from NetIQ Security Manager *agent* applications in an agent-based configuration or retrieves event data from targeted IT systems itself. NetIQ Security Manager agents (including agents running in what is called a proxy agent mode) collect real-time and log data. NetIQ Security Manager central computer provides correlation services by applying correlation rules to received data, and generating responses when rule matches occur. NetIQ Security Manager central computer also performs trend analysis by gathering data from monitored log databases to construct and store data for trend analysis reporting. NetIQ Security Manager agent applications send collected event data to the NetIQ Security Manager central computer. NetIQ Security Manager central computer stores configuration data and data collected from targeted IT systems in a database in the IT environment.

The NetIQ Security Manager *console* application allows administrators to view and manage collected event data and generated alerts and manage TOE functions. The console provides interfaces that can be used by administrators to

[1] Note in Figure 2 that SSL is used to protect communication between the central computer and the UNIX and iSeries agents, while alternate protection, labeled *MS CAPI, is used in conjunction with Windows agents. In the case of MS CAPI, the cryptographic APIs available in Windows are used to authenticate both ends of the connection and to encrypt the traffic as summarized later in this document.

monitor alerts about real-time events. The console component provides a web console function to monitor alerts about real-time events and view summary reports of archival log data using a web browser. The console provides analysis functions to create and evaluate summary, forensic analysis, and trend analysis reports. The console provides a development environment to customize processing rules, computer groups, and other manager subcomponents. The NetIQ Security Manager console application includes the following components: Monitor Console, Incident Management Console, Development Console, Configuration snap-in, Analysis Console, Web Console. These console components are described further in section 6.1.2 (“Security Management”).

2.2.1 Physical Boundaries

The components that make up the TOE are:

- NetIQ Security Manager central computer applications
- NetIQ Security Manager agent applications
- NetIQ Security Manager console applications

The machine that the NetIQ server components is installed on is referred to as the “central computer”.

The NetIQ Security Manager central computer, NetIQ Security Manager console (and agents configured to support agentless-configurations) run on the following platforms:

- Windows 2003 Server SP1

The NetIQ Security Manager central computer and NetIQ Security Manager console store collected event data and configuration information in the following database servers:

- Microsoft SQL Server 2000

The NetIQ Security Manager central computer and NetIQ Security Manager console rely on the following to provide secured web-based interfaces:

- Microsoft Internet Information Server 5.0

The NetIQ Security Manager central computer and NetIQ Security Manager console can generate send alert messages using the following notification mechanisms:

- SNMP compatible management server
- SMTP compatible email server

The NetIQ Security Manager console web-based interface can be accessed using:

- Microsoft Internet Explorer 6.0

2.2.1.1 Supported Targeted IT Systems

Note that while the TOE is designed to support many more products, only the following are those that were subject to testing due to practical limitations on the evaluation.

- Firewalls
    - Checkpoint NG-R55
    - Cisco Secure Pix Firewall (Cisco PIX (OS) version 6.3)
- Intrusion Detection Systems
    - Cisco IDS 4.1 running on Cisco IDS 4210 appliance
- Antivirus applications
    - Symantec Antivirus Corporate Edition 9.x
- Routers and Switches
    - Cisco Internet Operating System (IOS) versions 12.2 to 12.3

- Operating Systems
  - Red Hat Linux Advance Server 3.0 (10.21.121.243)
  - Windows Server 2003 SP1 and Professional SP2
  - IBM iSeries running OS/400 v5 Release 2
  - Sun Solaris 9

2.2.2 Logical Boundaries

The TSF provides the following security functions:

- Identification and authentication
- Security management
- Protection of the TSF
- Intrusion detection and event correlation

2.2.2.1 Identification and authentication

Users of targeted IT systems do not log into the TOE. The NetIQ Security Manager console application provides user interfaces that administrators may use to manage TOE functions. The NetIQ Security Manager console application does not identify and authenticate individual administrators. The operating system and the database in the IT Environment are relied on to individually identify and authenticate administrators. The TOE maintains authorization information that determines which TOE functions an authenticated administrator that possesses a given role may perform.

2.2.2.2 Security management

The NetIQ Security Manager console application provides user interfaces that administrators may use to manage TOE functions. The TOE recognizes the following *operating system* groups, which each correspond to TOE roles:

- OnePointOp Reporting
- OnePointOp Users
- OnePointOp Operators
- OnePointOp ConfgAdms

The TOE recognizes the following *database* groups:

- EeaDasLocator
- EeaReportViewer
- VigilEntUserAccess

The database groups do not correspond to TOE roles given that the user must also be a member of the OnePointOp groups for the set of TOE functions that require that the user be a member of any additional database groups, as described in section 6.1.2 (“Security Management”).

User accounts in the OnePointOp Reporting group have permission to use the Log Manager Analysis Console. Reporting users typically use the Analysis Console to run Forensic Analysis reports, Summary reports, and view Trend Analysis.

User accounts in the OnePointOp Users group have permission to views in the Monitor Console. These users can monitor the information that Security Manager collects.

User accounts in the OnePointOp Operators group have all the permissions of the OnePointOp Users group. In addition, operators can modify the information that Security Manager collects and what the product does with the collected information. Operators typically use the Monitor Console and Development Console.

User accounts in the OnePointOp ConfgAdms group have all the permissions of the OnePointOp Operators group. In addition, users in the ConfgAdms group can also modify the list of computers where Security Manager installs agents (the Managed Computers list), as well as configure settings in the Configuration Wizard. Security Manager configuration administrators typically use the Monitor Console, Development Console Configuration snap-ins, Configuration Wizard, and Deployment Wizard.

Monitor Console, Incident Management Console, Development Console, Configuration snap-in, Analysis Console, and Web Console NetIQ Security Manager console application components are described further in section 6.1.2 (“Security Management”).

2.2.2.3 Protection of the TSF

The NetIQ Security Manager console checks that administrators have been authenticated by the IT environment before allowing access to its interfaces. The TOE relies on the operating system in the environment to protect its application components and to provide a secure runtime environment. The TOE relies on SSL (for UNIX and iSeries agents) and available Microsoft Windows Cryptographic APIs (MS CAPI) (for Windows agents) provided by the environment to authenticate the end points and to protect communication between Security Manager central computer and agent components. The TOE also relies on the environment to provide HTTPS to protect communication between Security Manager console and the web browser.

2.2.2.4 Intrusion detection and event correlation

The TOE can detect changes to both targeted IT system resource operation as well as configuration changes. Collected data from all targeted IT system resources is correlated by the TOE and interfaces are provided to authorized administrators to perform analysis of the correlated data. When the TOE collects data from agents that are located on targeted IT system resources, the console component passes the collected data into the following datastreams (work flows):

- Real-time datastreams
- Correlation datastreams
- Log management datastreams
- Reporting and trend analysis datastreams

Datastream processing is described further in section 6.1.4 (“Intrusion detection and event correlation”).

2.3 TOE Documentation

NetIQ offers a series of documents that describe the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features. Refer to Section 6 for information about these and other documentation associated with the TOE.

3. Security Environment

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL 2) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1 Assumptions

3.1.1 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.

3.1.2 Physical Assumptions

A.LOCATE	The server components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.1.3 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.

3.2 Threats

3.2.1 Threats to the TOE

T.ADMIN_ERROR	An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.MASQUERADE	An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.
T.TSF_COMPROMISE	A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).

3.2.2 Threats to the IT System the TOE Monitors

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

T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors.

4. Security Objectives

4.1 Security Objectives for the TOE

O.ADMIN_ROLE	The TOE will define authorizations that determine the actions authorized administrator roles may perform.
O.IDANLZ	The TOE must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.IDSCAN	The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
O.IDSENS	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.
O.MANAGE	The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.
O.OFLOWS	The TOE must appropriately handle potential System data storage overflows.
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.TOE_PROTECTION	The TOE will protect itself and its assets from external interference or tampering.

4.2 Security Objectives for the Environment

OE.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.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
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.
OE.INTROP	The TOE is interoperable with the IT System it monitors.

4.3 Security Objectives for the IT Environment

OE.ADMIN_ROLE	The IT Environment will provide authorized administrator roles to isolate administrative actions.

OE.USER_AUTHENTICATION	The IT Environment will verify the claimed identity of users.
OE.USER_IDENTIFICATION	The IT Environment will uniquely identify users.
OE.TIME	The IT environment will provide a time source that provides reliable time stamps.
OE.TOE_PROTECTION	The IT environment will protect the TOE and its assets from external interference or tampering.

Application Note: OE.TOE_PROTECTION is intended to address the TOE in execution on its host as well as communication between distributed TOE components.

5. IT Security Requirements

This section defines the security functional requirements for the TOE as well as the security assurance requirements against which the TOE has been evaluated. All of the requirements have been copied from version 2.3 of the applicable Common Criteria documents, with the exception of the explicitly stated Security Functional Requirements.

5.1 TOE Security Functional Requirements

Requirement Class	Requirement Component
FIA: Identification and Authentication	FIA_ATD.1a: User Attribute Definition
FMT: Security management	FMT_MOF.1a: Management of security functions behavior
	FMT_MOF.1b: Management of security functions behavior
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1a: Security roles
FPT: Protection of the TOE security functions	FPT_RVM.1a: Non-bypassability of the TSP
IDC: Intrusion detection and event correlation	IDC_COL1(EX): Data Collection
	IDC_STG.2(EX): Data Loss Prevention
	IDC_COR.1(EX): Data Correlation
	IDC_ALR.1(EX): Data Alarms
	IDC_ADM.1(EX): Data Review

Table 1 Security Functional Components

5.1.1 Identification and authentication (FIA)

5.1.1.1 User attribute definition (FIA_ATD.1a)

FIA_ATD.1a.1 The TSF shall maintain the following list of security attributes belonging to individual ~~users~~ **roles**: **[authorizations]**.

5.1.2 Security management (FMT)

5.1.2.1 Management of security functions behavior (FMT_MOF.1a)

FMT_MOF.1a.1 The TSF shall restrict the ability to [***modify the behavior of***] the functions **[**

a.) **Data collection**
b.) **Data correlation**
c.) **Data alarms]**

to **[OnePointOp Operators, OnePointOp ConfigAdms]**.

Application note: The central computer component restricts access as above..

5.1.2.2 Management of security functions behavior (FMT_MOF.1b)

FMT_MOF.1b.1 The TSF shall restrict the ability to [***modify the behavior of***] the functions **[**

a.) **Data collection**
b.) **Data correlation**
c.) **Data alarms]**

to **[Administrators]**.

Application note: The Unix agent restricts access as above..

5.1.2.3 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to **[*query*]** the **[collected data and generated reports]** to **[OnePointOp Reporting, OnePointOp Users, OnePointOp Operators, OnePointOp ConfigAdms]**.

5.1.2.4 Specification of Management Functions (FMT_SMF.1)

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

a.) **Modify the behavior of data collection**
b.) **Modify the behavior of data correlation**
c.) **Modify the behavior of data alarms**
d.) **Query collected data and generated reports]**

5.1.2.5 Security roles (FMT_SMR.1)

FMT_SMR.1a.1 The TSF shall maintain the roles **[**

a.) **Windows: OnePointOp Reporting**
b.) **Windows: OnePointOp Users**
c.) **Windows: OnePointOp Operators**
d.) **Windows: OnePointOp ConfigAdms**
e.) **Unix: Administrators**]

FMT_SMR.1a.2 The TSF shall be able to associate users with roles.

Application note: Although the environment maintains role information, the TOE recognizes these roles and enforces the constraints.

5.1.3 Protection of the TOE security functions (FPT)

5.1.3.1 Non-bypassability of the TSP (FPT_RVM.1a)

FPT_RVM.1a.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 Intrusion detection and event correlation (IDC)

5.1.4.1 Data Collection (IDC_COL1(EX))

IDC_COL.1.1 The TSF shall collect the following information from the targeted IT System resource(s):

a.) Security mechanism operation; and
b.) Security mechanism configuration changes. (EX)

IDC_COL.1.2 At a minimum, the System shall collect and record date and time of the event, type of event, and subject identity. (EX)

5.1.4.2 Data Loss Prevention (IDC_STG.2(EX))

IDC_STG.2.1 The TSF shall ignore System data and send an alarm if the storage capacity has been reached. (EX)

5.1.4.3 Data Correlation (IDC_COR.1(EX))

IDC_COR.1.1 The TSF performs event correlation on all IDS data received. (EX)

5.1.4.4 Data Alarms (IDC_ALR.1(EX))

IDC_ALR.1.1 The TSF shall generate an alarm using one or more of the following notification mechanisms:

a.) Display alarm information to the administrator console
b.) Send alarm information to administrators using email
c.) Send alarm information to administrators using SNMP
d.) Execute a command
e.) Execute a script

in response to one or more of the following rule types:

a.) Event rules
b.) Filtering (database and conditional filters only) rules
c.) Missing event rules
d.) Alert rules
e.) Performance measuring rules
f.) Threshold rules (EX)

Application note: Scripts and commands can be used to support notification mechanisms for which there is no built-in support.

5.1.4.5 Data Review (IDC_ADM.1(EX))

IDC_ADM.1.1 The TSF shall provide authorized users with the capability to read collected data and generated reports. (EX)

IDC_ ADM.1.2 The TSF shall provide collected data and generated reports in a manner suitable for the user to interpret the information. (EX)

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs that are to be satisfied by the IT environment in which the TOE operates.

Requirement Class	Requirement Component
FIA: Identification and authentication	FIA_ATD.1b: User Attribute Definition
	FIA_UAU.2: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security management **FPT: Protection of the TSF**	FMT_SMR.1b: Security roles
	FPT_ITT.1a: Basic internal TSF data transfer protection
	FPT_ITT.1b: Basic internal TSF data transfer protection
	FPT_RVM.1b: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation
	FPT_STM.1: Reliable time stamps

Table 2 IT Environment Security Functional Components

5.2.1 Identification and authentication (FIA)

5.2.1.1 User attribute definition (FIA_ATD.1b)

FIA_ATD.1b.1 The ~~TSF~~ **IT Environment** shall maintain the following list of security attributes belonging to individual users: **[user identity, authentication data, group]**.

5.2.1.2 User authentication before any action (FIA_UAU.2)

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.

5.2.1.3 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The ~~TSF~~ **IT Environment** shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.2 Security management (FMT)

5.2.2.1 Security roles (FMT_SMR.1b)

FMT_SMR.1b.1 The ~~TSF~~ **IT Environment** shall maintain the roles **[**

a.) **Windows: OnePointOp Reporting**
b.) **Windows: OnePointOp Users**
c.) **Windows: OnePointOp Operators**
d.) **Windows: OnePointOp ConfigAdms**
e.) **Unix: Administrators**]

FMT_SMR.1b.2 The ~~TSF~~ **IT Environment** shall be able to associate users with roles.

Application note: Operating system and database groups that map to the above-listed roles are described in section 2.2.2.2 ("Security Management").

5.2.3 Protection of the TSF (FPT)

5.2.3.1 Basic internal TSF data transfer protection (FPT_ITT.1a)

FPT_ITT.1a.1 The ~~TSF~~ **IT Environment** shall protect TSF data from [***disclosure, modification***] when it is transmitted between separate parts of the TOE.

Application note: SSL is used to protect communication between TOE central computer and agent components.

5.2.3.2 Basic internal TSF data transfer protection (FPT_ITT.1b)

FPT_ITT.1b.1 The ~~TSF~~ **IT Environment** shall protect TSF data from [***disclosure, modification***] when it is transmitted between separate parts of the TOE **and IT Environment**.

Application note: HTTPS is used to protect communication between TOE console and IT Environment web browser components.

5.2.3.3 Non-bypassability of the TSP (FPT_RVM.1b)

FPT_RVM.1b.1 The ~~TSF~~ **IT Environment** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.2.3.4 TSF domain separation (FPT_SEP.1)

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

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

5.2.3.5 Reliable Time Stamps (FPT_STM.1)

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

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 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
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 3 EAL 2 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 that comprise the TOE.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
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

Users of targeted IT systems do not log into the TOE. The NetIQ Security Manager console application provides user interfaces that administrators may use to manage TOE functions. The NetIQ Security Manager console application does not identify and authenticate individual administrators. The NetIQ Security Manager console when an administrator attempts to access its interfaces first checks to see if the user has been authenticated by the operating system or the database in the IT Environment.

If the user has been successfully identified and authenticated by the environment, and if the user has been successfully identified and authenticated as a member of an operating system and database group that the TOE recognizes, the NetIQ Security Manager console provides access to its interfaces according to authorization data. Authorization data maintained by the TOE for each role that the TOE recognizes is used to determine the functions that a user possessing a given role (i.e. membership in an operating system and/or database group) may perform.

The TOE recognizes the following operating system groups, which each correspond to TOE roles:

- OnePointOp Reporting
- OnePointOp Users
- OnePointOp Operators

- OnePointOp ConfgAdms

The TOE recognizes the following database groups:

- EeaDasLocator
- EeaReportViewer
- VigilEntUserAccess

Operating system and database groups are described further in section 2.2.2.2 (“Security Management”).

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

- FIA_ATD.1a: The TOE maintains authorization information that determines which TOE functions a role may perform.

6.1.2 Security Management

The NetIQ Security Manager console application includes the following components:

- Monitor Console
- Incident Management Console
- Development Console
- Configuration snap-in
- Analysis Console
- Web Console

To use the Monitor Console, the authorized administrator operating system account must be a member of the OnePointOp Users group. The authorized administrator account must also be a member of the EeaDasLocator role in the database. Some tasks within the Monitor Console require membership in other OnePointOp groups. The Monitor Console allows authorized administrators to monitor real-time events and alerts for a configuration group. A configuration group has one database server storing information for a group of monitored computers or devices. The Monitor Console also allows authorized administrators to configure Security Manager settings for a configuration group. The Monitor Console uses Microsoft Management Console (MMC) technology and contains snap-ins, basic components of MMC. Authorized administrators can save MMC consoles as files with the .MSC extension. When authorized administrators save a console, its configuration settings are also saved. Authorized administrators can mail a console file to another user, who can open it on a different computer or on a different network, and the saved settings are retained for all the console items. Creating custom consoles allows for reducing training costs by enabling you to send security personnel interfaces tailored to their needs.

To use the Incident Management Console, the authorized administrator operating system account must be a member of the OnePointOp Users group. The authorized administrator account must also be a member of the EeaDasLocator role in the database. The Incident Management Console allows authorized administrators to monitor alerts about real-time events across multiple configuration groups.

To use the Development Console, the authorized administrator operating system account must be a member of the OnePointOp Operators group. The authorized administrator account must also be a member of the EeaDasLocator role in the database. The Development Console is available as an MMC. Authorized administrators can launch the Development Console in its own interface, or can add the Development Console as a snap-in to the Monitor Console while in author mode. The Development Console displays Windows computer groups, processing rulegroups, notification groups, and advanced rule functionality for one configuration group. Authorized administrators can create or modify computer groups and processing rules using the Development Console. Authorized administrators can create or modify computer attributes, which authorized administrators can use when creating Windows computer groups. Authorized administrators can also create or modify notification groups, scripts, and data providers, which can be used when creating processing rules.

To use the Configuration snap-in, the authorized administrator operating system account must be a member of the OnePointOp ConfgAdms group. The authorized administrator account must also be a member of the EeaDasLocator

role in the database. The Configuration snap-in allows authorized administrators to manage Windows agents and NetIQ Security Manager settings within a single configuration group. Authorized administrators can view and modify global configuration group settings, as well as configure settings for individual NetIQ Security Managers or agents. Authorized administrator can also add operators to a notification group. If authorized administrators want to manage components for several configuration groups, authorized administrators can add other Configuration snap-ins to the Monitor Console. The Configuration snap-in also allows authorized administrators to view and approve Windows agents before they are automatically installed on computers within the configuration group. The Configuration snap-in also allows authorized administrators to view and disapprove Windows agents before they are automatically uninstalled from computers within the configuration group.

To use the Analysis Console, the authorized administrator operating system account must be a member of the OnePointOp Reporting group. The authorized administrator account must also be a member of the following roles database roles:

- the EeaDasLocator,
- the EeaReportViewer
- the VigilEntUserAccess.

The Analysis Console allows authorized administrators to create, view, and print reports of data collected from computers, servers, devices, routers, and switches in the monitored enterprise. The Analysis Console allows authorized administrators to work with reports for one configuration group. Authorized administrators can change the configuration group for an Analysis Console.

To use the Web Console, the authorized administrator operating system account must be a member of the OnePointOp Users group. The authorized administrator account must also be a member of the EeaDasLocator role in the database. The Web Console provides remote monitoring and easy access for authorized administrators. The Web Console allows authorized administrators to view real-time data and Summary reports using any Windows platform that supports Microsoft Internet Explorer.

The Unix version of the NetIQ Security Manager agent components additionally includes a component called Unix Manager. Unix Manager provides interfaces that administrators can use to configure rules for Unix agents. Access to Unix Manager is restricted to users possessing administrative access to the machine that Unix Manager is installed on. Unix Manager may be installed on the same machine as a Unix agent, or it may be installed on a separate machine. There are Unix and Windows versions of Unix Manager.

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

- FMT_MOF.1a, b: The TOE restricts the ability to manage IDC settings to authorized administrators.
- FMT_MTD.1: The TOE restricts the ability to query collected data and generated reports to authorized users.
- FMT_SMF.1: The TOE provides authorized administrators with the ability to manage IDC settings and review collected data and correlation reports.
- FMT_SMR.1a: The TOE provides access to its interfaces according to authorization data maintained by the TOE for each role that the TOE recognizes.

6.1.3 Protection of the TSF

The NetIQ Security Manager console checks that administrators have been authenticated by the IT environment before allowing access to its interfaces. The NetIQ Security Manager console allows authenticated administrators access to its interfaces according to authorizations corresponding to the set of operating system and database roles that NetIQ Security Manager console recognizes. The application-based console interfaces perform this check when they are invoked using operating system interfaces. The web-based console interfaces perform this check after an HTTPS connection has been established using a web browser in the environment. The TOE relies on the operating system in the environment to protect its application components and to provide a secure runtime environment.

The TOE uses SSL (for UNIX and iSeries agents) and Microsoft Cryptographic APIs (MS CAPI) (for Windows agents), each provided by the IT environment, to ensure authentication of the endpoints and to protect

communication between Security Manager central computer and agent components. In the case of SSL, 256-bit keys are generated using SHA1PRNG in the IT environment and they are distributed during initialization so that subsequent SSL communication is both authenticated and encrypted (using AES). The keys are stored in a trusted database as well as in the installation directory of each agent where they are configured to limit access to root users. Note that a root certificate is manually installed on each TOE component during installation. In the case of MS CAPI, the TOE uses 1024-bit keys generated using MS CAPI and RSA provided by MS CAPI for mutual authentication. It also uses functions available via MS CAPI to ensure bi-directional encryption of the traffic using 40-bit keys padded to 56-bits. All the keys are generated, stored, and destroyed within the underlying operating system.

The TOE also relies on the web server in the environment to provide HTTPS to protect communication between Security Manager console and the web browser. The TOE relies on the database in the environment to protect collected event data and TOE configuration data.

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

- FPT_RVM.1a: The TOE requires that users are authenticated by the IT environment and that they are members of operating system and database groups that are recognized by the TOE, before access to TOE interfaces is allowed.

6.1.4 Intrusion detection and event correlation

The TOE provides the ability to monitor the security mechanisms of targeted IT system resources which can include intrusion detection systems, as well as operating systems, firewalls, and antivirus applications. The TOE can detect changes to both targeted IT system resource operation as well as configuration changes. Collected data from all targeted IT system resources is correlated by the TOE and interfaces are provided to authorized administrators to perform analysis of the correlated data. Authorized administrators also have the ability to configure alarms using event processing rules. When the TOE collects data from agents that are located on targeted IT system resources, the console component passes the collected data into the what are called real-time, correlation, log management, and reporting and trend analysis “datastreams” or work flows.

Real-time datastream processing starts when events occur on targeted IT system resources, when agents evaluate rules that are defined by, and administered using, the TOE. When a rule match occurs, the agent generates an alert and sends it to the NetIQ Security Manager, along with the events that triggered the alert. If the rule specifies to notify an authorized administrator, NetIQ Security Manager delivers alarm using the configured notification mechanism. NetIQ Security Manager stores alert and event data to the real-time database on the database server. NetIQ Security Manager console polls for updated information from NetIQ Security Manager by monitoring changes to the database. NetIQ Security Manager initially displays an alert; authorized administrators can then perform further analysis of the alert.

Correlation datastream processing starts when NetIQ Security Manager applies event correlation rules to collected data from targeted IT system resource(s). NetIQ Security Manager evaluates collected alerts and events against correlation rules as data arrives. When a rule match occurs, NetIQ Security Manager responds as the rule defines and sends the source events and resultant alerts to the database server. Authorized administrators can define event correlation rules to evaluate events received from the real-time datastream from Windows or Unix agents. To create event correlation rules, authorized administrators run the Correlation Wizard, which is an interface to the console component. The Correlation Wizard lets authorized administrators select multiple alerts and then define a relationship and time frame. Correlation rules can amplify the importance of alerts, suppress less important alerts, and alert authorized administrators to seemingly unrelated activities that may indicate a threat.

Log management datastream processing starts when NetIQ Security Manager normalizes event data collected from targeted IT system resource(s) and sends the normalized data to the database for storage. The console component is configured by default to retain log data in the database for 90 days. However, if the database reaches storage capacity, any new collected event data that is presented by agents to the NetIQ Security Manager is ignored and a warning is displayed in the NetIQ Security Manager console’s Monitor Console. When log data is older than the retention period, NetIQ Security Manager deletes the oldest data to free space for newer data. Authorized administrators can configure the log database retention period using interactive GUI interfaces to the console component. Log management datastream processing also includes NetIQ Security Manager periodically summarizing the collected data and assembling dimension information for trend analysis reports.

Reporting and trend analysis processing starts when NetIQ Security Manager finishes summarizing data. Dimension data is then loaded and and summary data is retrieved from the database. The trend analysis data cube is then updated, accumulating the day's summarized data with historical summary data. When processing is complete, authorized administrators can view the trend analysis report graphs using GUI interfaces to the console component. When the summary reports are complete, authorized administrators can also view these reports from GUI interfaces to the console component. Summary reports total the events by source to provide a snapshots of events, such as event count by date over a range of dates. The console component can be used by authorized administrators to configure which summary reports to publish and make available. For more information about alarms and reporting, see the security management description above.

When an event or threshold occurs that matches a processing rule, NetIQ Security Manager associates the specified alert and alert severity to that event and displays the alert in the NetIQ Security Manager console's Monitor Console, Incident Management Console, and Web Console. Alert severity allows administrators monitoring alerts to quickly determine the importance of the indicated condition. Alert severities are defined when the processing rules are created. Possible alert severities are defined as follows:

- Service Unavailable – Identifies alerts generated for missed agent heartbeats and other events indicating that an application or service is unavailable to its users.
- Security Breach – Identifies an alert that indicates a security compromise has occurred. Systems on the network are at risk.
- Critical Error – Identifies an alert that indicates a serious problem needing attention immediately.
- Error – Identifies an alert that is important and needs attention soon.
- Warning – Identifies an alert that might indicate future problems or lower priority issues requiring research.
- Information – Identifies an alert that simply provides information.
- Success – Identifies an alert that indicates a successful event or operation.

Using processing rules, administrators can also define real-time responses to a detected condition. The following processing rule types allow administrators to define responses for a processing rule match:

- Event rules
- Filtering (database and conditional filters only) rules
- Missing event rules
- Alert rules
- Performance measuring rules
- Threshold rules

Administrators can define the following responses within processing rules:

- Display alarm information to the administrator console
- Send alarm information to administrators using email
- Send alarm information to administrators using SNMP
- Execute a command
- Execute a script

Scripts and commands can be used to support notification mechanisms for which there is no built-in support.

The Intrusion detection and event correlation function is designed to satisfy the following security functional requirements:

- IDC_COL.1(EX): The TOE collects targeted IT system resource operation and configuration information from agents that are installed on the targeted IT system resource.

- IDC_STG.2 (EX): The TOE generates alarms using a configured notification mechanism when storage capacity for collected System data has been reached.
- IDC_COR.1(EX): The TOE correlates event data collected from targeted IT system resources for use in subsequent analysis by authorized administrators.
- IDC_ALR.1(EX): The TOE generates alarms that notify authorized administrators using the console, using email, using SMTP, and/or executing a command in a configured script. Note that alarms are generated in response to administratively-configured processing rules.
- IDC_ADM.1(EX): The TOE provides authorized administrators with the ability to interactively analyze collected data and generated reports using the GUI of the console component.

6.2 TOE Security Assurance Measures

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

- Configuration Management;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

6.2.1 Configuration Management

The configuration management measures applied by NetIQ ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, vulnerability analysis documentation, and configuration management documentation.

These activities are documented in:

- NetIQ Configuration Management Manual

The Configuration management assurance measure satisfies the following EAL 2 assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and Guidance

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

- NetIQ Delivery and Operation Procedures
- NetIQ Installation Guide

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

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

The Design Documentation provided for NetIQ Security Manager is provided in two documents:

- NetIQ IDS Functional Specification

- NetIQ IDS High-level Design

These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

The Development assurance measure satisfies the following EAL 2 assurance requirements:

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

6.2.4 Guidance documents

NetIQ provides guidance on how to properly utilize the TOE security functions, including function descriptions, warnings, effects, assumptions, etc. The installation and generation procedures, included in the administrator guidance, describe the steps necessary to install NetIQ IDS products in accordance with the evaluated configuration. Note that there are no conventional “users” of NetIQ products. All users of the TOE must belong to one or more of the OnePointOp Security Manager Groups and are classified either as administrators (System Admin or Configuration Admin) or users (Operator, Reporting User and User). As such, all applicable guidance for “administrator” and “users” is embodied in a single guide:

- User Guide, Security Manager, November 19, 2004
- Evaluation Guide, Security Manager, November 19, 2004
- Installation Guide, Security Manager, November 19, 2004
- Programming Guide, Security Manager, November 19, 2004

The Guidance documents assurance measure satisfies the following EAL 2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Tests

The Test Documentation is found in the following documents:

- NetIQ IDS Test Coverage
- NetIQ IDS Test Plan
- NetIQ IDS Test Procedures

NetIQ has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. NetIQ has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

The Tests assurance measure satisfies the following EAL 2 assurance requirements:

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

6.2.6 Vulnerability Assessment

The TOE administrator and user guidance documents describe the operation of NetIQ Security Manager and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements

outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references

There are no strength of function claims associated with the NetIQ Security Manager TOE. Therefore, there is no strength of function analysis document

NetIQ performed a vulnerability analysis of the TOE to identify weaknesses that can be exploited in the TOE. The vulnerability analysis is documented in:

- NetIQ IDS Vulnerability Assessment

The Vulnerability assessment assurance measure satisfies the following EAL 2 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

There are no Protection Profile claims.

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;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

		O.ADMIN_ROLE	O.IDANLZ	O.IDSCAN	O.IDSENS	O.MANAGE	O.OFLOWS	O.RESPON	O.TOE_PROTECTION	OE.ADMIN_ROLE	OE.USER_AUTHENTICATION	OE.USER_IDENTIFICATION	OE.TIME	OE.TOE_PROTECTION
Threats to the TOE	**T.ADMIN_ERROR**					x								
	T.MASQERADE	x								x	x	x		
	T.TSF_COMPROMISE								x					x
Threats to the IT System the TOE monitors	**T.FALACT**							x						
	T.FALASC		x											
	T.FALREC		x											
	T.INADVE				x									
	T.INFLUX						x							
	T.MISACT				x									
	T.MISUSE				x									
	T.SCNCFG			x										
	T.SCNMLC			x										
	T.SCNVUL			x										

Table 4 Environment to Objective Correspondence

8.1.1.1 T.ADMIN_ERROR

An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

This Threat is countered by ensuring that:

- O.MANAGE: The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

8.1.1.2 T.MASQUERADE

An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.

This Threat is countered by ensuring that:

- O.ADMIN_ROLE: The TOE will define authorizations that determine the actions authorized administrator roles may perform.
- OE.ADMIN_ROLE: The IT Environment will provide authorized administrator roles to isolate administrative actions.
- OE.USER_AUTHENTICATION: The IT Environment will verify the claimed identity of users.
- OE.USER_IDENTIFICATION: The IT Environment will uniquely identify users.

8.1.1.3 T.TSF_COMPROMISE

A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).

This Threat is countered by ensuring that:

- O.TOE_PROTECTION: The TOE will protect itself and its assets from external interference or tampering.
- OE.TOE_PROTECTION: The IT environment will protect the TOE and its assets from external interference or tampering.

8.1.1.4 T. FALACT

The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity

This Threat is countered by ensuring that:

- O.RESPON: The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity
- OE.TIME: The IT environment will provide a time source that provides reliable time stamps.

8.1.1.5 T. FALASC

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

This Threat is countered by ensuring that:

- The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
- OE.TIME: The IT environment will provide a time source that provides reliable time stamps.

8.1.1.6 T. FALREC

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

This Threat is countered ensuring that:

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

8.1.1.7 T. INADVE

Inadvertent activity and access may occur on an IT System the TOE monitors. T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors

This Threat is countered by ensuring that:

- O.IDSENS: The O.IDSENS objective address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data

8.1.1.8 T. INFLUX

An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle

This Threat is countered by ensuring that:

- O.OFLOWS: The TOE will appropriately handle potential System data storage overflows.

8.1.1.9 T. MISACT

Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

This Threat is countered by ensuring that:

- O.IDSENS: The O.IDSENS objective address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data

8.1.1.10 T. MISUSE

Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors

This Threat is countered by ensuring that:

- O.IDSENS: The O.IDSENS objective address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data

8.1.1.11 T. SCNCFG

Improper security configuration settings may exist in the IT System the TOE monitors

This Threat is countered by ensuring that:

- O.IDSCAN: The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change. The ST will state whether this threat must be addressed by a Scanner.

8.1.1.12 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

This Threat is countered by ensuring that:

- O.IDSCAN: The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change. The ST will state whether this threat must be addressed by a Scanner.

8.1.1.13 T. SCNVUL

Vulnerabilities may exist in the IT System the TOE monitors

This Threat is countered by ensuring that:

- O.IDSCAN: The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change. The ST will state whether this threat must be addressed by a Scanner.

8.1.2 Security Objectives Rationale for Environment Assumptions

This section provides evidence demonstrating coverage of the Non-IT security objectives by the environmental assumptions. The following table shows this assumption to objective mapping.

		OE.INSTALL	OE.CREDEN	OE.PERSON	OE.PHYCAL	OE.INTROP
Intended usage assumptions	**A.ACCESS**					x
	A.ASCOPE					x
	A.DYNMIC			x		x
Physical assumptions	**A.LOCATE**				x	
Personnel assumptions	**A.MANAGE**			x		
	A.NOEVIL	x	x			

Table 5: Complete coverage – environmental assumptions

8.1.1.1 A.ACCESS

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

This Assumption is satisfied by ensuring that:

- OE.INTROP: The OE.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.

This Assumption is satisfied by ensuring that:

- OE.INTROP: The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

8.1.1.3 A.DYNIMC

The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors data collected and produced by the TOE shall be protected from modification.

This Assumption is satisfied by ensuring that:

- OE.INTROP: The OE.INTROP objective ensures the TOE has the proper access to the IT System.
- OE.PERSON: The OE.PERSON objective ensures that the TOE will managed appropriately.

8.1.1.4 A.LOCATE

The server components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

This Assumption is satisfied by ensuring that:

- OE.PHYCAL: The OE.PHYCAL provides for the physical protection of the TOE.

8.1.1.5 A.MANAGE

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

This Assumption is satisfied by ensuring that:

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

8.1.1.6 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.

This Assumption is satisfied by ensuring that:

- OE.INSTALL: The OE.INSTAL objective ensures that the TOE is properly installed and operated.
- OE.CREDEN: The OE.CREDEN objective supports this assumption by requiring protection of all authentication data

8.2 Security Requirements Rationale

This section demonstrates how there is at least one functional component for each objective (and how all SFRs map to one or more objectives) by a discussion of the coverage for each objective.

	O.ADMIN_ROLE	O.IDANLZ	O.IDSCAN	O.IDSENS	O.MANAGE	O.OFLOWS	O.RESPON	O.TOE_PROTECTION	OE.ADMIN_ROLE	OE.USER_AUTHENTICATION	OE.USER_IDENTIFICATION	OE.TIME	OE.TOE_PROTECTION
FIA_ATD.1a	x												
FIA_ATD.1b									x		x		

	O.ADMIN_ROLE	O.IDANLZ	O.IDSCAN	O.IDSENS	O.MANAGE	O.OFLOWS	O.RESPON	O.TOE_PROTECTION	OE.ADMIN_ROLE	OE.USER_AUTHENTICATION	OE.USER_IDENTIFICATION	OE.TIME	OE.TOE_PROTECTION
FIA_UAU.2										x			
FIA_UID.2											x		
FMT_MOF.1a					x								
FMT_MOF.1b					x								
FMT_MTD.1					x								
FMT_SMF.1					x								
FMT_SMR.1a	x												
FMT_SMR.1b									x				
FPT_ITT.1a													x
FPT_ITT.1b													x
FPT_RVM.1a								x					
FPT_RVM.1b													x
FPT_SEP.1													x
FPT_STM.1												x	
IDC_ADM.1(EX)					x								
IDC_ALR.1(EX)							x						
IDC_COL.1(EX)			x	x									
IDC_COR.1(EX)		x											
IDC_STG.2(EX)						x							

Table 6 Objective to Requirement Correspondence

8.2.1.1 O.ADMIN_ROLE

T*he TOE will define authorizations that determine the actions authorized administrator roles may perform.*

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1a: The TOE maintains authorization information that determines which TOE functions a role may perform.
- FMT_SMR.1a: The TOE provides access to its interfaces according to authorization data maintained by the TOE for each role that the TOE recognizes.

8.2.1.2 O. IDANLZ

The TOE must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future)

This TOE Security Objective is satisfied by ensuring that:

- IDC_COR.1(EX): The TOE correlates event data collected from targeted IT system resources for use in subsequent analysis by authorized administrators.

8.2.1.3 O. IDSCAN

The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System

This TOE Security Objective is satisfied by ensuring that:

- IDC_COL.1(EX): The TOE collects targeted IT system resource operation and configuration information from agents that are installed on the targeted IT system resource.

8.2.1.4 O. IDSENS

The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS

This TOE Security Objective is satisfied by ensuring that:

- IDC_COL.1(EX): The TOE collects targeted IT system resource operation and configuration information from agents that are installed on the targeted IT system resource.

8.2.1.5 O.MANAGE

The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MOF.1a, b: The TOE restricts the ability to manage IDC settings to authorized administrators.
- FMT_MTD.1: The TOE restricts the ability to query collected data and generated reports to authorized users.
- FMT_SMF.1: The TOE provides authorized administrators with the ability to manage IDC settings and review collected data and correlation reports.
- IDC_ADM.1(EX): The TOE provides authorized administrators with the ability to interactively analyze collected data and generated reports using the GUI of the console component.

8.2.1.6 O. OFLOWS

The TOE must appropriately handle potential System data storage overflows

This TOE Security Objective is satisfied by ensuring that:

- IDC_STG.2 (EX): The TOE generates alarms using a configured notification mechanism when storage capacity for collected System data has been reached.

8.2.1.7 O. RESPON

The TOE must respond appropriately to analytical conclusions

This TOE Security Objective is satisfied by ensuring that:

- IDC_ALR.1(EX): The TOE generates alarms that notify authorized administrators using the console, using email, using SMTP, and/or executing a command in a configured script. Note that alarms are generated in response to administratively-configured processing rules.

8.2.1.8 O.TOE_PROTECTION

The TOE will protect itself and its assets from external interference or tampering.

This TOE Security Objective is satisfied by ensuring that:

- FPT_RVM.1a: The TOE requires that users are authenticated by the IT environment and that they are members of operating system and database groups that are recognized by the TOE, before access to TOE interfaces is allowed.

8.2.1.9 OE.ADMIN_ROLE

The IT Environment will provide authorized administrator roles to isolate administrative actions.

This IT Environment Security Objective is satisfied by ensuring that:

- FIA_ATD.1b: The IT environment maintains user identification, authentication data, and groups (which the TOE maps to roles).
- FMT_SMR.1b: The IT Environment provides roles that correspond to operating system user groups and database roles. Any user account that is assigned in the IT environment to one or more system-defined operating system user groups and database roles is considered an “authorized administrator”.

8.2.1.10 OE.USER_AUTHENTICATION

The IT Environment will verify the claimed identity of users.

This IT Environment Security Objective is satisfied by ensuring that:

- FIA_UAU.2: The IT environment authenticates individual users as members of system-defined operating system user groups and/or database roles.

8.2.1.11 OE.USER_IDENTIFICATION

The IT Environment will uniquely identify users.

This IT Environment Security Objective is satisfied by ensuring that:

- FIA_ATD.1b: The IT environment maintains user identification, authentication data, and groups (which the TOE maps to roles).
- FIA_UID.2: The IT environment identifies individual users.

8.2.1.12 OE. TIME

The IT environment will provide a time source that provides reliable time stamps.

This IT Environment Security Objective is satisfied by ensuring that:

- FPT_STM.1: The IT environment provides reliable time stamps to the TOE.

8.2.1.13 OE.TOE_PROTECTION

The IT environment will protect the TOE and its assets from external interference or tampering.

This IT Environment Security Objective is satisfied by ensuring that:

- FPT_ITT.1a: SSL provided by the IT environment is used to protect communication between central computer and agent components.
- FPT_ITT.1b: HTTPS provided by the web server in the IT Environment is used to protect communication between TOE console and IT Environment web browser components.
- FPT_RVM.1b: The IT Environment is relied on to ensure that TOE interfaces cannot be bypassed.
- FPT_SEP.1: The IT Environment is relied on to provide a secure domain.

8.3 Security Assurance Requirements Rationale

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

8.4 Strength of Functions Rationale

The overall strength of function claim of SOF-basic is believed to be commensurate with the overall assurance claim of EAL 2. The only applicable security function is Security Management where passwords are used by Unix agent administrators as evidence of their claimed identities. The intent is that the password mechanism meets or exceeds SOF-basic and the evidence can be found in the strength of function analysis included in NetIQ Vulnerability Analysis.

8.5 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satsified and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ST Requirement	CC Dependencies	ST Dependencies
FIA_ATD.1a	none	none
FIA_ATD.1b	none	none
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1a	FIA_UID.1	FIA_UID.2
FMT_SMR.1b	FIA_UID.1	FIA_UID.2
FPT_ITT.1a	none	none
FPT_ITT.1b	none	none
FPT_RVM.1a	none	none
FPT_RVM.1b	none	none
FPT_SEP.1	none	none
FPT_STM.1	none	none
IDC_ADM.1(EX)	none	none
IDC_ALR.1(EX)	none	none
IDC_COL.1(EX)	FPT_STM.1	FPT_STM.1
IDC_COR.1(EX)	none	none
IDC_STG.2(EX)	none	none
ACM_CAP.2	none	none
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ATE_COV.1	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_FUN.1	none	none

ST Requirement	CC Dependencies	ST Dependencies
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.1
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1

Table 7: Requirement Dependencies

8.6 Explicitly Stated Requirements Rationale

A family of IDC requirements was created to specifically address the data collected and analysed by an IDS. 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 IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions, with the exception of time stamps provided by the IT environment to support event correlation.

8.7 TOE Summary Specification Rationale

Each subsection in the TSS 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. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of 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. **Table 8 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Identification and authentication	**Security management**	**Protection of the TSF**	**Intrusion detection**
FIA_ATD.1a	x			
FMT_MOF.1a		x		
FMT_MOF.1b		x		
FMT_MTD.1		x		
FMT_SMF.1		x		
FMT_SMR.1a		x		
FPT_RVM.1a			x	
IDC_ADM.1(EX)				x
IDC_ALR.1(EX)				x
IDC_COL.1(EX)				x
IDC_COR.1(EX)				x
IDC_STG.2(EX)				x

Table 8 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.