ForeScout ActiveScout / CounterACT
Security Target

Version 2.4

26 June 2005

REF: ST

PREPARED FOR:

ForeScout Technologies, Inc.
10001 N. De Anza Blvd.
Cupertino, CA 95014

DOCUMENT CONTROL

DOCUMENT HISTORY

Version	Date	Description
0.1	July, 2003	initial version
0.3	14 February, 2004	addressing EORs
1.4	15 July, 2004	addressing EORs
1.5	9 August, 2004	addressing EOR_INT 8/8/04 ; EOR_DES – 8 Aug 2004
1.6	12 September, 2004	addressing EOR_OBJ 9/5/04 ; EOR_ENV – 5 Sep 2004
1.7	1 January, 2005	major reorganization, including addressing EOR_ASE_REQ-05 – 5 Dec 2004
1.8	4 February 2005	addressing ETR Version 0.3 – dated 25 January 2005
1.9	8 March 2005	Minor changes to functional requirements
2.0	17 March 2005	Minor changes in response to evaluator comments
2.1	8 April 2005	Minor changes in response to validator comments
2.2	4 May 2005	Addition of iterations of FMT_MSA.3 and FDP_ACF.1 to the IT Environment in order to meet dependencies for FDP_ACC.1 iteration in the IT Environment
2.3	24 May 2005	Moved FPT_ITT.1 and FPT_ITT.3 to the IT Environment.
2.4	26 June 2005	Update based on validator comments.

TABLE OF CONTENTS

TABLES

REFERENCES

Evaluation Documentation

AGD	ForeScout Administrator and User Guidance
ATE	ForeScout Test Plan
ATE-EVIDENCE	ForeScout Test Evidence
CFM	ForeScout Configuration Management
DEL-IGS	ForeScout Secure Delivery, Installation, Generation and Startup
FSP	ForeScout Functional Specification
HLD	ForeScout High Level Design
RCR	ForeScout Representation Correspondence
ST	ForeScout Security Target
VLA-SOF	ForeScout Vulnerability Assessment and Strength of Functions Analysis

TOE Documentation

AS-SM-UM	ForeScout ActiveScout Site Manager User Manual
AS-INST-GUIDE	ForeScout Active Scout Installation Guide

Third-Party Documentation

VSS-GS	Getting Started with Visual SourceSafe http://msdn.microsoft.com/library/default.asp?url=/library/en-us/guides/html/vstskgetting_started.asp
VSS-UG	Using Visual SourceSafe http://msdn.microsoft.com/library/default.asp?url=/library/en-us/guides/html/vstskusing_vss.asp

Common Criteria Documentation

CC-PART-2	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, Revision 256, January 2004.
CC-PART-3	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, Revision 256, January 2004
CEM	Common Criteria for Information Technology Security Evaluation Common Evaluation Method, Version 2.2, Revision 256, January 2004

GLOSSARY AND ABBREVIATIONS

GLOSSARY AND TERMS

This section gives definition of some of the TOE-specific terminology used in this document.

Scout Flow Control Policy	The policy which specifies the traffic that is to be allowed to flow unimpeded to the protected network and, in contrast, which traffic that is to be intercepted and handled in accordance with the TOE's protective features.
Scout Management Policy	The policy which specifies the TOE management privileges assigned to each of the TOE administrators.
IT Environment Access Control Policy	The policy implemented by the Linux (Red-Hat 7.2-based) Operating System, which restricts IT environment-level privileges to install, delete and modify TOE components, including TOE data, to authorized administrators.

ABBREVIATIONS

The following Common Criteria-related abbreviations are used in this document:

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification

1 SECURITY TARGET INTRODUCTION

1.1 OVERVIEW

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

The TOE is ForeScout ActiveScout / CounterACT , an IDP (Intrusion Detection and Prevention) software product that protects networks at a single external access point from network-borne threats. The TOE identifies impending attacks against the protected network by identifying the reconnaissance activities (e.g., network probing) that precede them, and then neutralizes the attacks by blocking them before they penetrate the protected network.

1.2 ST IDENTIFICATION

Title:	ForeScout ActiveScout / CounterACT Security Target
ST Version:	2.4
ST Date:	26 June 2005
ST Author:	Standards Institution of Israel
TOE:	ForeScout ActiveScout Version 3.0.5/ CounterACT Version 4.1.0
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004, CCIMB-2004-01-002.
EAL:	Assurance claims conform to EAL2 from Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004.
Protection Profile:	No Protection Profile compliance is claimed.
Keywords:	Network, hacker, attack, Intrusion Prevention, Scout, Site Manager, Mark, ForeScout, Scout Flow Policy.

1.3 CONFORMANCE CLAIMS

The TOE is conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, January 2004, CCIMB-2004-01-002.
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, January 2004, CCIMB-2004-01-002.

1.4 DOCUMENT ORGANIZATION

Section 2	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 its 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 its environment.
Section 5	IT Security Requirements	This section presents the security functional requirements (SFR) for the TOE and IT environment that supports the TOE, and details the requirements for EAL 2.
Section 6	TOE Summary Specification	This section describes the security functions represented in the TOE that satisfy the security requirements.
Section 7	Protection Profile Claims	This section states the conformance of this ST to specific Protection Profile.
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.

1.5 CONVENTIONS, TERMINOLOGY, ACRONYMS

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 …").

Other sections of the Security Target – Other sections of the Security Target use bolding to highlight text of special interest, such as captions.

2 TOE DESCRIPTION

2.1 OVERVIEW

This section provides information regarding the TOE, by identifying the product type, and describing the evaluated configuration, the functionality and the boundaries.

2.2 TOE DESCRIPTION

The TOE is ForeScout ActiveScout / CounterACT , an IDP (Intrusion Detection and Prevention) software product that protects networks at a single external access point from network-borne threats. The TOE identifies impending attacks against the protected network by identifying the reconnaissance activities (e.g., network probing) that precede them, and then neutralizes the attacks by blocking them before they penetrate the protected network.

2.2.1 TOE COMPONENTS

The TOE consists of two components:

- a "Scout" component that monitors traffic to the network;
- a management component by which administrators manage the TOE, define policies, review audit logs, *etc.*

The first component can be either:

- ForeScout ActiveScout Scout, or
- ForeScout CounterACT Scout,

which are different configurations of the same product. Both have the same capabilities, share the same code base, and can be considered essentially identical for the purpose of this evaluation.

The second component can be either:

- ForeScout ActiveScout Site Manager (which is used to manage ForeScout ActiveScout Scout), or
- ForeScout CounterACT Site Manager (which is used to manage ForeScout CounterACT),

which are different configurations of the same product. Both have the same capabilities, share the same code base, and can be considered essentially identical for the purpose of this evaluation.

In the remainder of this document:

- references to "Scout" should be understood as referring to both ForeScout ActiveScout Scout and ForeScout CounterACT Scout, and
- references to "Manager" should be understood as referring to both ForeScout ActiveScout Site Manager and ForeScout CounterACT Site Manager.

2.2.2 SCOUT

Scout is positioned outside the firewall and monitors Internet traffic for signs of pre-attack activity. Scout is responsible for accurately identifying potential attackers, marking them as potential threats, and implementing a blocking policy that prevents the attackers from infiltrating the network. Scout identifies potential attackers by recognizing reconnaissance techniques that precede the attack itself, on the basis of known scanning methods.

Scout assumes that reconnaissance activities ("scans") must be launched against a network prior to an attack, in order to gather information available network services and resources. Scout identifies these reconnaissance activities, replies with false information (a "mark"), and implements a pre-defined policy that can block any subsequent activity that includes this mark.

Scout identifies a scan request from an external network based upon concrete scan type and a minimum number of occurrences of scan events from the same source (threshold). The threshold enables Scout to define the level of sensitivity and to minimize false negative scenarios.

Additionally, the implemented policy allows Scout to block events, to monitor them, or to pass them through to the firewall.

The block/monitor status is limited to a pre-defined amount of time, which can expire if no other scan request is encountered.

Scout is also responsible for: administrator identification and authentication, assigning user privileges, managing security aspects of the product, auditing, logging and Scout protection.

2.2.3 MANAGER

Manager is a Java-based application that enables an administrator to locally and remotely configure and administer Scout, view Scout monitoring and generate reports. Residing on any point of the network, Manager also presents a visual overview of Scout's threat prevention activity, including a geographical representation of potential attackers and the preventive steps taken against them.

Operational activities performed by Manager are policy definition and update, user definition and management data and audit log presentations.

Manager enables the administrator to define the Scout Flow Control Policy. Scout allows transferring of requests from an untrusted network to the internal trusted network ruled by the Scout Flow Control Policy. The policy is attacker-based, not request based, and the blocking mechanism is applied to IP address previously identified as potential attacker or attacker. The administrator can also manually modify an attacker state.

As defined by the policy, Scout can block a specific IP for a specified period of time, forward the pass/no pass decision to the firewall, or stop blocking.

Scout is positioned (see Figure 1 below) between the router and the firewall and is able to monitor all traffic passing from the Internet. The Administrative Console is located in the internal protected network.

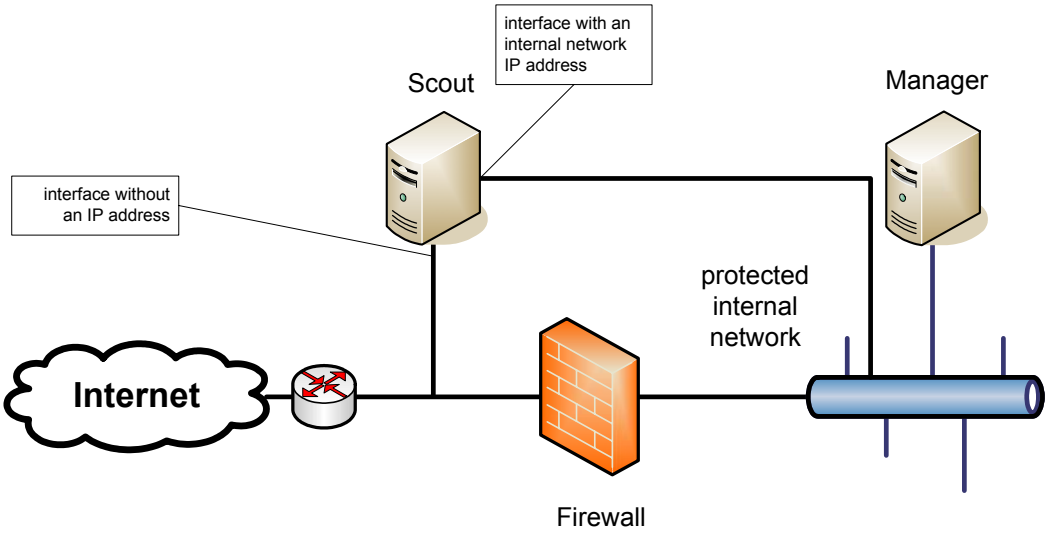
2.3 SCOPE OF EVALUATION

This section provides a general description of the physical and logical scope and boundaries of the TOE.

2.3.1 EVALUATED CONFIGURATION

The evaluated configuration is illustrated in Figure 1.

Figure 1 Evaluated Configuration



The evaluated configuration consists of two machines (meeting the requirements specified in "TOE System Requirements" below). One of the machines runs Scout and the other runs Manager.

The Scout machine, which monitors traffic entering the protected network, is located between the firewall and the router. The Scout machine has 2 interfaces:

- an interface with no IP address facing the Internet
- an interface with an IP address facing the internal (protected) network

The Manager machine is located inside the protected network.

The Manager and Scout communicate via SSL. The TOE consists of only the Scout and Manager software; the platforms (machines) and their operating systems are not included in the TOE.

2.3.2 Physical Boundary

The physical boundary of the TOE includes both Scout and Manager. The hardware and operating systems that both applications run on is outside the scope of this evaluation.

2.3.3 Logical Boundary

The logical boundary is defined by the external interfaces at which the Security Functions are implemented. The Security Functions are:

- **Security Audit** – the TOE generates audit information for security-relevant events and enables authorized administrators to view the audit records.
- **Identification and Authentication** – the TOE allows only users who have been successfully identified and authenticated (authorized administrators) to access security-relevant functionality, including viewing audit records.
- **Security Management** – the TOE enables authorized administrators to define policies in which the parameters affecting the attack identification process and the response are specified, as well as defining other administrators and system-wide parameters.

- **Attack Detection and Prevention** – the TOE protects networks from attack by responding with false information and then blocking the attack and thus rendering it harmless.

See "TOE Security Functions" on page 33 for a detailed description of the Security Functions.

2.3.4 Hardware Requirements

The hardware on which the TOE runs is outside the scope of the evaluation. See "TOE System Requirements" below.

2.4 TOE System Requirements

2.4.1 Deliverables

The deliverable package of the TOE includes a single CD with the following:

- A hardened version of Linux (Red-Hat 7.2-based) Operating System (which is not part of the TOE)
- Product documentation
- Scout executable and files
- Manager executable and files

2.4.2 Configuration

In the evaluated configuration, Scout and manager are installed on two machines.

Note – The Linux OS is not part of the TOE.

2.4.3 Scout System Requirements

- A dedicated machine with a Pentium III 600 MHz processor or higher
- 512MB RAM
- 20GB free space on the hard drive
- CD drive
- OS – The OS (Linux) is installed together with the TOE (see "Deliverables" above).

Note – The TOE will be tested only on the Linux platform.

2.4.4 Manager System Requirements

- A non-dedicated machine with a Pentium III 600 MHz processor or higher, running Windows 98/NT/2000, Linux or Sun Solaris.
- 256MB RAM
- 120MB free space on the hard drive
- CD drive

3 SECURITY ENVIRONMENT

This section describes the security aspects of the environment in which the TOE should be used and the manner in which it is expected that the TOE will be used. These include:

- threats that the TOE is designed to counter
- organizational security policies with which the TOE is designed to comply
- assumptions about the operational environment and the TOE's intended method of use

3.1 THREATS

This paragraph describes all the threats to the assets against which the TOE or its environment is required to counter.

T.UA-ACCESS An unauthorized user may gain access to or modify TOE data stored in the TOE database.

T.UA-ACTION An authorized user may exceed his or her privileges and perform unauthorized modifications of TOE data which go undetected. For example, the user may:

- modify the Scout Flow Control Policy for a Scout for which the user is not authorized to do so, or
- modify details of a Scout Flow Control Policy which the user is not allowed to modify.

T.UA-TRANSIT An unauthorized user may gain access to or modify TOE data when it is in transit between distributed parts of the TOE.

T.ATTACK An attacker may gain access to the protected network via the unprotected network (Internet) to which the protected network is connected, using any of a variety of well-known attack methods, and gain access to and/or modify user data.

T.DISABLE An attacker may disable the TOE or modify its behavior and thus expose the protected network to attack.

3.2 ORGANIZATIONAL SECURITY POLICIES

P.MANAGE IT Systems are protected from unauthorized access and modification.

3.3 ASSUMPTIONS

A.ADMIN The administrators assigned to manage the TOE are competent, properly trained, not careless, not willfully negligent, not hostile, follow the guidance and instruction provided in the TOE documentation, and install and administer the TOE in a manner consistent with organizational policies.

A.LOCATE The TOE components are located in a physically secured area, protected from unauthorized physical access.

A.BANDW	The volume of incoming traffic monitored by the TOE does not exceed the volume specified in TOE administrator guidance documentation.
A.TIME	The operating environment provides a reliable time stamp for use by the TOE.

4 SECURITY OBJECTIVES

This section describes the security objectives, which – taken together – counter the threats, while complying with the organizational security policies and remaining consistent with the assumptions, as listed in the previous section.

4.1 SECURITY OBJECTIVES FOR THE TOE

O.MANAGE The TOE must provide the functionality that enables an authorized administrator to configure the TOE, define and enforce TOE security policies (for example, the Scout Flow Control Policy), and monitor the TOE's activities.

O.AUTH The TOE must ensure that only authorized administrators are able to access the TOE and its data by uniquely identifying and authenticating all users attempting to access the TOE and its data.

O.AUDIT-MGM The TOE must generate audit records of all security-related actions of TOE users to ensure that these actions can be traced to the users who performed them.

O.AUDIT-RVW The TOE must provide the capability to review audit records.

O.DETECT The TOE must detect attempted attacks and protect the protected network from these attacks.

O.AUDIT-ATK The TOE must generate audit records of detected attack attempts.

O.ALERT The TOE must have the capability to respond to specified events by alerting administrators.

4.2 SECURITY OBJECTIVES FOR THE IT ENVIRONMENT

O.E.TRANSIT The IT environment must have the ability to protect TSF data in transit between distributed parts of the TOE.

O.E.TOE-PRT The IT environment must protect the TOE data from unauthorized deletion or modification.

O.E.TIME The IT environment must provide a reliable time-stamp for the TOE to be used for audit records.

4.3 SECURITY OBJECTIVES FOR THE NON–IT ENVIRONMENT

O.E.ADMIN Authorized TOE administrators must be properly trained in all aspects of TOE and TOE resource administration, and must be neither negligent nor hostile.

O.E.BACKUP The TOE, its data and the systems on which it runs will be restored to a secure state after failure by following the relevant backup and restore procedures.

O.E.LOCATE The TOE components must be located in a physically secured area, protected from unauthorized physical access.

O.E.INSTALL	The TOE and its associated hardware and software environment must be installed, maintained and managed in a manner that complies with the TOE security objectives.
O.E.BANDW	The volume of incoming traffic monitored by the TOE is not permitted to exceed the volume specified in TOE administrator guidance documentation.

5 IT SECURITY REQUIREMENTS

This section contains the security requirements that are provided by the TOE and the IT environment. These requirements consist of security functional and assurance components for the TOE derived from Part 2 and 3 of the CC.

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

This section describes the Security Functional Requirements that are satisfied by the TOE.

Table 1. TOE Security Functional Requirement Components

Security Functional Class	Security Functional Requirement	Description
Security Audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_STG.1	Protected audit trail storage
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.2	Complete information flow policy
	FDP_IFF.1	Simple security attributes
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles

5.1.1 FAU_ARP.1 – Security Alarms

FAU_ARP.1 The TSF shall take [assignment: *send an alert to alert destination as defined by the Scout Manager*] upon detection of a potential security violation.

5.1.2 FAU_GEN.1 – Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

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

b) All auditable events for the [selection; *basic*] level of audit, and

c) [assignment: *additional auditable events described in Table 2 below*].

Table 2. FAU_GEN Auditable Events

Component	Event	Details
FAU_ARP.1	potential security violation	date and time of the event, severity, IP source, IP destination
FAU_GEN.1	start-up and shutdown of audit functions	
FIA_UAU.2A	all use of the authentication mechanism	user identity, location, method
FIA_UID.2A	all use of the user identification mechanism	user identity , location, method
FMT_MOF.1	all modifications in the behavior of the functions of the TSF	
FMT_MTD.1	modifications to the values of TSF data	
FMT_SMR.1A	modification to the group of users that are part of a role	user identity
FMT_MSA.1A	all modifications of the values of security attributes	
FMT_MSA.3A	modifications of the default setting of permissive or restrictive rules all modifications of the initial values of security attributes	
FDP_IFF.1	all decisions on requests for information flow	

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [assignment*: no other information*].

5.1.3 FAU_GEN.2 – User Identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.4 FAU_SAA.1 – Potential Violation Analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [assignment:

correlation analysis to known source IP address, presence of mark in packet] known to indicate a potential security violation;

b) [assignment: *no other rules*].

5.1.5 FAU_SAR.1– Audit Review

FAU_SAR.1.1 The TSF shall provide [assignment: *administrators*] with the capability to read [assignment: *all auditable events*] from the audit records.

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

5.1.6 FAU_SAR.2 – Restricted Audit Review

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

5.1.7 FAU_STG.1– Protected Audit Trail Storage

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

FAU_STG.1.2 The TSF shall be able to [selection: prevent] modifications to the audit records in the audit trail.

5.1.8 FDP_ACC.1a – Subset Access Control

FDP_ACC.1.1a The TSF shall enforce the [assignment: *Scout Management Policy*] *on* [assignment: *administrators*].

5.1.9 FDP_ACF.1a – Security Attribute Based Access Control

FDP_ACF.1.1a The TSF shall enforce the [assignment: *Scout Management Policy]* to objects based on the following: [assignment:

subject: administrators

- *Scout identity with associated privileges*

object: Scout

- *Scout Flow Control Policy].*

FDP_ACF.1.2a The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *Access is granted on requested operations based on privileges granted for the Scout.*].

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

FDP_ACF.1.4a The TSF shall explicitly deny access of subjects to objects based on the [assignment: *no explicit rules*].

5.1.10 FDP_IFC.2 – Complete Information Flow Policy

FDP_IFC.2.1 The TSF shall enforce the [assignment: *Scout Flow Control Policy*] on [assignment: (*client hosts*) *and the* (*traffic monitored by the TOE)*] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

5.1.11 FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [assignment: *Scout Flow Control Policy*] based on the following types of subject and information security attributes: [assignment:

a) IP address of source subject

b) IP address of destination subject

c) state

d) time to expire.]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled ~~subject~~ **source** and controlled ~~information~~ **target** via a controlled operation if the following rules hold: [assignment:

a) "monitor" state is specified in the source table for this sender.

b) "block" state is specified in the source table, and Time To Expire parameter equal 0.

c) No occurrence with the actual IP address does exist at the source table.]

FDP_IFF.1.3 The TSF shall enforce the [assignment: *no additional information flow rules*].

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

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

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

5.1.12 FIA_UAU.2A – User Authentication Before Any Action

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

5.1.13 FIA_UID.2A – User Identification Before Any Action

FIA_UID.2.1a The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.14 FMT_MOF.1 – Management of Security Function Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *modify the behavior of*] the functions [assignment:

a) start-up and shutdown of the enforcement of the Scout Flow Control Policy;

b) create, delete, modify, and view information flow security policy rules that permit or deny information flow;

] to [assignment: *administrator*].

5.1.15 FMT_MTD.1 – Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *query*, *modify*] the [assignment: *source table data*] to the [assignment: *administrator*].

5.1.16 FMT_MSA.1A – Management of Security Attributes

FMT_MSA.1.1a The TSF shall enforce the [assignment: *Scout Management Policy*] to restrict the ability to [*change_default*] the security attributes:

[assignment:

a) address of source subject

b) address of destination subject

c) state

d) time to expire

e) create, delete, modify, and view administrator attribute values.]

to [assignment: *administrator*].

5.1.17 FMT_MSA.3A – Static Attribute Initialization

FMT_MSA.3.1a The TSF shall enforce the [assignment: *Scout Management Policy*] to provide [selection: *restrictive* [assignment: *no other properties*]] default values for security attributes that are used to enforce the SFP.

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

5.1.18 FMT_SMF.1A – Specification of Management Functions

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

a) management of audit data,

b) management of TSF policy

].

5.1.19 FMT_SMR.1A – Security Roles

FMT_SMR.1.1a The TSF shall maintain the roles [assignment: *administrator*].

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

5.2 Security Requirements for the IT Environment

This section lists the Security Functional Requirements that are satisfied by the IT Environment.

5.2.1 FPT_STM.1 – Reliable Time Stamps

FPT_STM.1.1 The ~~TSF~~ **IT environment** shall be able to provide reliable time stamps for ~~its own~~ use **by the TSF**.

5.2.2 FDP_ACC.1B – Subset Access Control

FDP_ACC.1.1b The ~~TSF~~ **IT Environment** shall enforce the [assignment: *IT Environment Access Control Policy*] *on* [assignment: subjects: *OS authorized users including OS administrator and TOE administrator roles; objects: TOE data; operations: TOE data modification, and deletion*].

5.2.3 FDP_ACF.1B – Security Attribute Based Access Control

FDP_ACF.1.1b The ~~TSF~~ **IT Environment** shall enforce the [assignment: *IT Environment Access Control Policy]* to objects based on the following: [assignment: *subjects: OS authorized users including OS administrators and TOE administrators; objects: TOE data; operations: modification and deletion of TOE data is limited to TOE administrators*]

FDP_ACF.1.2b The ~~TSF~~ **IT Environment** shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *Access is granted on requested operations based on privileges granted by the OS*.].

FDP_ACF.1.3b The ~~TSF~~ **IT Environment** shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *no explicit rules*].

FDP_ACF.1.4b The ~~TSF~~ **IT Environment** shall explicitly deny access of subjects to objects based on the [assignment: *no explicit rules*].

5.2.4 FIA_UAU.2B – User Authentication Before Any Action

FIA_UAU.2.1b The ~~TSF~~ **IT Environment** shall require each user to be successfully authenticated before allowing any other **IT Environment** ~~T~~SF-mediated actions on behalf of that user.

5.2.5 FIA_UID.2B – User Identification Before Any Action

FIA_UID.2.1b The ~~TSF~~ **IT Environment** shall require each user to identify itself before allowing any other **IT Environment** ~~T~~SF-mediated actions on behalf of that user.

5.2.6 FMT_MSA.1B – Management of Security Attributes

FMT_MSA.1.1b The ~~TSF~~ **IT Environment** shall enforce the [assignment: *IT Environment Access Control Policy*] to restrict the ability to [selection: *modify, delete*] the security attributes:

[assignment:

OS attributes associated with delete, modify permissions on TOE Data]

to [assignment: TOE *administrator*].

5.2.7 FMT_MSA.3B – Static Attribute Initialization

FMT_MSA.3.1b The ~~TSF~~ **IT Environment** shall enforce the [assignment: *IT Environment Access Control Policy*] to provide [selection: *restrictive* [assignment: *no other properties*]] default values for security attributes that are used to enforce the **IT Environment** SFP.

FMT_MSA.3.2b The ~~TSF~~ **IT Environment** shall allow the [assignment: *OS administrator*] to specify alternative initial values to override the default values when an object or information is created.

5.2.8 FMT_SMF.1B – Specification of Management Functions

FMT_SMF.1.1b The ~~TSF~~ **IT Environment** shall be capable of performing the following security management functions: [assignment:

a) specification of access controls on TOE data files that allow modification and deletion of data only by the TOE administrator.

].

5.2.9 FMT_SMR.1B – Security Roles

FMT_SMR.1.1b The ~~TSF~~ **IT Environment** shall maintain the roles [assignment: *TOE administrator; OS administrator*].

FMT_SMR.1.2b The ~~TSF~~ **IT Environment** shall be able to associate users with roles.

5.2.10 FPT_ITT.1 – Basic Internal TSF Data Protection

FPT_ITT.1.1 The ~~TSF~~ **IT Environment** shall protect TSF data from [selection: *disclosure and modification*] when it is transmitted between separate parts of the TOE.

5.2.11 FPT_ITT.3 – TSF Data Integrity Monitoring

FPT_ITT.3.1 The ~~TSF~~ **IT Environment** shall be able to detect [selection: *modification of data*] for TSF data transmitted between separate parts of the TOE.

FPT_ITT.3.2 Upon detection of a data integrity error, the ~~TSF~~ **IT Environment** shall take the following actions [assignment: *no action*].

5.3 TOE SECURITY ASSURANCE REQUIREMENTS

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

Table 3. TOE Security Assurance Requirement Components

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.2 Configuration Items
Delivery and Operation (ADO)	ADO_IGS.1 Installation, Generation, and Start-up Procedures
	ADO_DEL.1 Delivery Procedures
Development (ADV)	ADV_FSP.1 Informal Functional Specification
	ADV_HLD.1 Descriptive High Level Design
	ADV_RCR.1 Informal Correspondence Demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator Guidance
	AGD_USR.1 User Guidance
Tests (ATE)	ATE_IND.2 Independent Testing - Sample
	ATE_COV.1 Evidence of Coverage
	ATE_FUN.1 Functional Testing
Vulnerability assessment (AVA)	AVA_SOF.1 Strength of the TOE Security Function Evaluation
	AVA_VLA.1 Developer Vulnerability Analysis

5.3.1 ACM_CAP.2 - CONFIGURATION ITEMS

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 labeled 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 ADO_DEL.1 – Delivery Procedures

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.

5.3.3 ADO_IGS.1 – Installation, Generation, and Start-up Procedures

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.

5.3.4 ADV_FSP.1 – Informal Functional Specification

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.

5.3.5 ADV_HLD.1 – Descriptive High-Level Design

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.

5.3.6 ADV_RCR.1 – Informal Correspondence Demonstration

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.

5.3.7 AGD_ADM.1 – Administrator Guidance

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 behavior 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.

5.3.8 AGD_USR.1 – User Guidance

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 behavior found in the statement of the 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.

5.3.9 ATE_COV.1 – Evidence of Coverage

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.

5.3.10 ATE_FUN.1 – Functional Testing

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.

5.3.11 ATE_IND.2 – Independent Testing – Sample

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.

5.3.12 AVA_SOF.1 – Strength of the TOE Security Function Evaluation

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

AVA_SOF.1.1c For each mechanism with a strength of the TOE security function claim the strength of the 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 the TOE security function claim the strength of the 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.

5.3.13 AVA_VLA.1 – Developer Vulnerability Analysis

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.

5.4 Strength of Function Claim

In addition to these requirements, the TOE satisfies a minimum strength of function "SOF-basic."

The applicable (that is, probabilistic or permutational) Security Functional Requirements are:

FIA_UAU.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2 The TSF requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6 TOE SUMMARY SPECIFICATION

This chapter describes the Security Functions implemented by the TOE to address the Security Functional Requirements claimed by the TOE (see "TOE Security Functional Requirements" on page 20).

The mapping of the TOE Security Functions to the Security Functional Requirements is summarized in below.

6.1 TOE SECURITY FUNCTIONS

The TOE Security Functions are:

- **Security Audit** – the TOE generates audit information for security-relevant events and enables authorized administrators to view the audit records.
- **Identification and Authentication** – the TOE allows only users who have been successfully identified and authenticated (authorized administrators) to access security-relevant functionality, including viewing audit records.
- **Security Management** – the TOE enables authorized administrators to define policies in which the parameters affecting the attack identification process and the response are specified, as well as defining other administrators and system-wide parameters.
- **Attack detection and Prevention** – the TOE protects networks from attack by responding with false information and then blocking the attack and thus rendering it harmless.

6.1.1 SECURITY AUDIT

The TOE generates audit records for the following events:

- start-up and shutdown of the audit function
- modifications to the policy enforcement function
- modifications to the TOE data

Each audit record includes the date and time as obtained from the IT environment (OS), user identity (when applicable), type of event, and its outcome (success or failure).

The audit records can be viewed by authorized administrators. It is possible to filter the view according to various parameters.

In addition, certain events (as specified in the TSP), can trigger alerts, which are sent to Manager for immediate attention.

The Security Audit function satisfies the following Security Functional Requirements:

FAU_GEN.1	The TSF generates an audit record of the auditable events as listed in Table 2 (page 21).
FAU_GEN.2	The TSF records sufficient information within each audit record to fully describe the event and identify the user who initiated the event.
FAU_SAR.1	The TSF provides the administrator with the capability to read the audit records and shall present the audit records in a manner suitable for the administrator to interpret the records.

FAU_SAR.2	The TSF allows only authorized administrators access to the audit records.
FAU_STG.1	The TSF protects stored audit data from deletion and detects modifications to the audit data.

6.1.2 Identification and Authentication (I&A)

The TOE maintains a list of user accounts and data about these accounts: name, credential data, and a list of privileges. The TOE identifies and authenticates users (based on user name and password) before allowing them to assume the administrative role defined by their privileges. No user may perform any administrative functions unless the identification and authentication are successful.

The Identification and Authentication (I&A) function satisfies the following Security Functional Requirements:

FIA_UAU.2A	The TSF requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_UID.2A	The TSF requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3 Security Management

Administrators define policies in which the parameters affecting the attack identification process and the response are specified, as well as defining other administrators and system-wide parameters.

The Security Management function satisfies the following Security Functional Requirements:

FDP_ACC.1A	The TSF enforces the Scout Management Policy on administrators.
FDP_ACF.1A	The TSF enforces the Scout Management Policy to control administrator access to each Scout's Scout Flow Control Policy based on the administrator's privileges for each Scout.
FMT_MOF.1	The TSF restricts the ability to modify the behavior of the TSF to authorized administrators.
FMT_MTD.1	The TSF restricts the ability to query and modify the TSF data to authorized administrators.
FMT_MSA.1A	The TSF enforces the Scout Management Policy to restrict the ability to modify security attributes.
FMT_MSA.3A	The TSF enforces the Scout Management Policy to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_SMF.1A	The TSF enables the specification of management functions.
FMT_SMR.1A	The TSF maintains the role administrator, and is able to associate users with that role.

6.1.4 Attack Detection and Prevention

The TOE protects networks from attack by identifying the reconnaissance activities that precede attacks, responding with false information and then identifying the false information embedded in the actual attack attempt, which is then blocked by the TOE and thus rendered harmless.

The detected reconnaissance activities and the subsequent attack attempts (if they materialize) are logged and administrators are alerted, in accordance with the policies defined by the TOE administrators.

The Attack Detection and Prevention function satisfies the following Security Functional Requirements:

FAU_ARP.1	In the event of a potential security violation, the TSF sends an alert to an alert destination and generates an audit record.
FAU_SAA.1	The TSF applies a set of rules in monitoring the audited events and based upon these rules indicates a potential violation of the TSP.
FDP_IFC.2	The TSF enforces the Scout Flow Control Policy on the (traffic monitored by the TOE) and ensures that all such traffic is covered by an information flow control SFP.
FDP_IFF.1	The TSF enforces the Scout Flow Control Policy based on subject and information security attributes.

6.2 TOE Security Assurance Measures

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

- Configuration Management
- Delivery and Operation
- Development
- Guidance Documents
- Tests
- Strength of Function Analysis and Vulnerability Assessment

6.2.1 Configuration Management

The configuration management measures applied by ForeScout Technologies ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. ForeScout Technologies ensures changes to the implementation representation are controlled. ForeScout Technologies 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:

- ForeScout Technologies Configuration Management Plan

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

- ACM_CAP.2

6.2.2 Delivery and Operation

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

These activities are documented in:

- ForeScout Delivery and Operation Procedures
- ForeScout Installation and User Guide

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

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

ForeScout Technologies has documents describing all facets of the design of the TOE. 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).

These activities are documented in:

- ForeScout Functional Specification
- ForeScout High-level Design
- ForeScout Representation Correspondence

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

ForeScout Technologies provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- ActiveScout SiteManager User's Guide

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

- AGD_ADM.1
- AGD_USR.1

6.2.5 TESTS

The test documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

These activities are documented in:

- ForeScout Test Plan
- ForeScout Test Results

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

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

6.2.6 STRENGTH OF FUNCTION ANALYSIS AND VULNERABILITY ASSESSMENT

6.2.6.1 STRENGTH OF FUNCTIONS ANALYSIS

ForeScout Technologies 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.

The only applicable (i.e., probabilistic or permutational) security functional requirements are FIA_UAU.2 (user authentication before any action) and FIA_UID.2 (user identification before any action).

This analysis is documented in:

- ForeScout Strength of Function Analysis

The Strength of Functions Analysis assessment assurance measure satisfies the following EAL 2 assurance requirements:

- AVA_SOF.1

6.2.6.2 VULNERABILITY ASSESSMENT

ForeScout Technologies 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:

- ForeScout Vulnerability Assessment

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

- AVA_VLA.1

7 PROTECTION PROFILE CLAIMS

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

8 RATIONALE

8.1 INTRODUCTION

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

- Security Objectives
- Security Requirements
- TOE Summary Specification
- SFR dependencies
- Internal consistency

8.2 SECURITY OBJECTIVES RATIONALE

This section shows that:

- each threat, organizational security policy and assumption is addressed by at least one security objective, and
- each security objective addresses at least one threat, organizational security policy or assumption.

Table 4. Mapping of Security Environment to Security Objectives

Security Environment	Security Objectives														
	O.MANAGE	O.AUTH	O.AUDIT-MGM	O.AUDIT-RVW	O.DETECT	O.AUDIT-ATK	O.ALERT	O.E.TRANSIT	O.E.TOE-PRT	O.E.TIME	O.E.ADMIN	O.E.BACKUP	O.E.LOCATE	O.E.INSTALL	O.E.BANDW
T.UA-ACCESS		X													
T.UA-TRANSIT								X							
T.UA-ACTION			X	X											
T.ATTACK	X				X	X	X								
T.DISABLE									X						
P.MANAGE									X		X			X	
A.ADMIN											X	X		X	
A.LOCATE													X		
A.BANDW															X

A.TIME										X					

8.2.1 T.UA-ACCESS

An unauthorized user may gain access to or modify TOE data stored in the TOE database.

This threat is addressed as follows:

- O.AUTH ensures that only authorized administrators are able to access the TOE and its data by uniquely identifying and authenticating all users attempting to access the TOE and its data.

8.2.2 T.UA-TRANSIT

An unauthorized user may gain access to or modify TOE data when it is in transit between distributed parts of the TOE.

This threat is addressed as follows:

- O.E.TRANSIT ensures that that the IT environment protects TSF data in transit between separate parts of the TOE.

8.2.3 T.UA-ACTION

An authorized user may exceed his or her privileges and perform unauthorized modifications of TOE data which go undetected.

This threat is addressed as follows:

- O.AUDIT-MGM ensures that the TOE generates audit records of all security-related actions of TOE users to ensure that these actions can be traced to the users who performed them.
- O.AUDIT-RVW ensures that the TOE provides the capability to review audit records.

8.2.4 T.ATTACK

An attacker may gain access to the protected network via the unprotected network (Internet) to which the protected network is connected and gain access to and/or modify user data.

This threat is addressed as follows:

- O.MANAGE ensures that the TOE provides the functionality that enables an authorized administrator to configure the TOE, define and enforce TOE security policies, and monitor the TOE's activities.
- O.DETECT ensures that the TOE detects attempted attacks and protects the protected network from these attacks.
- O.AUDIT-ATK ensures that the TOE generates audit records of detected attack attempts.
- O.ALERT ensures that the TOE responds to specified events by sending alerting administrators.

8.2.5 T.DISABLE

An attacker may disable the TOE or modify its behavior and thus expose the protected network to attack.

This threat is addressed as follows:

- O.E.TOE-PRT ensures that the IT environment protects the TOE data from unauthorized deletion or modification.

8.2.6 P.MANAGE

IT Systems are protected from unauthorized access and modification.

This organizational policy is addressed as follows:

- O.E.ADMIN ensures that authorized TOE administrators are properly trained in all aspects of TOE and TOE resource administration, and are neither negligent nor hostile.
- O.E.INSTALL ensures that the TOE and its associated hardware and software environment are installed, maintained and managed in a manner that complies with the TOE security objectives.
- O.E.TOE-PRT ensures that the IT environment protects the TOE data from unauthorized deletion or modification.

8.2.7 A.ADMIN

The administrators assigned to manage the TOE are competent, properly trained, not careless, not willfully negligent, not hostile, follow the guidance and instruction provided in the TOE documentation, and install and administer the TOE in a manner consistent with organizational policies.

This assumption is addressed as follows:

- O.E.ADMIN ensures that authorized TOE administrators are properly trained in all aspects of TOE and TOE resource administration, and are neither negligent nor hostile.
- O.E.BACKUP ensures that the TOE, its data and the systems on which it runs are restored to a secure state after failure by following the relevant backup and restore procedures.
- O.E.INSTALL ensures that the TOE and its associated hardware and software environment are installed, maintained and managed in a manner that complies with the TOE security objectives.

8.2.8 A.LOCATE

The TOE components are located in a physically secured area, protected from unauthorized physical access.

This assumption is addressed as follows:

- O.E.LOCATE ensures that the TOE components are located in a physically secured area, protected from unauthorized physical access.

8.2.9 A.BANDW

The volume of incoming traffic monitored by the TOE does not exceed the volume specified in TOE administrator guidance documentation.

This assumption is addressed as follows:

- O.E.BANDW ensures that the volume of incoming traffic monitored by the TOE is not permitted to exceed the volume specified in TOE administrator guidance documentation.

8.2.10 A.TIME

The operating environment provides a reliable time stamp for use by the TOE.

This assumption is addressed as follows:

- O.E.TIME ensures that the IT environment provides a reliable time-stamp for the TOE to be used for audit records.

8.3 SECURITY REQUIREMENTS RATIONALE

This section provides a rationale for the completeness and internal consistency of the claimed Security Functional Requirements (see "TOE Security Functional Requirements" on page 20) in meeting the identified security objectives (see "Security Objectives" on page Security Objectives) by showing that:

- each Security Functional Requirement addresses at least one TOE security objective, and
- each TOE security objective is addressed by at least one Security Functional Requirement.

Note – Security objectives for the IT environment and for the non-IT environment are addressed by assumptions or organizational security policies, as indicated in Table 4 on page 39.

Table 5. Mapping of Security Functional Requirements to TOE Security Objectives

Security Functional Requirements	TOE Security Objectives									
	O.MANAGE	O.AUTH	O.AUDIT-MGM	O.AUDIT-RVW	O.DETECT	O.AUDIT-ATK	O.ALERT	O.E.TRANSIT	O.E.TIME	O.E.TOE-PRT
FAU_ARP.1						X	X			
FAU_GEN.1			X			X				
FAU_GEN.2			X							
FAU_SAA.1					X					
FAU_SAR.1				X						
FAU_SAR.2				X						
FAU_STG.1			X							
FDP_ACC.1A		X								
FDP_ACC.1B										X
FDP_ACF.1A		X								
FDP_ACF.1B										X
FDP_IFC.2					X					
FDP_IFF.1					X					
FIA_UAU.2A		X								
FIA_UAU.2B										X
FIA_UID.2A		X								
FIA_UID.2B										X
FMT_MOF.1		X								
FMT_MSA.1A		X								
FMT_MSA.1B										X
FMT_MSA.3A		X								
FMT_MSA.3B										X
FMT_MTD.1		X								
FMT_SMF.1A	X									
FMT_SMF.1B										X
FMT_SMR.1A	X	X								

Security Functional Requirements	TOE Security Objectives									
	O.MANAGE	O.AUTH	O.AUDIT-MGM	O.AUDIT-RVW	O.DETECT	O.AUDIT-ATK	O.ALERT	O.E.TRANSIT	O.E.TIME	O.E.TOE-PRT
FMT_SMR.1B										X
FPT_ITT.1								X		
FPT_ITT.3								X		
FPT_STM.1									X	

8.3.1 O.MANAGE

The TOE must provide the functionality that enables an authorized administrator to configure the TOE, define and enforce TOE security policies (for example, the Scout Flow Control Policy), and monitor the TOE's activities.

FMT_SMF.1A The TSF enables the specification of management functions.

FMT_SMR.1A The TSF maintains the role administrator, and is able to associate users with that role.

8.3.2 O.AUTH

The TOE must ensure that only authorized administrators are able to access the TOE and its data by uniquely identifying and authenticating all users attempting to access the TOE and its data.

FDP_ACC.1A The TSF enforces the Scout Management Policy on administrators.

FDP_ACF.1A The TSF enforces the Scout Management Policy to control administrator access to each Scout's Scout Flow Control Policy based on the administrator's privileges for each Scout.

FIA_UAU.2A The TSF requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2A The TSF requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FMT_MOF.1 The TSF restricts the ability to modify the behavior of the TSF to authorized administrators.

FMT_MTD.1 The TSF restricts the ability to query and / or modify the TSF data to authorized administrators.

FMT_MSA.1A The TSF enforces the Scout Management Policy to restrict the ability to modify security attributes.

FMT_MSA.3A The TSF enforces the Scout Management Policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_SMR.1A	The TSF maintains the role administrator, and is able to associate users with that role.

8.3.3 O.AUDIT-MGM

The TOE must generate audit records of all security-related actions of TOE users to ensure that these actions can be traced to the users who performed them.

FAU_GEN.1	The TSF generates an audit record of the auditable events as listed in Table 2 (page 21).
FAU_GEN.2	The TSF records sufficient information within each audit record to fully describe the event and identify the user who initiated the event.
FAU_STG.1	The TSF protects stored audit data from deletion and detects modifications to the audit data.

8.3.4 O.AUDIT-RVW

The TOE must provide the capability to review audit records.

FAU_SAR.1	The TSF provides the administrator with the capability to read the audit records and presents the audit records in a manner suitable for the administrator to interpret the records.
FAU_SAR.2	The TSF allows only authorized administrators access to the audit records.

8.3.5 O.DETECT

The TOE must detect attempted attacks and protect the protected network from these attacks.

FDP_IFC.2	The TSF enforces the Scout Flow Control Policy on the traffic monitored by the TOE and ensures that all such traffic is covered by an information flow control SFP.
FDP_IFF.1	The TSF enforces the Scout Flow Control Policy based on subject and information security attributes.
FAU_SAA.1	The TSF applies a set of rules in monitoring the audited events and based upon these rules indicates a potential violation of the TSP.

8.3.6 O.AUDIT-ATK

The TOE must generate audit records of detected attack attempts.

FAU_GEN.1	The TSF generates an audit record of the auditable events as listed in Table 2 (page 21).
FAU_ARP.1	In the event of a potential security violation, the TSF sends an alert to an alert destination.

8.3.7 O.ALERT

The TOE must have the capability to respond to specified events by alerting administrators.

FAU_ARP.1	In the event of a potential security violation, the TSF sends an alert to an alert destination.

8.3.8 O.E.TRANSIT

The IT environment must have the ability to protect TSF data in transit between distributed parts of the TOE.

FPT_ITT.1	The IT environment protects TSF data from modification when it is in transit between separate parts of the TOE.
FPT_ITT.3	When the IT environment detects modifications of TSF data in transit between separate parts of the TOE, it aborts the transaction.

8.3.9 O.E.TIME

The IT environment must provide a reliable time-stamp for the TOE to be used for audit records.

FPT_STM.1	The IT environment provides reliable time stamps for use by the TSF.

8.3.10 O.E.TOE-PRT

The IT environment must protect the TOE data from unauthorized deletion or modification.

FDP_ACC.1B	The IT environment enforces the IT Environment Access Control Policy.
FDP_ACF.1B	The IT environment enforces the IT Environment Access Control Policy which allows only TOE. Administrators to modify or delete TOE data.
FIA_UAU.2B	The IT environment requires authentication before any TOE TSF action.
FIA_UID.2B	The IT environment requires identification before any TOE TSF action.
FMT_MSA.1B	The IT environment enforces the IT Environment Access Control Policy to restrict the ability to modify security attributes.
FMT_MSA.3B	The IT Environment enforces the IT Environment Access Control Policy to provide restrictive default values for security attributes that are used to enforce the SFP.
FMT_SMF.1B	The IT Environment maintains the roles TOE administrator and OS Administrator, and is able to associate users with that role
FMT_SMR.1B	The IT Environment enforces the IT Environment Access Control Policy to restrict the ability to modify security attributes.

8.4 SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCIES RATIONALE

Table 6. Functional Requirements Dependencies

Requirement	Dependencies	Included ?
FAU_ARP.1	FAU_SAA.1	Yes, TOE SFR
FAU_GEN.1	FPT_STM.1	Yes, IT environment SFR
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Yes TOE SFR Yes, hierarchical to the TOE SFR FIA_UID.2A
FAU_SAA.1	FAU_GEN.1	Yes TOE SFR
FAU_SAR.1	FAU_GEN.1	Yes, TOE SFR
FAU_SAR.2	FAU_SAR.1	Yes, TOE SFR
FAU_STG.1	FAU_GEN.1	Yes, TOE SFR
FDP_ACC.1A	FDP_ACF.1	Yes, TOE SFR
FDP_ACF.1A	FDP_ACC.1 FMT_MSA.3	Yes, TOE SFR Yes, TOE SFR
FDP_IFC.2	FDP_IFF.1	Yes, TOE SFR
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Yes, hierarchical to IFC 2 Yes, TOE SFR

Requirement	Dependencies	Included ?
FIA_UAU.2A	FIA_UID.1	Yes hierarchical to the TOE SFR FIA_UID.2A
FIA_UID.2A	none	
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Yes, TOE SFR Yes, TOE SFR
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Yes, TOE SFR Yes, TOE SFR
FMT_MSA.1A	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	Yes, TOE SFR Yes, TOE SFR Yes, TOE SFR
FMT_MSA.3A	FMT_MSA.1 FMT_SMR.1	Yes, TOE SFR Yes, TOE SFR
FMT_SMF.1A	none	
FMT_SMR.1A	FIA_UID.1	Yes, hierarchical to the TOE SFR FIA_UID.2A
FDP_ACC.1B	FDP_ACF.1	Yes, IT environment SFR
FDP_ACF.1B	FDP_ACC.1 FMT_MSA.3	Yes, IT environment SFR Yes, IT environment SFR
FIA_UAU.2B	FIA_UID.1	Yes hierarchical to the IT environment SFR FIA_UID.2B
FIA_UID.2B	none	
FMT_MSA.1B	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	Yes, IT environment SFR Yes, IT environment SFR Yes, IT environment SFR
FMT_MSA.3B	FMT_MSA.1 FMT_SMR.1	Yes, IT environment SFR Yes, IT environment SFR
FMT_SMF.1B	none	
FMT_SMR.1B	FIA_UID.1	Yes, hierarchical to the IT Environment SFR FIA_UID.2B
FPT_ITT.1	none	

Requirement	Dependencies	Included ?
FPT_ITT.3	FPT_ITT.1	Yes, IT Environment SFR

8.5 SECURITY ASSURANCE REQUIREMENTS RATIONALE

EAL2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. The security objectives defined for the TOE are consistent with an EAL2 assurance level and EAL2 is sufficient to satisfy the security objectives of the TOE.

EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behavior. The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain). EAL2 also provides assurance through a configuration list for the TOE and evidence of secure delivery procedures. The TOE and related documentation have all of the characteristics required for EAL2.

Table 7 provides a mapping of the EAL2 Security Assurance Components to the documentation demonstrating how the TOE and the TOE developer satisfy the requirements. The detailed justification for the mapping is given in "TOE Security Assurance Measures" on page 35.

Table 7. Mapping of Security Assurance Requirements to Documents and Rationale

Assurance Components	Documents Satisfying the Assurance Component	Rationale
ACM_CAP.2	ForeScout Technologies Configuration Management Plan	Shows the CM system is being used. Configuration Item List(s) is comprised of List of the source code files and version numbers List of design documents with version numbers Test documents with version numbers User and administrator documentation with version numbers
ADO_IGS.1	ForeScout Delivery and Operation Procedures ForeScout Installation and User Guide	Provides detailed instructions for installation of the product by the distributor.
ADO_DEL.1		Provides a description of all procedures that are necessary to maintain security when distributing the product to the distributor. Applicable across all phases of delivery from packaging, storage, distribution
ADV_FSP.1	ForeScout Functional Specification	Describes the TSF interfaces and TOE functionality

Assurance Components	Documents Satisfying the Assurance Component	Rationale
ADV_HLD.1	ForeScout High-Level Design	Describes the TOE subsystems and their associated security functionality
ADV_RCR.1	ForeScout Representation Correspondence	Provides the following two dimensional mappings: 1. TSS and functional specification; 2. functional specification and high-level design.
AGD_ADM.1	ForeScout ActiveScout SiteManager User's Guide	Describes how to administer the TOE securely.
AGD_USR.1		Describes the secure use of the TOE.
ATE_IND.2	ForeScout Test Plan ForeScout Test Results	Not applicable
ATE_COV.1		Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_FUN.1		Test documentation includes test plans and procedures and expected and actual results.
AVA_SOF.1	ForeScout Strength of Function Analysis	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
AVA_VLA.1	ForeScout Vulnerability Assessment	Provides an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.6 STRENGTH OF FUNCTIONS RATIONALE

The claimed TOE minimum strength of function is SOF-basic. This strength of function level was selected because it generally corresponds with the claimed assurance level of EAL 2.

The TOE includes security functional requirements that have a specific strength of function metrics or a mechanism of a probabilistic or permutational nature.

The password mechanism is of a probabilistic or permutational nature. The password mechanism is used in the Identification and Authentication security function to authenticate user identity. The relevant Security Functional Requirements are:

- FIA_UAU.2
- FIA_UID.2

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 [VLA-SOF].

8.7 TOE SUMMARY SPECIFICATION RATIONALE

The following table represents a mapping between the security functions in this Security Target to their related TOE Security Functional Requirements; the rationale for how each security function meets the corresponding Security Functional Requirement is provided in Section 6.1, which lists each SFR and describes how the SFR is met by the TOE Security Function.

Table 8. Mapping of Security Functional Requirements to TOE Security Functions

Security Functional Requirements	TOE Security Functions			
	Security Audit (SA)	Identification and Authentication (I & A)	Security Management (SM)	Attack Detection and Prevention (AD & P)
FAU_ARP.1				X
FAU_GEN.1	X			
FAU_GEN.2	X			
FAU_SAA.1				X
FAU_SAR.1	X			
FAU_SAR.2	X			
FAU_STG.1	X			
FDP_ACC.1A			X	
FDP_ACF.1A			X	
FDP_IFC.2				X
FDP_IFF.1				X
FIA_UAU.2A		X		
FIA_UID.2A		X		
FMT_MOF.1			X	
FMT_MSA.1A			X	
FMT_MSA.3A			X	
FMT_MTD.1			X	
FMT_SMF.1A			X	
FMT_SMR.1A			X	