SECURIFY

Securify SecurVantage™ 5.0
Security Target

Version 2.0

Last Revision: February 10, 2006

Prepared by:

CYGNACOM SOLUTIONS

An Entrust Company

Suite 5200♦7925 Jones Branch Drive♦McLean, VA 22102-3305♦703 848-0883♦Fax 703 848-0960

Revision History

Date	Version	Author	Description
01/05/05	1.0	Debra Baker, CygnaCom	First draft
02/10/06	2.0	Jose Caldera, Securify	Evaluation release

Table of Contents

1 SECURITY TARGET INTRODUCTION 7

1.1 SECURITY TARGET IDENTIFICATION 7
1.2 SECURITY TARGET OVERVIEW 8
1.3 COMMON CRITERIA CONFORMANCE 8
1.4 DOCUMENT ORGANIZATION 8

2 TOE DESCRIPTION 9

2.1 PRODUCT TYPE 9
2.2 SECURVANTAGE™ COMPONENTS 9
2.2.1 SecurVantage™ Studio 12
2.2.2 SecurVantage™ Monitor 14
2.2.3 SecurVantage™ Enterprise 15
2.2.4 SecurVantage™ Enterprise Reporting Gateway 16
2.3 TSF BOUNDARY AND SCOPE OF THE EVALUATION 17
2.4 LOGICAL BOUNDARY 17
2.5 SECURITY ENVIRONMENT 18

3 TOE SECURITY ENVIRONMENT 18

3.1 ASSUMPTIONS 18
3.2 THREATS 19
3.3 POLICIES 20

4 SECURITY OBJECTIVES 21

4.1 SECURITY OBJECTIVES FOR THE TOE 21
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT 22
4.2.1 Security Objectives for the IT Environment 22
4.2.2 Non-IT Security Objectives 22

5 IT SECURITY REQUIREMENTS 23

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS 23
5.1.1 SFRs for Studio, Monitor, and Enterprise are in section 5.1.1. SFRs for Enterprise Reporting Gateway are in section 5.1.2 25
5.1.2 SFRs for Enterprise Reporting Gateway are below: 34
5.2 TOE SECURITY ASSURANCE REQUIREMENTS 42
5.3 SECURITY REQUIREMENTS FOR THE IT ENVIRONMENT 43
5.3.1 Class FPT: Protection of the TSF 43
5.3.2 Class FTP: Trusted Path/Trust Channel 44
5.4 STRENGTH OF FUNCTION 45

6 TOE SUMMARY SPECIFICATION 46

6.1 IT SECURITY FUNCTIONS 46
6.1.1 Overview 46
6.1.2 SecurVantage™ Studio 46
6.1.3 SecurVantage™ Monitor 47
6.1.4 SecurVantage™ Enterprise 51
6.1.5 SecurVantage™ Enterprise Reporting Gateway 54
6.2 ASSURANCE MEASURES 56
6.3 STRENGTH OF FUNCTION 57

7 PP CLAIMS 57

8 RATIONALE 57

8.1 SECURITY OBJECTIVES RATIONALE 57
8.1.1 Organizational Security Policies 57
8.1.2 Threats to Security 58
8.1.3 Assumptions 69
8.2 SECURITY REQUIREMENTS RATIONALE 72
8.2.1 Requirements for the TOE 72
8.2.2 Requirements for the IT Environment 80
8.2.3 Dependencies 81
8.2.4 Strength of Function Rationale 86
8.2.5 Assurance Requirements Rationale 86
8.2.6 Explicitly Stated Requirements Rationale 86
8.3 TOE SUMMARY SPECIFICATION RATIONALE 87
8.3.1 IT Security Functions 87
8.3.2 Assurance Measures 100
8.3.3 Strength of Function 104
8.4 PP CLAIMS RATIONALE 105

9 ACRONYMS 106

Figures and Tables

Figures

FIGURE 2-1 TYPICAL SECURVANTAGE DEPLOYMENT 10
FIGURE 2-2 SECURVANTAGE™ SYSTEM ARCHITECTURE 12
FIGURE 2-3 NETWORK TOPOLOGY 13
FIGURE 2-4 STUDIO ANALYSIS ENVIRONMENT 14

Tables

TABLE 3-1 TOE USAGE ASSUMPTIONS 18
TABLE 3-2 TOE PHYSICAL ASSUMPTIONS 19
TABLE 3-3 TOE PERSONNEL ASSUMPTIONS 19
TABLE 3-4 THREATS 19
TABLE 3-5 ORGANIZATIONAL SECURITY POLICIES 20
TABLE 4-1 TOE SECURITY OBJECTIVES 21
TABLE 4-2 SECURITY OBJECTIVES FOR THE IT ENVIRONMENT 22
TABLE 4-3 NON-IT SECURITY OBJECTIVES 22
TABLE 5-1 FUNCTIONAL COMPONENTS 23
TABLE 5-2 SECURVANTAGE™ USER ACCESS POLICY 28
TABLE 5-3 SECURVANTAGE™ ER USER ACCESS POLICY 36
TABLE 5-4 MANAGEMENT OF SECURITY ATTRIBUTES 39
TABLE 5-5 MANAGEMENT OF TSF DATA 40
TABLE 5-6 EAL3 ASSURANCE COMPONENTS 42
TABLE 5-7 FUNCTIONAL COMPONENTS FOR THE IT ENVIRONMENT 43
TABLE 8-1 MAPPING OF ORGANIZATIONAL SECURITY POLICIES TO SECURITY OBJECTIVES FOR THE TOE 57
TABLE 8-2 ALL THREATS TO SECURITY COUNTERED 59
TABLE 8-3 MAPPING SECURITY OBJECTIVES FOR THE TOE AND IT ENVIRONMENT TO THREATS/POLICIES 67
TABLE 8-4 REVERSE MAPPING OF NON-IT SECURITY OBJECTIVES FOR THE ENVIRONMENT TO THREATS/POLICIES/ ASSUMPTIONS 69
TABLE 8-5 ALL ASSUMPTIONS ADDRESSED 69
TABLE 8-6 ALL OBJECTIVES MET BY FUNCTIONAL COMPONENTS 72
TABLE 8-7 ALL OBJECTIVES FOR THE IT ENVIRONMENT MET BY REQUIREMENTS FOR IT ENVIRONMENT 77
TABLE 8-8 MAPPING OF IT SECURITY FUNCTIONAL REQUIREMENTS TO OBJECTIVES FOR THE TOE 79
TABLE 8-9 MAPPING OF SECURITY FUNCTIONAL REQUIREMENTS FOR THE IT ENVIRONMENT TO OBJECTIVES FOR THE IT ENVIRONMENT 81
TABLE 8-10 DEPENDENCIES FOR TOE 81
TABLE 8-11 DEPENDENCIES FOR IT ENVIRONMENT 86
TABLE 8-12 MAPPING OF FUNCTIONAL REQUIREMENTS TO TOE SUMMARY SPECIFICATION 87
TABLE 8-13 ASSURANCE MEASURES RATIONALE 100

1 Security Target Introduction

1.1 Security Target Identification

TOE Identification:

Securify SecurVantage™ Studio: 5.0 (V50_CC_7)

Securify SecurVantage™ Monitor (SM): 5.0 (V50_CC_7) with patch "Patch2" (V50_324)

Securify SecurVantage™ Monitor (Harvester): 5.0 (V50_CC_7) with patch "Patch2" (V50_324)

Securify SecurVantage™ Monitor (LE): 5.0 (V50_CC_7) with patch "Patch2" (V50_324)

Securify SecurVantage™ Enterprise: 5.0 (V50_CC_7) with patch "Patch2" (V50_324)

Securify SecurVantage™ Enterprise Reporting Gateway: 5.0 (V50_CC_7) with patch "Patch2" (V50_324)

ST Title:	Securify SecurVantage™ Version 5.0 Security Target
ST Version:	2.0
ST Authors:	CygnaCom/Securify
ST Date:	February 10, 2006
Assurance level:	EAL3
Keywords:	Network Security, Monitoring, Analysis, Identification, Authentication, Access Control, Audit, and Security Target

1.2 Security Target Overview

This Security Target (ST) defines the Information Technology (IT) security requirements for Securify SecurVantage™ Version 5.0. Securify SecurVantage™ is an automated security system that enables customers to generate business-driven security policies, monitor networks for compliance, produce relevant network operational information, and provides quantitative network and application trend reporting. This software product consists of an environment for policy development and security analysis, a real-time monitoring system to continuously verify conformance to business practices and security policies, and an Enterprise management and trend reporting system. The SecurVantage™ system is driven by a customer-specific policy that formally describes the desired operation of the network.

1.3 Common Criteria Conformance

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 3 from the Common Criteria Version 2.2, January 2004.

1.4 Document Organization

The main sections of an ST are the ST Introduction, Target of Evaluation (TOE) Description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specification, and Rationale.

Section 2, the *TOE Description*, describes the product type and the scope and boundaries of the TOE.

Section 3, *TOE Security Environment*, identifies assumptions about TOE's intended usage and environment and threats relevant to secure TOE operation.

Section 4, *Security Objectives*, defines the security objectives for the TOE and its environment.

Section 5, *IT Security Requirements*, specifies the TOE Security Requirements. The TOE security requirements are made up of Functional Requirements and Assurance Requirements. This section also includes Security Requirements for the IT Environment.

Section 6, *TOE Summary Specification*, describes the IT Security Functions and Assurance Measures.

Section 7, *Protection Profile (PP) Claims*, is not applicable. This product does not claim conformance to any PP.

Section 8, *Rationale*, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

Acronym definitions and references are provided in sections 9 and 10.

2 TOE Description

2.1 Product Type

Securify SecurVantage™ is an automated security system that enables customers to generate business-driven security policies, monitor networks for compliance and produce relevant network operational information. This software product consists of an environment for policy development and security analysis, a real-time monitoring system to continuously verify conformance to business practices and security policies, and an enterprise management and trend reporting system. The SecurVantage™ system is driven by a customer-specified policy that formally describes the desired operation of the network.

2.2 SecurVantage™ Components

SecurVantage™ relies on a proprietary policy language that translates business requirements and security policies into a formal, machine monitored specification (a "policy") describing the "correct" behavior of the network.

SecurVantage™ then evaluates, in real time, the packets flowing through the network at all levels of the protocol stack and makes decisions on whether the traffic is consistent with the policy specification. This information is then presented in a web-based analysis environment in terms that are specific to the business, and actionable for the team running the network.

SecurVantage™ consists of four major components:

SecurVantage™ Studio provides management interfaces that allows for the authoring of network security policy at multiple levels.

SecurVantage™ Monitor evaluates monitored network traffic according to the security policy translating business requirements.

SecurVantage™ Enterprise combines multiple monitoring points into a single, real-time monitoring and management console.

SecurVantage™ Enterprise Reporting Gateway component of SecurVantage™ Enterprise Reporting solution, is used in providing quantitative network and application trend reporting.

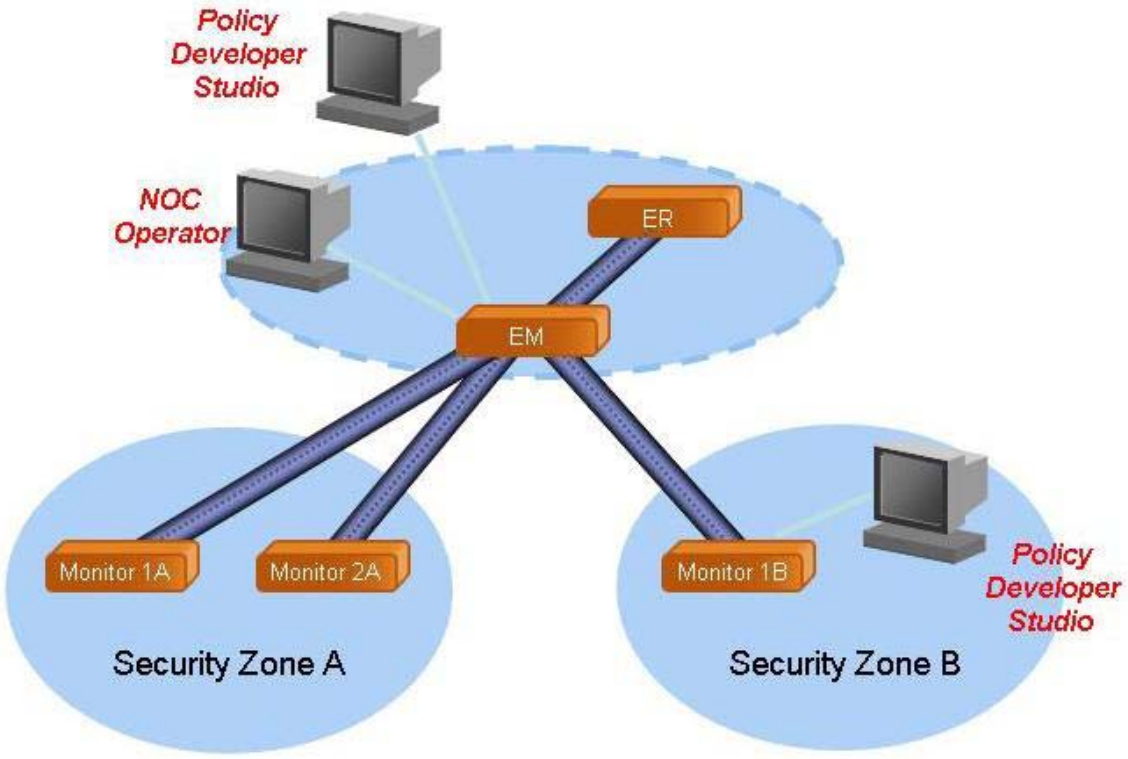

Figure 2-1 Typical SecurVantage Deployment

Figure 2-1 shows a typical deployment of SecurVantage™, although SecurVantage™ Monitor can be placed anywhere on the network. It does not necessarily have to be on its own sub-network and does not have to be connected through a switch. Typically, SecurVantage™ Monitor is connected to the SPAN port of a switch (see limitations) where there is traffic relevant to the policy. However, there are no assumptions about the source of the traffic. It is recommended that the Monitor be deployed in a trusted environment. In this Figure Monitor refers either to SM/Harvester pair or Monitor LE. ER refers to ER Gateway and ER Warehouse (not evaluated).

Limitations:

SecurVantage™ Monitor audits IPv4 packets when transported over Ethernet frames with length less than 1518 bytes. Notice that this includes neither IPv6 packet nor Ethernet Jumbo frames. These types of packets are discarded without logging.

Administrators are advised to configure any switch that may be present in the environment to disable Ethernet Jumbo frames.

Product Overview:

A SecurVantage™ Policy is a set of rules that describe the expected behavior of the systems within a network. Network objects represent systems. A network object can be one or many IP addresses.

Each rule in the Policy describes how the system will log a network transaction between two network objects. All network transactions are logged and represented as an event (see network event definition below). Each event represents the information contained in the headers of the actual packets within the network transaction.

Network event: In SecurVantage™, an output of the policy engine is created when network traffic is evaluated against a policy. A network event is a summary of the set of protocol events that make up a complete application level session on the network. For example, viewing a web page creates a network event that summarizes the underlying IP association, TCP connection and HTTP Get protocol events.

A network event is identified by the packet, which initiates an application session between devices. The policy engine assigns the following information to the network event, based on the protocol events and the most relevant policy rule that fires during policy evaluation:

- Source and destination IP addresses, the derived policy network objects, network object names, and services that those IP addresses resolve to.
- Outcome components assigned, including: protocol, outcome, protocol component and criticality.
- Owner: either the outcome, service, or reporting element owner in that order of precedence.
- Source and destination routing objects to provide IP routing information.
- Event time and other relevant protocol details.

The policy assigns by default a severity to every event, such that all events are logged by default. These default values can be changed by the user of the system to accommodate specific security policies. A severity has one of the following options: Critical, High, Medium, Warning, Monitor, or Ok. All events other than Monitor and Ok are fully logged in the system down to the protocol details level (source and target network object name, IP addresses, protocols, SRC port, DST port, TCP flags, UDP association, etc.). Events that have a severity value of Ok are logged at a summary level (source and target network object name and service name).

Events logged as Critical are also called Alerts and copied to a separate Alert table. Alerts can trigger SMTP and SNMP messages to other management systems.

Flow of Information:

Monitor captures network traffic and converts it into network events. As mentioned, every event has an associated severity. Monitor compares the event with a local copy of the Security Policy (previously uploaded by the user – Policy files are terminated with a “pdx” suffix) and logs the events according to their assigned severity as specified in the Security Policy. Logged traffic and Critical events (Alerts) are stored in the Monitor database and can be accessed via Monitor web interface or through Studio. Data is stored in the Monitor for a window of time (for normal deployment scenarios, around three weeks). This data is accessible via web interface for the last 48 hours and through Studio for as long as the data stays in the database.

If an Enterprise system is deployed, Enterprise copies information from the Monitors connected to it and aggregates this into a local database. This database is accessible through the web interface for a period

of 48 hours. The Enterprise serves also as a conduit to the Monitors' databases when detailed information is requested by the Studio application.

If the Enterprise Reporting component is deployed, then data moves from the Enterprise system to the ER Gateway. The ER Gateway inserts the data into the ER Warehouse, where it becomes available to the third-party report-generation engine (not evaluated).

SecurVantage™ consists of the policy development and analysis environment coupled with the monitoring system and the Enterprise management system. Figure 2-2 SecurVantageTM System Architecture shows the System Architecture.

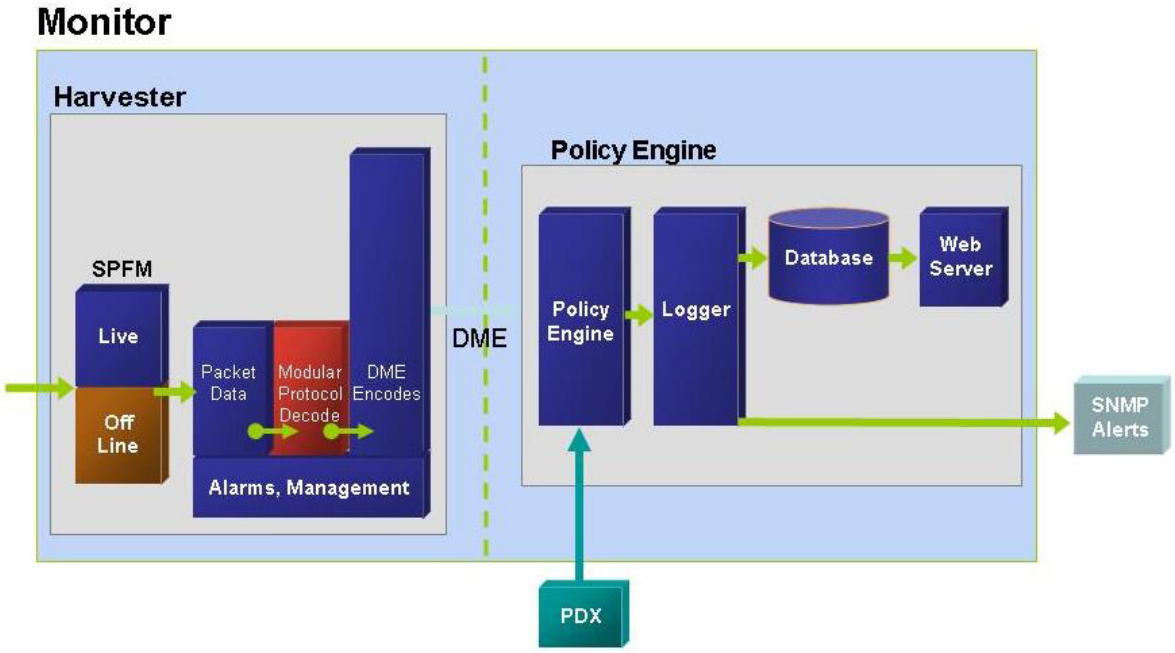

Figure 2-2 SecurVantage™ System Architecture

2.2.1 SecurVantage™ Studio

Securify's SecurVantage™ Studio provides a management interface that allows for the authoring of network security policy at multiple levels.

A typical policy requires a simple depiction of the topology of the network to be monitored. The network topology is constructed with "network objects" such as routers, firewalls, and subnets which can be created within the drag and drop environment, depicted in the figure below:

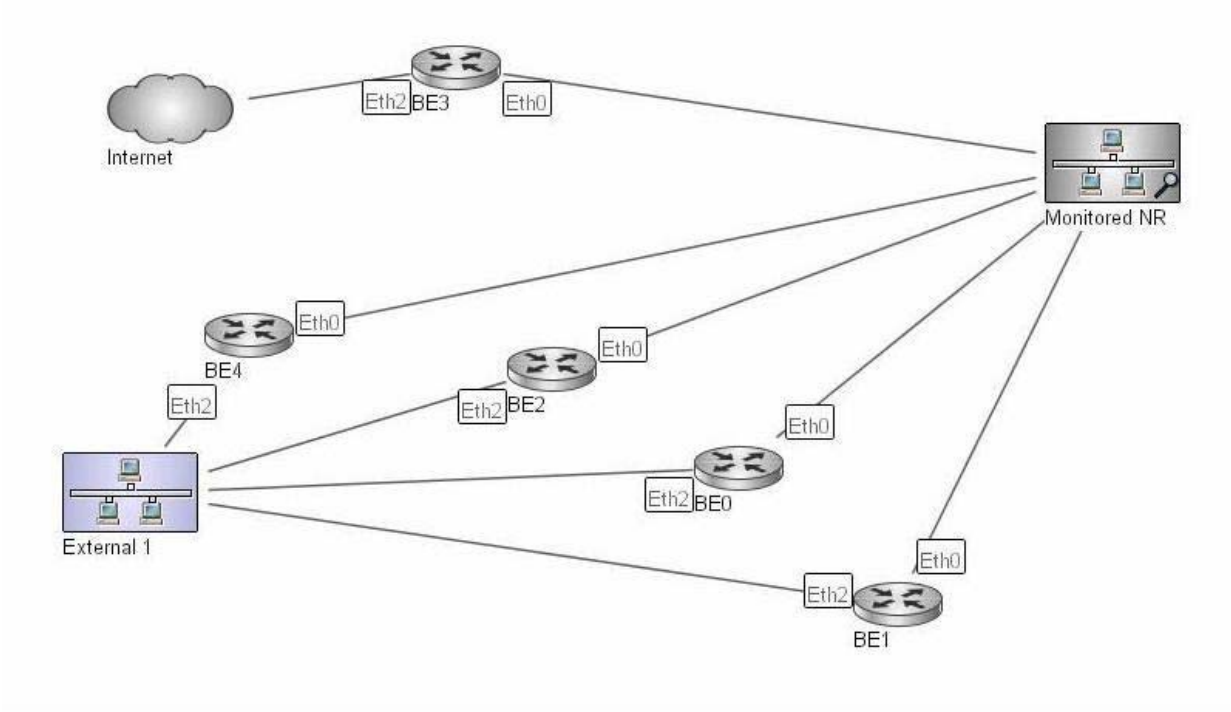

Figure 2-3 Network Topology

Network objects are functional groups of devices that exhibit a similar network function or behavior.

Using Rules to Tie Together Network Objects: The Security Policy is a set of rules used to create a set of relationships between network objects and describe how these network objects should interact. Rules can be general and applied throughout the OSI protocol stack, authored for multiple IP addresses, or applied to one specific network address. A high level rule can specify things such as routing tables and allowed IP level traffic, while a low level rule can specify the exact HTTP requests allowed into a web server or the authentication mechanism that the SSH protocol should exhibit on a network.

Analysis Environment: Studio provides an analysis interface that allows users to perform detailed analysis on network traffic being evaluated by the security policy. This analysis can be performed either locally in the Studio or remotely on a Monitor.

Offline analysis of Network Traffic: The Monitor can be configured to capture network traffic (in files) before policy evaluation occurs on the Monitor. These files are called DME (a Securify proprietary format) files. Studio is able to read DME files from disk and then evaluate the traffic contained in them using a policy running locally in Studio. Information about network security events is written to a local database and queried using a Java-based user interface within the Studio application. This analysis environment, depicted in Figure 2-4 Studio Analysis Environment below, enables easy querying using various constraints on specific scenarios of interest via a spreadsheet metaphor. Studio allows a drill down on the network security events to the protocol layers.

Online analysis of Network Traffic: Studio can be also be configured to query the database running remotely on a Monitor. Studio makes an authenticated connection to the Monitor to access information about network security events generated at that particular Monitor location (in the network). The same interface depicted in Figure 2-4 is used for such purposes.

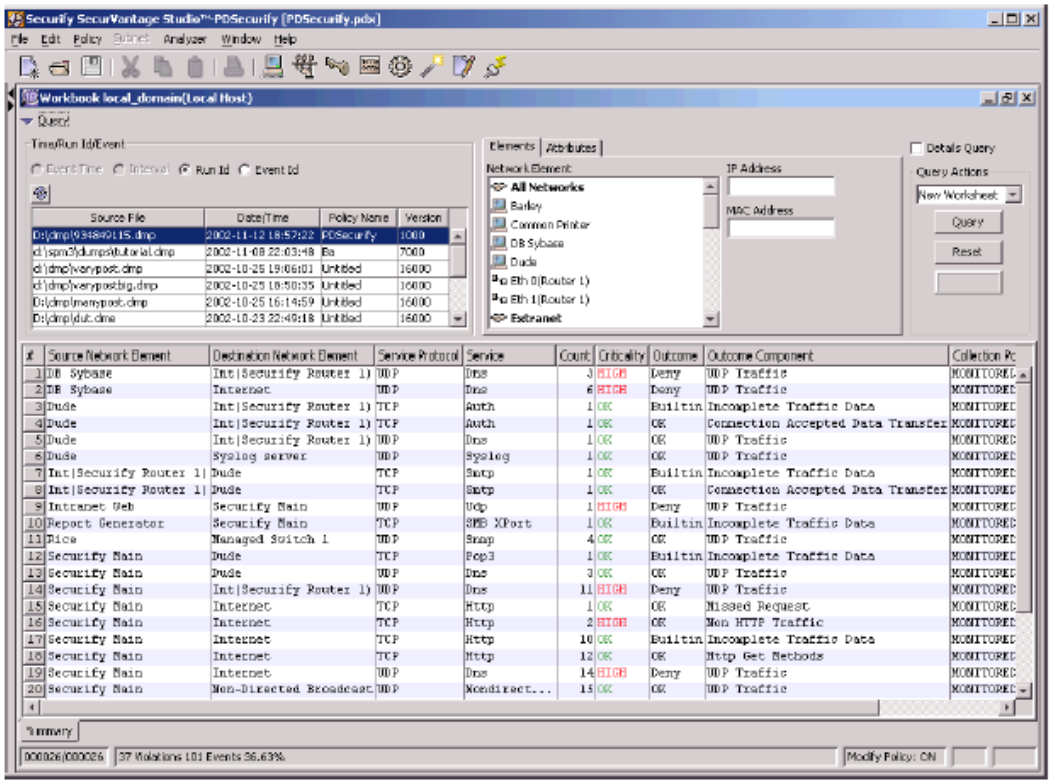

Figure 2-4 Studio Analysis Environment

2.2.2 SecurVantage™ Monitor

SecurVantage™ Monitor is a network monitoring and reporting system. Monitor evaluates real-time traffic on a continuous basis against the security policy. Monitor is available in two forms: one form as a high bandwidth version consisting of two systems (Securify SecurVantage™ Monitor) and the other form as a low bandwidth solution consisting of only one system (Securify SecurVantage™ Monitor LE).

Real-Time Monitoring: SecurVantage™ Monitor or Monitor LE resides within a customer's network and evaluates, in real time, IPv4 packets flowing through the network at all levels of the protocol stack. Network transactions are automatically and continuously evaluated for conformance to a customer specific policy.

Analysis and Actions: Data, related to network traffic, is captured, evaluated, and stored as network and protocol events in a database for web-based analysis and alert generation. SecurVantage™ Monitor

uses this data to make decisions on whether the traffic is consistent with the policy specification. This information is then presented in a web-based analysis environment in terms specific to the business and actionable by the team running the network.

Controlled Access: To meet security and operational requirements, SecurVantage™ Monitor provides role-based access to views and system functionality. User-roles include: the Operator role, for viewing operations conformance data; the Analyst role, for analyzing the network security events generated by specific policies; the Developer role for creating, modifying and promoting policy; the SV (SecurVantage™) Manager role for managing the operations of SecurVantage™ in the operations environment; and the Account Manager role.

Real-Time Event Viewing and Reporting: Traffic conformance data can be accessed, via a defined role described above, in real time, through a web browser over an encrypted link. The SecurVantage™ Monitor uses the network objects as defined in the policy, to provide the context to view network security events. Users can query details of recent network security events within a window of 48 hours through a web browser. As previously mentioned, through Securify SecurVantage™ Studio users can access data in a window of 4 weeks or more, depending upon the density of the network events.

Auditing: SecurVantage™ Monitor and Monitor LE store the results of monitored and evaluated network traffic in a local database. These records cannot be deleted or modified. A copy of events logged as critical is also kept in a different table called Alerts, to ease management of these critical events. Alerts may be deleted from this table when users have addressed them either in their infrastructure or in the Security Policy. Note that these alerts are not the original data stored in the database. In other words, users can delete alerts but not the original data. In addition, SecurVantage™ Monitor and Monitor LE keep an auditing trail of every transaction that occurs in the system. These audit trails are referred to as Application Logs and User Logs. Application Logs store audit trails of the application inner subsystems, internal operations, web- and application-related logs and system syslogs. User Logs store audit trails of every user transaction, including actions and configuration.

2.2.3 SecurVantage™ Enterprise

SecurVantage™ Enterprise aggregates and manages multiple SecurVantage™ Monitors into a single, real-time web-based viewing and reporting interface and management console. SecurVantage™ Enterprise provides a common operational environment for user access, Monitor configuration and policy management across multiple Monitors and policy domains. With SecurVanatge™ Enterprise, real-time network security events and conformance information is viewable through a web browser and can be presented in a variety of reports, ranging from general network health to detailed network event information about a given IP, host, service, or ports in the network.

Management of Multiple Policy Domains: Policy management becomes centralized when multiple Monitors are connected to a SecurVantage™ Enterprise. Promoting and reverting policy is executed at the SecurVantage™ Enterprise by mapping a policy to one or more Monitors. Such mapping across Monitors is called a "Policy Domain". A Monitor can run only one policy, but one policy can run on multiple Monitors. The resulting network events can be viewed on the SecurVantage™ Enterprise by individual Policy Domain as well as across multiple Policy Domains. Administration of policy on Monitors also utilizes the same policy-to-monitor mapping mechanism.

Controlled Access: To meet security and operational requirements, SecurVantage™ Enterprise provides role-based access to views and system functionality. User-roles include: the Operator role, for viewing operations conformance data; the Analyst role, for analyzing the network security events

generated by specific policies; the Developer role for creating, modifying, and promoting policy; the SV (SecurVantage™) Manager role for managing the operations of SecurVantage™ in the operations environment; and the Account Manager role to administer user accounts.

Real-Time Event Viewing and Reporting: Traffic conformance data can be accessed in real time, via a defined role described above, through a web browser over an encrypted link. The SecurVantage™ Enterprise uses the network objects as defined in the policies (running in each connected Monitor) to provide the context to view aggregated network security events across multiple Monitors. Users can query details of recent network security events within a window of 48 hours.

Auditing: SecurVantage™ Enterprise pulls data from the associated SecurVantage™ Monitors and stores this data in a local database for user consumption. This data is a reduced copy of the data stored in the SecurVantage™ Monitor's database. These records cannot be deleted or modified. Since SecurVantage™ Monitors are managed through the SecurVantage™ Enterprise, actions on the alerts are really pertinent to the SecurVantage™ Monitors as described in the Auditing section of SecurVantage™ Monitor. SecurVantage™ Enterprise keeps an audit trail of all Application related transactions and User related transactions (these audit trails are described under the Auditing section of the SecurVantage™ Monitor component).

2.2.4 SecurVantage™ Enterprise Reporting Gateway

SecurVantage™ Enterprise Reporting (ER) solution is composed of an ER Gateway and an ER Warehouse (ER Warehouse is not evaluated). Each of these is installed on separate machines.

The ER Gateway has a web-based Administrator GUI that is used to administer the ER Gateway and Enterprise components.

SecurVantage™ Enterprise Reporting Gateway is used in providing quantitative network and application trend reporting from one or multiple SecurVantage™ Enterpise systems. Using daily, weekly, and monthly reports from SecurVantage™ Enterprise Reporting , network security managers and executives can review the overall security status of the network based on their specific policy. Reports range from overall network security policy compliance to detailed information on applications and network assets.

Robust Reporting Capabilites: SecurVantage™ Enterprise Reporting provides a range of reporting capabilities that enable users to run customer-specific summaries and detailed reports, on demand or scheduled on a regular basis. With SecurVantage™ Enterprise Reporting, high-level summary reports present the security status of both the Enterprise and individual business units. SecurVantage™ Enterprise Reporting can also be used to deliver detailed reports, including top violators, top targets and violations by protocol to aid in measuring and tracking the impact of security decisions. Report templates include policy compliance by date and policy compliance by reporting element. SecurVantage™ Reporting also offers variable reports which allow user-defined selection of parameters by IP address, reporting element, network object, policy outcome or port. With SecurVantage™ Enterprise Reporting, reports can be run hourly, daily, or according to user-defined parameters. Report data is available in a range of formats (PDF, HTML, Excel, etc.) for integration into business documents or information management systems.

Easy Access to Security Data to Measure Effectiveness: SecurVantage™ Enterprise Reporting facilitates security process management by providing authorized users with easy access to a range of quantitative security data that allows them to measure the effectiveness of security programs. SecurVantage™ Enterprise Reporting provides users with a range of reports that deliver an ongoing picture over time of overall network security operation. By simplifying access to data, authorized users can retrieve security metrics more often and in greater detail to support important decisions related to resource allocation, project priority, and workflow optimization.

2.3 TSF Boundary and Scope of the Evaluation

The evaluated configuration includes the following:

- SecurVantage™ Studio 5.0 (V50_CC_7) running on Microsoft Windows XP
- SecurVantage™ Monitor 5.0 (V50_CC_7 with patch "Patch 2": V50_324) running on Linux Red Hat 7.2
- SecurVantage™ Monitor LE 5.0 (V50_CC_7 with patch "Patch 2": V50_324) running on Linux Red Hat 7.2
- SecurVantage™ Enterprise 5.0 (V50_CC_7 with patch "Patch 2": V50_324) running on Linux Red Hat 7.2
- SecurVantage™ Enterprise Reporting Gateway 5.0 (V50_CC_7 with patch "Patch 2": V50_324) running on Linux Red Hat 7.2

The TOE includes the SecurVantage™ Studio, Monitor, Monitor LE, Enterprise, and Enterprise Reporting Gateway software, but it does not include the underlying operating system software, embedded databases or hardware. The Enterprise Reporting 5.0 Warehouse is not included in this evaluation. Active Vulnerability Scanner (known as Vulnerability Assessment feature) and Packet Capture though shipped with the Monitor and Monitor LE products are not part of the evaluation. These features are turned off by default and they will remain off for the purpose of this evaluation.

2.4 Logical Boundary

The TOE provides the following security features:

- **Security Audit** - SecurVantage™ provides its own auditing capabilities separate from those of the Operating System.
- **Access Control** - SecurVantage™ provides its own access control (authorization) separate from the Operating System between subjects and objects within the TOE's Scope of Control. This is covered by the SecurVantage™ User Access Policy.
- **User Identification and Authentication** - SecurVantage™ provides user identification and authentication through the use of user accounts.

- **Security Management** - SecurVantage™ provides security management through the use of the Administrator Interfaces. Through the enforcement of the SecurVantage™ User Access Policy, the ability to manage various security attributes is controlled.
- **Partial Protection of TSF** - SecurVantage™ protects its programs and data from unauthorized access through its own interfaces.

2.5 Security Environment

It is assumed that there will be no untrusted users or software on the SecurVantage™ hosts. SecurVantage™ relies upon the underlying operating system platforms to provide reliable time stamps and to protect the SecurVantage™ hosts from other interference or tampering. SecurVantage™ relies upon third-party encryption software to provide protection of data transfer between TOE components and for a trusted communication path between authorized administrators and the TOE. SecurVantage™ Enterprise Reporting Warehouse is a third party product and therefore is considered part of the TOE environment. The underlying operating system software and hardware, Tomcat, Apache, OpenSSL, and PureTLS encryption software are part of the TOE environment.

The TOE security environment can be categorized as follows:

- **Cryptographic Support** - The TOE relies on the IT environment to provide cryptographic support and the cryptographic module. This includes OpenSSL and PureTLS.
- **Partial Protection of TSF** - SecurVantage™ relies on the underlying OS to provide security capabilities for the TOE's protection. For the TOE's own protection the OS includes requirements that relate to the integrity of the TSF. These include SFP domain separation, non-bypassability, and a reliable time-stamp.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1 TOE Usage Assumptions

TOE Intended Usage Assumptions		
1	A.Dynmic	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
2	A.Trusted	There will be no untrusted users of the TOE and no untrusted software loaded on the TOE host platforms.

Table 3-2 TOE Physical Assumptions

TOE Physical Assumptions		
3	A.Protct	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
4	A.Locate	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

Table 3-3 TOE Personnel Assumptions

TOE Personnel Assumptions		
5	A.Admin	The administrator is trusted to correctly configure the TOE.
6	A.Manage	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
7	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.
8	A.Password	Administrators and users will follow the guidance provided by the TOE documentation for choosing good passwords.

3.2 Threats

The following are threats identified for both the TOE and the IT System it monitors. The TOE itself has threats and is also responsible for addressing threats to the environment in which it resides.

The attacker for all threats is assumed to have an unsophisticated level of expertise, with access to standard equipment and public information.

Table 3-4 Threats

Threats		
1	T.Abuse	An undetected compromise of the TOE may occur as a result of an authorized user of the TOE (intentionally or otherwise) performing actions the individual is authorized to perform.
2	T.Access	An authorized user of the TOE may access information or resources without having permission from the person who owns, or is responsible for, the information or resource.
3	T.BadPassword	Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorized access to the TOE.
4	T.Bypass	An attacker may attempt to bypass TSF security functions.
5	T.BypassDisclosure	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
6	T.BypassIntegrity	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

Threats		
7	T.DataLoss	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
8	T.Halt	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
9	T.ImpConfig	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
10	T.OFlows	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
11	T.Mismanage	Administrators may make errors in the management of security functions and TSF data, if administrative tools are not provided. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.
12	T.Privil	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
13	T.RemoteAttack	A threat agent may be able to view, modify, and/or delete security-related information that is sent between a remotely located Authorized Administrator and the TOE.
14	T.Tamper	An attacker may attempt to modify TSF programs and data.
15	T.Transmit	TSF data may be disclosed or modified by an attacker while being transmitted between TOE components.
16	T.Undetect	Attempts by an attacker to violate the security policy may go undetected.

3.3 Policies

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

Table 3-5 Organizational Security Policies

Organizational Security Policies		
1	P.Accact	Users of the TOE shall be accountable for their actions within the system.
2	P.Access	All data collected and produced by the TOE shall only be used for authorized purposes.
3	P.Analyz	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to system data and appropriate response actions taken.
4	P.Detect	Static configuration information must be collected that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, unauthorized access, or malicious activity of IT System assets.
5	P.Manage	The TOE shall only be managed by authorized users.

4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 Security Objectives for the TOE

The following are the TOE security objectives:

Table 4-1 TOE Security Objectives

TOE Security Objectives		
1	O.Access	The TOE must allow authorized users to access only appropriate TOE functions and data.
2	O.Admin	The TOE must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions.
3	O.Audit	The TOE must record audit records for data accesses and use of the system functions.
4	O.BruteForce	The TOE must lock user account after a number of consecutive failed attempts in a given window of time
5	O.DataIntegrity	The TOE must ensure the integrity of all audit and system data.
6	O.IDAnlz	The TOE must accept data and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
7	O.IDAuth	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
8	O.IDSens	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, unauthorized access, or malicious activity of IT system assets.
9	O.ManageData	The TOE must be able to store and maintain properties of users and resources including information to support primary and application authentication.
10	O.MultipleAuthen	The TOE must provide multiple authentication mechanisms.
11	O.NonBypass	The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.
12	O.OFlows	The TOE must appropriately handle potential audit and system data storage overflows.
13	O.PartialDomainSep	The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.
14	O.PasswordQual	The TOE must be able to specify password rules strong enough to deter password guessing.
15	O.ProtectAuth	The TOE will provide protected authentication feedback.
16	O.Revoke	The TOE will allow authorized users to revoke security attributes within the TSC.
17	O.Reauthenticate	The TOE requires reauthentication to change user's own password
18	O.Roles	The TOE must support multiple administrative roles.

4.2 Security Objectives for the Environment

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

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Table 4-2 Security Objectives for the IT Environment

IT Environment Security Objectives		
1	OE.ComIntegrity	The IT environment must protect the integrity of data transmitted within the TOE via digital signature. Upon receipt of data from a component (Studio, Monitor, Monitor LE, and Enterprise, or Enterprise Reporting Gateway) of the TOE, the IT environment must verify that the received data accurately represents the data that was originally transmitted.
2	OE.Confidentiality	The IT environment must protect the confidentiality of data transmitted between the major components (Studio, Monitor, Monitor LE, and Enterprise, and Enterprise Reporting Gateway) of the TOE via the use of encryption. Communication must be protected, either locally or remotely, from being revealed. When communication occurs over a network, it must be encrypted by the environment. Additionally, the IT environment must protect the confidentiality of its dialogue with an authorized administrator, either locally or remotely, via encryption.
3	OE.NonBypass	The IT environment must ensure that its protection mechanisms cannot be bypassed.
4	OE.PartialDomainSep	The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.
5	OE.Time	The IT environment must provide reliable time stamps.

4.2.2 Non-IT Security Objectives

The Non-IT Security Objectives are as follows:

Table 4-3 Non-IT Security Objectives

Non-IT Security Objectives		
6	ON.Creden	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner that is consistent with IT security.
7	ON.Install	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.
8	ON.Operations	There must be procedures in place in order to ensure that the TOE will be managed and operated in a secure manner.
9	ON.Password	Personnel working as authorized administrators and users must follow the TOE

Non-IT Security Objectives		
		guidance about choosing good passwords.
10	ON.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
11	ON.Phycal	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
12	ON.NoUntrusted	The authorized administrator will ensure that there are no untrusted users and no untrusted software on the SecurVantage Server hosts.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

The TOE security functional requirements are listed in Table 5-1. They are all taken from Part 2 of the Common Criteria.

Table 5-1 Functional Components

("*" refers to all iterations of a component)

TOE Security Functional Components		
No.	**Component**	**Component Name**
1	FAU_ARP.1	Security alarms
2	FAU_GEN.1*	Audit data generation
3	FAU_SAA.3	Simple attack heuristics
4	FAU_SAR.1*	Audit review
5	FAU_SAR.2*	Restricted audit review
6	FAU_SAR.3	Selectable audit review
7	FAU_SEL.1	Selective audit
8	FAU_STG.2*	Guarantees of audit data availability
9	FAU_STG.4*	Prevention of audit data loss
10	FDP_ACC.2*	Complete access control
11	FDP_ACF.1*	Security attribute based access control
12	FIA_AFL.1*	Authentication failure handling
13	FIA_ATD.1*	User attribute definition
14	FIA_SOS.1*	Verification of secrets
15	FIA_UAU.2*	User authentication before any action
16	FIA_UAU.5*	Multiple authentication mechanisms
17	FIA_UAU.6*	Re-authenticating
18	FIA_UAU.7*	Protected authentication feedback
19	FIA_UID.2*	User identification before any action

TOE Security Functional Components		
No.	**Component**	**Component Name**
20	FMT_MOF.1*	Management of security functions behavior
21	FMT_MSA.1*	Management of security attributes
22	FMT_MSA.3*	Static attribute initialization
23	FMT_MTD.1*	Management of TSF data
24	FMT_MTD.2*	Management of limits on TSF data
25	FMT_REV.1	Revocation
26	FMT_SMF.1*	Specification of management functions
27	FMT_SMR.1*	Security roles
28	FPT_ITA.1	Inter-TSF availability within a defined availability metric
29	FPT_RVM_EXP.1*	Non-bypassability of the TSP
30	FPT_SEP_EXP.1*	TSF domain separation
31	FTA_SSL.3*	TSF-initiated termination
32	FTA_TSE.1*	TOE session establishment

Operations on IT security requirements are identified as follows:

- Iteration – component number is distinguished by appending a number, preceded by a hyphen. Example: FIA_UAU.7.1-1. Iterations of elements within a component are labeled with numbers in brackets, e.g., FIA_UAU.7.1.1-1 [1] and FIA_UAU.7.1.1-1 [2].
- Assignment – text is bolded italics and enclosed in brackets. Example: FAU_ARP.1.1 The TSF shall take [***action to send an email or SNMP message if a critical event is generated and the system is set to send such an email or SNMP message; otherwise no action***] upon detection of a potential security violation.
- Selection – text is bolded italics and enclosed in brackets. Example: FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***remote and local***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
- Refinement – text is underlined, bolded italics. Example: FPT_STM.1.1 The ***IT environment*** shall be able to provide reliable time stamps for its own use

5.1.1 SFRs for Studio, Monitor, and Enterprise are in section 5.1.1. SFRs for Enterprise Reporting Gateway are in section 5.1.2

5.1.1.1 Class FAU: Security Audit

FAU_ARP.1 Security Alarms

Hierarchical to: No other components

FAU_ARP.1.1 The TSF shall take ***[action to send an email or SNMP message when the system is configured to do so only when***:

A critical violation is generated
A threshold of violation compliance per domain is crossed
otherwise no action] upon detection of a potential security violation.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_GEN.1-1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1-1 The TSF shall be able to generate an audit record of the following auditable events:

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

b) All auditable events for the [***not specified***] level of audit; and

c) ***[the following auditable events:***

All IPv4 network and IPv4 protocol events of the monitored network(s) (unless rate limits are exceeded); and
Application log records recording the times and number of events in which rate limits were exceeded]

FAU_GEN.1.2-1 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [service, protocol, protocol attributes, or customer-specified policy attributes (hostname, service name, outcome name, event severity and owner)].

Application note: For rate limiting, the application logs number of packets received versus those processed.

Application note: Every event is associated with only one severity. Event severity is assigned one of the following levels: Critical, High, Medium, Warning, Monitor, Informational, or Ok.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAA.3 Simple attack heuristics

Hierarchical to: FAU_SAA.1

FAU_SAA.3.1 TSF shall be able to maintain an internal representation of the following signature events [***default and customer-specified protocol usage policy and system connection profile***] that may indicate a violation of the TSP.

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [***network traffic***].

FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

Dependencies: No dependencies

FAU_SAR.1-1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1-1 [1] The TSF shall provide [***Operator, Analyst, and Developer***] with the capability to read [***Event Data***] from the audit records.

FAU_SAR.1.1-1 [2] The TSF shall provide [***Operator, Analyst, and Developer***] with the capability to read [***Alerts***] from the audit records.

FAU_SAR.1.1-1 [3] The TSF shall provide [***SV Manager***] with the capability to read [***Application Log data***] from the audit records.

FAU_SAR.1.1-1 [4] The TSF shall provide [***Account Manager and SV Manager***] with the capability to read [***User Log data***] from the audit records.

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2-1 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1-1 The TSF shall prohibit all users read access to the audit records, except those users who have been granted explicit read-access.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform [***searches, sorting, and ordering***] of audit data based on [***event severity and event type***].

Dependencies: FAU_SAR.1 Audit review

Application note: Every event is associated with only one severity. Event Severity is one of the following levels: Critical, High, Medium, Warning, Monitor, or Ok.

FAU_SEL.1 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [host identity and event type]

b) [service, protocol, protocol attributes, or customer-configured policy attributes (hostname, service name, outcome name, event severity and owner)].

Dependencies:

- FAU_GEN.1 Audit data generation
- FMT_MTD.1 Management of TSF data

Application note: Every event is associated with only one severity. Event Severity is one of the following levels: Critical, High, Medium, Warning, Monitor, or Ok.

FAU_STG.2-1 Guarantees of audit data availability

Hierarchical to: FAU_STG.1

FAU_STG.2.1-1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2-1 The TSF shall be able to [***prevent***] unauthorized modifications to the audit records in the audit trail.

FAU_STG.2.3-1 The TSF shall ensure that [***4 gigabytes of***] audit records will be maintained when the following conditions occur: [***audit storage exhaustion***].

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.4-1 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1-1 The TSF shall [***overwrite the oldest stored audit records***] and [***take no other actions***] if the audit trail storage is full.

Dependencies: FAU_STG.1 Protected audit trail storage

5.1.1.2 Class FDP: User Data Protection

FDP_ACC.2-1 Complete access control

Hierarchical to: FDP_ACC.1

FDP_ACC.2.1-1 The TSF shall enforce the [Table 5-2 SecurVantageTM User Access Policy] on [Subjects and Objects listed in Table 5-2 SecurVantageTM User Access Policy] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2-1 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Dependencies: FDP_ACF.1 Security attribute based access control

Table 5-2 SecurVantage™ User Access Policy

User Access Policy: Roles/Subjects (Monitor and Enterprise)					
Objects	Operator	Analyst	Developer	SV Manager	Account Manager
Event Data	View	View	View		
Machines	View Status	View Status	View Status Start/Restart Stop	View Status Start/Restart Stop Configure	View Status
DMEs		Download	Download		
User Access					Manage
Policy History	View	View	View		
Policies		Extract	Upload Revert Extract		
Alerts	Manage	Manage	Manage		
Application Logs				View	
User Logs					View

FDP_ACF.1-1 Security attribute-based access control

Hierarchical to: No other components.

FDP_ACF.1.1-1 The TSF shall enforce the [Table 5-2 SecurVantageTM User Access Policy] to objects based on the following: [See Table 5-2 SecurVantageTM User Access Policy].

FDP_ACF.1.2-1 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***see Table 5-2 SecurVantageTM User Access Policy***].

FDP_ACF.1.3-1 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [***no additional rules***].

FDP_ACF.1.4-1 The TSF shall explicitly deny access of subjects to objects based on the following rules: [***no additional explicit denial rules***].

Dependencies:

- FDP_ACC.1 Subset access control

- FMT_MSA.3 Static Attribute initialization

5.1.1.3 Class FIA: Identification and Authentication

FIA_AFL.1-1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1-1 The TSF shall detect when [***an SVManager configurable positive integer within 0-100***] unsuccessful authentication attempts occur related to [***login***].

FIA_AFL.1.2-1 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall:

[***not allow the credential to authenticate to the application for period of time configurable by the SV Manager ;***
leave an audit trail in the user application log]

Dependencies: FIA_UAU.1 Timing of authentication

FIA_ATD.1-1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1-1 The TSF shall maintain the following list of security attributes belonging to individual users: [***user name, roles, hash of the password or certificate, type of authentication***].

Dependencies: No dependencies

FIA_SOS.1-1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1-1 The TSF shall provide a mechanism to verify that secrets meet [***a password policy of***
Minimum of 8 characters;
Maximum of 64 characters;
At least one lower case character;
At least one upper case character; and
At least one numeric character]

Dependencies: No dependencies

FIA_UAU.2-1 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1-1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.5-1 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1-1 The TSF shall provide [***password mechanism and certificate verification***] to support user authentication.

FIA_UAU.5.2-1 The TSF shall authenticate any user's claimed identity according to the [***hash of the password or the certificate fingerprint match***].

Dependencies: No dependencies

FIA_UAU.6-1 Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1-1 The TSF shall re-authenticate the user under the conditions [***for changing their own password***]

Dependencies: No dependencies

FIA_UAU.7-1 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1-1 [1] The TSF shall provide only [***a confirmation of user name and asterisks for password-based authentication***] to the user while the authentication is in progress.

FIA_UAU.7.1-1 [2] The TSF shall provide only [***certificate dialog box for certificate-based authentication***] to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID.2-1 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1-1 The TSF shall require each user to be self-identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

5.1.1.4 Class FMT: Security Management

FMT_MOF.1-1 Management of security functions behavior

Hierarchical to: No other components

FMT_MOF.1.1-1 [1] The TSF shall restrict the ability to [***modify the behavior of***] the functions [***account lockout***] to [***SV Manager***]

FMT_MOF.1.1-1 [2] The TSF shall restrict the ability to [***modify the behavior of***] the functions [***auditing***] to [***Developer***]

Dependencies:

- FMT_SMF.1 Specification of management functions
- FMT_SMR.1 Security roles

FMT_MSA.1-1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1-1 The TSF shall enforce the [**Table 5-2 SecurVantageTM User Access Policy**] to restrict the ability to [**query, modify, or delete**] the security attributes [**user identity, roles, password- or certificate-based authentication**] to [**Account Manager**].

Dependencies:

- [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]
- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

FMT_MSA.3-1 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1-1 The TSF shall enforce the [**Table 5-2 SecurVantageTM User Access Policy**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2-1 The TSF shall allow the [***Account Manager***] to specify alternative initial values to override the default values when an object or information is created.

Dependencies:

- FMT_MSA.1 Management of security attributes
- FMT_SMR.1 Security roles

FMT_MTD.1-1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1-1 [1] The TSF shall restrict the ability to [***query***] the [***Event Data***] to [***Operator, Analyst and Developer***].

FMT_MTD.1.1-1 [2] The TSF shall restrict the ability to [***query***] the [***Machines Status***] to [***Operator, Analyst, Developer, SV Manager, and Account Manager***].

FMT_MTD.1.1-1 [3] The TSF shall restrict the ability to [***modify***] the [***Machines Status***] to [***SV Manager***].

FMT_MTD.1.1-1 [4] The TSF shall restrict the ability to [***query***] the [***DMEs***] to [***Analyst, SV Manager and Developer***].

FMT_MTD.1.1-1 [5] The TSF shall restrict the ability to [***query, modify, delete***, ***or create***] the [***User Access***] to [***Account Manager***].

FMT_MTD.1.1-1 [6] The TSF shall restrict the ability to [***query***] the [***Policy History***] to [***Operator, Analyst, and Developer***].

FMT_MTD.1.1-1 [7] The TSF shall restrict the ability to [***query***] the [***Policies***] to [***Analyst, and Developer***].

FMT_MTD.1.1-1 [8] The TSF shall restrict the ability to [***modify, delete, or create***] the [***Policies***] to [***Developer***].

FMT_MTD.1.1-1 [9] The TSF shall restrict the ability to [***manage***] the [***Alerts***] to [***Operator, Analyst and Developer***].

FMT_MTD.1.1-1 [10] The TSF shall restrict the ability to [***query***] the [***Application Logs***] to [***SV Manager***].

FMT_MTD.1.1-1 [11] The TSF shall restrict the ability to [***query***] the [***User Logs***] to [***Account Manager***].

Dependencies:

- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles

FMT_MTD.2-1 Management of limits on TSF data

Hierarchical to: No other components.

FMT_MTD.2.1-1 [1] The TSF shall restrict the specification of the limits for [***account lockout***] to [***SV Manager***]

FMT_MTD.2.1-1 [2] The TSF shall restrict the specification of the limits for [***compliance threshold***] to [***SV Manager***]

FMT_MTD.2.2-1 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [***lock user account; send snmp trap or email***]

Dependencies:

- FMT_MTD.1 Management of TSF data
- FMT_SMR.1 Security roles

FMT_REV.1 Revocation

Hierarchical to: No other components.

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the [***users, subjects, or objects***] within the TSC to [***Account Manager***].

FMT_REV.1.2 The TSF shall enforce the rules [***at the next login attempt***].

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1-1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1-1 The TSF shall be capable of performing the following security management functions:

[query Event Data,
query or modify Machines Status,
query DMEs,
query, modify, delete, or create User Access,
query Policy History,
query, modify, delete, or create Policies,
query Alerts,
query Application Logs,
query User Logs
set lock account policies]

Dependencies: No Dependencies

FMT_SMR.1-1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1-1 The TSF shall maintain the roles [***Operator, Analyst, Developer, SV Manager, and Account Manager***].

FMT_SMR.1.2-1 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.1.5 Class FPT: Protection of the TSF

FPT_ITA.1 Inter-TSF availability within a defined availability metric

Hierarchical to: No other components.

FPT_ITA.1.1 The TSF shall ensure the availability of [***critical alerts***] provided to a remote trusted IT product within [***5 minutes***] given the following conditions [***web interface not available and infrastructure to trusted IT system is accessible***]

Dependencies: No dependencies

FPT_RVM_EXP.1-1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-1 The TSF, when invoked by the underlying host OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

FPT_SEP_EXP.1-1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_EXP.1.1-1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI .

FPT_SEP_EXP.1.2-1 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.1.1.6 Class FTA: TOE access

FTA_SSL.3-1 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1-1 The TSF shall terminate an interactive session after [***30 minutes of user inactivity***]

Dependencies: No dependencies

FTA_TSE.1-1 TOE session establishment

Hierarchical to: No other components.

FTA_TSE.1.1-1 The TSF shall be able to deny session establishment based on [***number of consecutive failed login attempts***]

Dependencies: No dependencies

5.1.2 SFRs for Enterprise Reporting Gateway are below:

5.1.2.1 Class FAU: Security Audit

FAU_GEN.1-2 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1-2 The TSF shall be able to generate an audit record of the following auditable events:

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

b) All auditable events for the [not specified] level of audit; and

c) [***the following auditable events***:

Login/logout of users
Create, edit, and delete user accounts
Add, edit, or remove Enterprises
Change user's password]

FAU_GEN.1.2-2 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***none***].

Application note: The ER Gateway provides two types of diagnostic logs which enable an authorized user to examine system traffic and performance on the ER Gateway—User Logs and Application Logs.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1-2 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1-2 [1]The TSF shall provide [***the ER Account Manager***] with the capability to read [***the User activity log information***] from the audit records.

FAU_SAR.1.1-2 [2]The TSF shall provide [***the ER SV Manager***] with the capability to read [***the Gateway log information and user logs***] from the audit records.

FAU_SAR.1.2-2 The TSF shall provide the audit record information in a manner suitable interpretation by the user..

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2-2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1-2 The TSF shall prohibit read access of audit records to all users except those who have been explicitly granted read access.

Dependencies: FAU_SAR.1 Audit review

FAU_STG.2-2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1

FAU_STG.2.1-2 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2-2 The TSF shall be able to [***prevent***] unauthorized modifications to the audit records in the audit trail.

FAU_STG.2.3-2 The TSF shall ensure that [***800 megabytes of***] audit records will be maintained when the following conditions occur:[a***udit storage exhaustion***].

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.4-2 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1-2 The TSF shall [***overwrite the oldest stored audit records***] and [***take no other actions***] if the audit trail storage is full.

Dependencies: FAU_STG.1 Protected audit trail storage

5.1.2.2 Class FDP: User Data Protection

FDP_ACC.2-2 Complete access control

Hierarchical to: FDP_ACC.1

FDP_ACC.2.1-2 The TSF shall enforce the [***SecurVantage™ ER User Access Policy]*** on [***Subjects and Objects listed in Table 5-3 SecurVantageTM ER User Access Policy***] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2-2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Dependencies: FDP_ACF.1 Security attribute based access control.

Table 5-3 SecurVantage™ ER User Access Policy

ER User Access Policy: Roles/Subjects		
Objects	ER SV Manager	ER Account Manager
Machines	View Status Start/Restart Stop Configure	View Status
User Access		Manage
Application Logs	View	
User Logs		View

FDP_ACF.1-2 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1-2 TSF shall enforce the [***SecurVantage™ ER User Access Policy***] to objects based on the following: [***See Table 5-3 SecurVantageTM ER User Access Policy***].

FDP_ACF.1.2-2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***See Table 5-3 SecurVantageTM ER User Access Policy***].

FDP_ACF.1.3-2 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [***no additional rules***].

FDP_ACF.1.4-2 The TSF shall explicitly deny access of subjects to objects based on the following rules: [***no additional explicit denial rules***].

Dependencies:

- FDP_ACC.1 Subset access control
- FMT_MSA.3 Static Attribute initialization

5.1.2.3 Class FIA: Identification and Authentication

FIA_AFL.1-2 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1-2 The TSF shall detect when [***an ER SV Manager configurable positive integer within 0-100***] unsuccessful authentication attempts occur related to [***login***].

FIA_AFL.1.2-2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall:

[***not allow the credential to authenticate to the application for a period of time configurable by the ER SV Manager and leave an audit trail in the user application log***]

Dependencies: FIA_UAU.1 Timing of authentication

FIA_ATD.1-2 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1-2 The TSF shall maintain the following list of security attributes belonging to individual users: [***user name, roles, hash of the password or certificate, type of authentication***].

Dependencies: No dependencies

FIA_SOS.1-2 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1-2 The TSF shall provide a mechanism to verify that secrets meet [***a password policy of***

Minimum of 8 characters;
Maximum of 64 characters;
At least one lower case character;

At least one upper case character; and
At least one numeric character]

Dependencies: No dependencies

FIA_UAU.2-2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1-2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.5-2 Multiple authentication mechanisms

Hierarchical to: No other components.

FIA_UAU.5.1-2 The TSF shall provide [***password mechanism and certificate verification***] to support user authentication.

FIA_UAU.5.2-2 The TSF shall authenticate any user's claimed identity according to the [***hash of the password or the certificate fingerprint match***].

Dependencies: No dependencies

FIA_UAU.6-2 Re-authenticating

Hierarchical to: No other components.

FIA_UAU.6.1-2 The TSF shall re-authenticate the user under the conditions [***for changing their own password***]

Dependencies: No dependencies

FIA_UAU.7-2 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1-2 The TSF shall provide only [***a confirmation of user name and asterisks for password-based authentication***] to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID.2-2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1-2 The TSF shall require each user to be self-identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: No dependencies.

5.1.2.4 Class FMT: Security Management

FMT_MOF.1-2 Management of Security Functions Behavior

Hierarchical to: No other components.

FMT_MOF.1.1-2 The TSF shall restrict the ability to [***determine the behavior of***] the functions [***listed in Table 5-5***] to [***the authorized roles identified in Table 5-5***].

Dependencies:

- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

FMT_MSA.1-2 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1-2 The TSF shall enforce the [***SecurVantage™ ER User Access Policy***] to restrict the ability to [***query, modify, delete, [and other operations as specified in Table 5-4] the security attributes as specified in Table 5-4***] to [***the role as specified in Table 5-4***].

Dependencies: [FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

Table 5-4 Management of Security Attributes

Subjects with roles of the following:	Allowed Action on Specified Security Attributes
ER Account Manager	• Assign new users to roles and modify passwords (own and others) • Query, create, edit, and delete user name
ER SV Manager	• change own password

FMT_MSA.3-2 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1-2 The TSF shall enforce the [***SecurVantage™ ER User Access Policy***] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2-2 The TSF shall allow the [***ER Account Manager***] to specify alternative initial values to override the default values when an object or information is created.

Dependencies:

- FMT_MSA.1 Management of security attributes
- FMT_SMR.1 Security roles

FMT_MTD.1-2 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1-2 The TSF shall restrict the ability to [***query, modify, delete***, [***see operations specified in Table 5-5***]] the [***TSF Data as specified in Table 5-5 to*** [***the role as specified in Table 5-5***].

Dependencies:

- FMT_SMR.1 Security roles
- FMT_SMF.1 Specification of Management Functions

Table 5-5 Management of TSF Data

Security Function	Operation	TSF data	Authorized Role
Security Audit	View	Application logs	ER SV Manager
Security Audit	View	User Activity Log	ER Account Manager
Identification and Authentication	Query, create, edit, and delete	User name	ER Account Manager
Identification and Authentication	Change	User password	ER Account Manager
Security Management	Assign users to	Roles	ER Account Manager
Security Management	View	ER Gateway status	ER SV Manager
Security Management	Start, stop, and restart	ER Gateway	ER SV Manager
Security Management	Add, edit, or remove	Enterprises	ER SV Manager
Security Management	Check	Connectivity to an Enterprise	ER SV Manager

FMT_MTD.2-2Management of limits on TSF data

Hierarchical to: No other components.

FMT_MTD.2.1-2 The TSF shall restrict the specification of the limits for [***account lockout***] to [***ER SV Manager***]

FMT_MTD.2.2-2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [***lock user account; send SNMP trap or email***]

Dependencies:

- FMT_MTD.1 Management of TSF data
- FMT_SMR.1 Security roles

FMT_SMF.1-2 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1-2 The TSF shall be capable of performing the following security management functions: **[**

- ***determine the behavior of the functions listed in Table 5-5 to the authorized roles identified in Table 5-5,***
- ***query, modify, delete, and create as specified in Table 5-4 the security attributes as specified in Table 5-4 (see FMT_MSA.1-2),***
- ***query, modify, delete, and create as specified in Table 5-5 and the TSF Data as specified in Table 5-5(See FMT_MTD.1-2)].***

Dependencies: No Dependencies

FMT_SMR.1-2 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1-2 The TSF shall maintain the roles [***ER SV Manager and ER Account Manager***].

FMT_SMR.1.2-2 The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

5.1.2.5 Class FPT: Protection of the TSF

FPT_RVM_EXP.1-2 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-2 The TSF, when invoked by the underlying host OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

FPT_SEP_EXP.1-2 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_EXP.1.1-2 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

FPT_SEP_EXP.1.2-2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.1.2.6 Class FTA: TOE access

FTA_SSL.3-2 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1-2 The TSF shall terminate an interactive session after a [***30 minutes of user inactivity***]

Dependencies: No dependencies

FTA_TSE.1-2 TOE session establishment

Hierarchical to: No other components.

FTA_TSE.1.1-2 The TSF shall be able to deny session establishment based on [***number of consecutive failed login attempts***]

Dependencies: No dependencies

5.2 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 3 (EAL3) taken from Part 3 of the Common Criteria. None of the assurance component is redefined. The assurance components are listed in Table 5-6.

Table 5-6 EAL3 Assurance Components

EAL3 Assurance Class	EAL3 Assurance Components	
Configuration management	ACM_CAP.3	Authorization controls
	ACM_SCP.1	TOE CM coverage
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design

EAL3 Assurance Class	EAL3 Assurance Components	
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.3 Security requirements for the IT Environment

Table 5-7 Functional Components for the IT Environment

No.	Component	Component Name
33	FPT_ITT.1	Basic internal TSF data transfer protection
34	FPT_RVM_EXP.1-3	Non-bypassability of the TSP
35	FPT_SEP_EXP.1-3	TSF domain separation
36	FPT_STM.1	Reliable time stamps
37	FTP_TRP.1	Trusted path

5.3.1 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

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

Dependencies: No dependencies

Application note: The TOE relies on the IT Environment to secure the network path between TOE Components.

FPT_RVM_EXP.1-3 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-3 The ***IT environment*** shall ensure that the Operating System Security Policy enforcement functions are invoked and succeed before each function within the Operating System's Scope of Control is allowed to proceed.

Dependencies: No dependencies

FPT_SEP_EXP.1-3 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_EXP.1.1-3 The ***IT environment*** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface.

FPT_SEP_EXP.1.2-3 The ***IT environment*** shall enforce separation between the security domains of subjects in the Operating System's Scope of Control.

Dependencies: No dependencies

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

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

Dependencies: No dependencies

5.3.2 Class FTP: Trusted Path/Trust Channel

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

FTP_TRP.1.1 The ***IT environment*** shall provide a communication path between ***the TSF*** and [***remote and local***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The ***IT environment*** shall permit [***local users and remote users***] to initiate communication via the trusted path.

FTP_TRP.1.3 The ***IT environment*** shall require the use of the trusted path for [initial user authentication and [***accessing Live Data, Analysis Data, Configuration Data, User Access Data, Policy History, Policy, New Alerts, and Alert History***]].

Dependencies: No dependencies

5.4 Strength of Function

The minimum strength of function level for the TOE security functional requirements is SOF-basic. This applies to the FIA_SOS.1*, verification of secrets, security functional requirements.

6 TOE Summary Specification

6.1 IT Security Functions

6.1.1 Overview

The following sections describe the IT Security Functions in each of the SecurVantage™ components.

6.1.2 SecurVantage™ Studio

Studio Analyze Data Function	
S-AD-1	Studio provides users with the capability to read information from the audit records according to the Table 5-2 SecurVantageTM User Access Policy. (FAU_SAR.1.1-1 [1], FAU_SAR.1.1-1 [2], FAU_SAR.1.1-1 [3], FAU_SAR.1.1-1 [4], FAU_SAR.1.2-1) • Operator, Analyst, and Developer can read live Event Data • Studio provides the audit records in a manner suitable for the user to interpret the information.
S-AD-2	Studio prohibits all users read access to the audit records, except those that have been granted explicit read access. (FAU_SAR.2.1-1)
S-AD-3	Studio provides the ability to perform searches, sorting, and ordering of the audit data, based on event severity and event type. (FAU_SAR.3)
S-AD-4	Studio provides users with the capability to read event data and alerts from the local audit record as DME files. (FAU_SAR.1.1-1 [1], FAU_SAR.1.1-1 [2])

Studio User Login Function	
S-UL-1	Studio provides the certificate dialog box when certificate-based authentication is used. (FIA_UAU.7.1-1 [2])
S-UL-2	Studio protects password display with asterisks when username/password authentication is used. (FIA_UAU.7.1-1 [1])

Studio Create Policy Function	
S-P-1	Studio provides users with the capability of select what type of events to audit and what severity to be assigned when such events occurred in the network (FAU_SEL.1)

6.1.3 SecurVantage™ Monitor

Monitor Manage User Access Function	
M-MUA-1	Monitor maintains the following information for each user: user name, hash of the password or certificate, roles, and whether authentication is password or certificate based. (FIA_ATD.1.1-1)
M-MUA-2	Monitor requires that user passwords be: • Minimum of 8 characters in the password • Maximum of 64 characters • At least one lower case character • At least one upper case character • At least one numeric character (FIA_SOS.1-1)
M-MUA-3	Monitor enforces the SecurVantage™ User Access Policy (See Table 5-2 SecurVantageTM User Access Policy) (FDP_ACC.2.1-1, FDP_ACC.2.2-1) (FDP_ACF.1.1-1, FDP_ACF.1.2-1, FDP_ACF.1.3-1, FDP_ACF.1.4-1)
M-MUA-4	Monitor restricts the ability to query, modify, or delete the username, roles, and password- or certificate-based authentication security attribute to Account Manager. (FMT_MSA.1.1-1)
M-MUA-5	Monitor provides restrictive default values for security attributes as specified in Table 5-2 SecurVantageTM User Access Policy and allows the Account Manager to specify alternative initial values. (FMT_MSA.3.1-1, FMT_MSA.3.2-1)
M-MUA-6	Monitor restricts the ability to access data as specified in Table 5-2 SecurVantageTM User Access Policy. (FMT_MTD.1.1-1 [1], FMT_MTD.1.1-1 [2], FMT_MTD.1.1-1 [3], FMT_MTD.1.1-1 [4], FMT_MTD.1.1-1 [5], FMT_MTD.1.1-1 [6], FMT_MTD.1.1-1 [7], FMT_MTD.1.1-1 [8], FMT_MTD.1.1-1 [9], FMT_MTD.1.1-1 [10], FMT_MTD.1.1-1 [11])
M-MUA-7	Monitor restricts the ability to revoke security attributes associated with users, subjects, and objects to Account Manager. (FMT_REV.1)
M-MUA-8	Monitor is capable of providing the security management functions as specified in Table 5-2 SecurVantageTM User Access Policy. (FMT_SMF.1.1-1)
M-MUA-9	Monitor maintains the roles Operator, Analyst, Developer, SV Manager, and Account Manager. (FMT_SMR.1.1-1, FMT_SMR.1.2-1)
M-MUA-10	Monitor ensures that the Table 5-2 SecurVantageTM User Access Policy is invoked and succeeds before each function is allowed to proceed. (FPT_RVM_EXP.1.1-1)
M-MUA-11	Monitor maintains a security domain for its own execution and enforces separation between security domains of users initiating actions through its own TSFI. (FPT_SEP_EXP.1.1-1, FPT_SEP_EXP.1.2-1)
M-MUA-12	Monitor allows SV Manager to set and configure the parameters of the account lockout feature (FMT_MOF.1,1-1 [1], FMT_MOF.1,1-1 [2]) (FMT_MTD.2.1-1 [1], FMT_MTD.2.1-1 [2], FMT_MTD.2.2-1)

Monitor User Login Function	
M-UL-1	Monitor requires each user to self identify before being allowed to perform any other actions. (FIA_UID.2.1-1)
M-UL-2	Monitor requires each user to successfully authenticate with either a password or certificate before being allowed any other actions. (FIA_UAU.2.1-1)
M-UL-3	The hash of the given password must match the stored hash of the user password. The given certificate must produce the same SHA-1 hash as the stored user hash. (FIA_UAU.5.1-1, FIA_UAU.5.2-1)
M-UL-4	Monitor provides only confirmation of user name and asterisks for password when password authentication is used. (FIA_UAU.7.1-1 [1], FIA_UAU.7.1-1 [2])
M-UL-5	Monitor locks user accounts when consecutive failed login attempts are performed on a given account (FIA_AFL.1.1-1, FIA_AFL.1.2-1) (FTA_TSE.1.1-1)
M-UL-6	Users need to reauthenticate before changing their own passwords (FIA_UAU.6.1-1)
M-UL-7	Users session is terminated after 30 minutes of inactivity (FTA_SSL.3.1-1)
M-UL-8	Monitor uses X509 certificates to authenticate each machine in the system. It uses this authentication to enable connections between machines. Monitor authenticates any SecurVantage™ component's claimed identity according to the certificate fingerprint match. (FIA_UAU.5.1-1, FIA_UAU.5.2-1)

Monitor Collect Data Function	
M-CD-1	Monitor sends an email or SNMP message if a critical event is generated even when web interface component is down (FAU_ARP.1) (FPT_ITA.1)

Monitor Collect Data Function	
M-CD-2	Monitor is able to generate audit records. (FAU_GEN.1.1-1, FAU_GEN.1.2-1) Startup and shutdown of the audit functions is recorded in the User Log. Network and protocol events are recorded in the Monitor database. Network and protocol events describe flows of network traffic based on IPv4 datagrams. For network and protocol events, the following is recorded: • Host identity • Service • Protocol • Protocol attributes The following customer-specified policy attributes may also be recorded: • Hostname • Service name • Outcome name • Event severity • Owner Monitor records based on the following conditions: • Legal IPv4 datagrams • Ethernet 2 encapsulation (length <= 1514 bytes) • Gigabit Ethernet Jumbo frames are not supported Monitor does not check IP, UDP and TCP checksums Reassembly of IP fragment and TCP segments is based on a first-received-is-used rule. A high performance Monitor captures 100% data: • at a rate between 150 - 325 Mbits per second; • for a typical policy that yields around 4% violations; • in a network with a typical network traffic distribution ranging from transaction processing (150Mbits/s) to service networks (325Mbits/s). Monitor can handle higher data rates and more complex policies by sampling the observed network traffic. A Monitor LE captures 100% data: • at a rate less than 100 Mbits per second; • for a typical policy that yields around 4% violations; • in a network with a typical network traffic distribution.
M-CD-3	Monitor maintains an internal representation of signature events as defined in the customer-specified policy that may indicate a violation of the policy. Monitor is able to indicate an imminent violation of the policy when an event is found to match a signature event. (FAU_SAA.3)

Monitor Collect Data Function	
M-CD-4	Monitor is able to include or exclude auditable events from the set of audited events based on specific attributes. (FAU_SEL.1) These attributes include the following: • Host identity • Event type (network or protocol event) • Service • Protocol • Protocol attributes Customer-specified policy attributes: • Hostname • Service name • Outcome name • Event severity • Owner
M-CD-5	Monitor protects audit records from unauthorized deletion and modification. Monitor ensures that 4 gigabytes of audit records will be maintained when audit storage exhaustion occurs. (FAU_STG.2.1-1, FAU_STG.2.2-1, FAU_GEN.1.3-1)
M-CD-6	Monitor overwrites the oldest stored audit records if the audit trail is full. (FAU_STG.4.1-1)
M-CD-7	Monitor restrict the ability of changing the auditing events policy only to Developers (FMT_MOF.1.1-1 [1], FMT_MOF.1.1-1 [2])

Monitor Analyze Data Function	
M-AD-1	Monitor provides users with the capability to read information from the audit records according to the Table 5-2 SecurVantageTM User Access Policy. (FAU_SAR.1.1-1 [1], FAU_SAR.1.1-1 [2], FAU_SAR.1.1-1 [3], FAU_SAR.1.1-1 [4], FAU_SAR.1.2-1) • Operator, Analyst, and Developer can read Event Data • Operator, Analyst, and Developer can read Alerts • SV Manager can read Application Log data • Account Manager can read User Log data Monitor provides the audit records in a manner suitable for the user to interpret the information.
M-AD-2	Monitor prohibits all users read access to the audit records, except those who have been granted explicit read access. (FAU_SAR.2-1)

Monitor Analyze Data Function	
M-AD-3	Monitor provides the ability to perform searches, sorting, and ordering of the audit data, based on event severity and event type. (FAU_SAR.3)

6.1.4 SecurVantage™ Enterprise

Enterprise Manager User Access Function	
E-MUA-1	Enterprise maintains the following information for each user: user name, hash of the password or certificate, roles, and whether authentication is password or certificate based. (FIA_ATD.1.1-1)
E-MUA-2	Enterprise requires that user passwords be: • Minimum of 8 characters in the password • Maximum of 64 characters • At least one lower case character • At least one upper case character • At least one numeric character (FIA_SOS.1.1-1)
E-MUA-3	Enterprise enforces the SecurVantage™ User Access Policy (See Table 5-2 SecurVantageTM User Access Policy) (FDP_ACC.2.1-1, FDP_ACC.2.2-1) (FDP_ACF.1.1-1, FDP_ACF.1.2-1, FDP_ACF.1.3-1, FDP_ACF.1.4-1)
E-MUA-4	Enterprise restricts the ability to query, modify, or delete the username, roles, and password- or certificate-based authentication security attribute to Account Manager. (FMT_MSA.1.1-1)
E-MUA-5	Enterprise provides restrictive default values for security attributes as specified in Table 5-2 SecurVantageTM User Access Policy and allows the Account Manager to specify alternative initial values. (FMT_MSA.3.1-1, FMT_MSA.3.2-1)
E-MUA-6	Enterprise restricts the ability to access data as specified in Table 5-2 SecurVantageTM User Access Policy. (FMT_MTD.1.1-1 [1], FMT_MTD.1.1-1 [2], FMT_MTD.1.1-1 [3], FMT_MTD.1.1-1 [4], FMT_MTD.1.1-1 [5], FMT_MTD.1.1-1 [6], FMT_MTD.1.1-1 [7], FMT_MTD.1.1-1 [8], FMT_MTD.1.1-1 [9], FMT_MTD.1.1-1 [10], FMT_MTD.1.1-1 [11])
E-MUA-7	Enterprise restricts the ability to revoke security attributes associated with users, subjects, and objects to Account Manager. (FMT_REV.1)
E-MUA-8	Enterprise is capable of providing the security management functions as specified in Table 5-2 SecurVantageTM User Access Policy. (FMT_SMF.1.1-1)

Enterprise Manager User Access Function	
E-MUA-9	Enterprise maintains the roles Operator, Analyst, Developer, SV Manager, and Account Manager. (FMT_SMR.1.1-1, FMT_SMR.1.2-1)
E-MUA-10	Enterprise ensures that the Table 5-2 SecurVantageTM User Access Policy is invoked and succeeds before each function is allowed to proceed. (FPT_RVM_EXP.1.1-1)
E-MUA-11	Enterprise maintains a security domain for its own execution and enforces separation between security domains of users initiating actions through its own TSFI. (FPT_SEP_EXP.1.1-1, FPT_SEP_EXP.1.2-1)
E-MUA-12	Enterprise allows SV Managers to set and configure the parameters of the account lockout feature (FMT_MOF.1.1-1[1], FMT_MOF.1.1-1 [2]) (FMT_MTD.2.1-1 [1], FMT_MTD.2.1-1 [2], FMT_MTD.2.2-1)
E-MUA-13	Enterprise allows SV Manager to set a threshold of violation compliance per domain (FMT_MTD.2.1-1 [1], FMT_MTD.2.1-1 [2], FMT_MTD.2.2-1)

Enterprise User Login function	
E-UL-1	Enterprise requires each user to self identify before being allowed to perform any other actions. (FIA_UID.2.1-1)
E-UL-2	Enterprise requires each user to successfully authenticate with either a password or certificate before being allowed any other actions. (FIA_UAU.2.1-1)
E-UL-3	The hash of the given password must match the stored hash of the user password. The given certificate must produce the same SHA-1 hash as the stored user hash. (FIA_UAU.5.1-1, FIA_UAU.5.2-1)
E-UL-4	Enterprise provides only confirmation of user name and asterisks for password when password authentication is used. (FIA_UAU.7.1-1 [1], FIA_UAU.7.1-1 [2])

E-UL-5	Enterprise locks user accounts when consecutive failed login attempts are performed on a given account (FIA_AFL.1.1-1, FIA_AFL.1.2-1) (FTA_TSE.1.1-1)
E-UL-6	Users need to re-authenticate before changing their own passwords (FIA_UAU.6.1-1)
E-UL-7	User's session is terminated after 30 minutes of inactivity (FTA_SSL.3.1-1)

Enterprise Collect Data Function	
E-CD-1	Enterprise collects summary information on events and Alerts from the reporting monitors. Enterprise allows users to view information as per access in Table 5-2. (FAU_SAR.1.1.1-1 [1], FAU_SAR.1.1-1 [2]))
E-CD-2	Enterprise sends an SMTP or SNMP trap when compliance thresholds are crossed (FAU_ARP.1)

Enterprise Analyze Data Function	
E-AD-1	Enterprise provides users with the capability to read information from the audit records according to the Table 5-2 SecurVantageTM User Access Policy. (FAU_SAR.1.1-1 [1], FAU_SAR.1.1-1 [2], FAU_SAR.1.1-1 [3], FAU_SAR.1.1-1 [4], FAU_SAR.1.2-1) • Operator, Analyst, and Developer can read Event Data • Operator, Analyst, and Developer can read Alerts • SV Manager can read Application Log data • Account Manager can read User Log data Enterprise provides the audit records in a manner suitable for the user to interpret the information.
E-AD-2	Enterprise prohibits all users read access to the audit records, except those who have been granted explicit read access. (FAU_SAR.2.1-1)
E-AD-3	Enterprise provides the ability to perform searches, sorting, and ordering of the audit data, based on event severity and event type. (FAU_SAR.3)

6.1.5 SecurVantage™ Enterprise Reporting Gateway

ER Gateway (ER GW) Audit Function	
ER-AU-1	ER Gateway is able to generate an audit record of the following auditable events: • Login/logout of users • Create, edit, and delete user accounts • Add, edit, or remove Enterprises • Change user's password ER GW records within each audit record at least the following information: Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event The ER GW provides two types of diagnostic logs that enables an authorized user to examine system traffic and performance on the ER Gateway—user logs and application logs. (FAU_GEN.1.1-2, FAU_GEN.1.2-2)
ER-AU-2	ER Gateway provides the ER Account Manager with the capability to read the user activity log information from the audit records. ER GW provides the ER SV Manager with the capability to read the Gateway log information from the audit records. ER GW provides the audit records in a manner suitable for the user to interpret the information. (FAU_SAR.1.1-2 [1], FAU_SAR.1.1-2 [2], FAU_SAR.1.2-2)
ER-AU-3	ER Gateway prohibits all users read access to the audit records, except those users that have been granted explicit read-access. (FAU_SAR.2.1-2)
ER-AU-4	ER Gateway protects audit records from unauthorized deletion and modification. ER Gateway ensures that 800 megabytes of audit records will be maintained until the audit file is full (FAU_STG.2.1-2, FAU_STG.2.2-2, FAU_STG.2.3-2)
ER-AU-5	ER Gateway overwrites the oldest stored audit records if the audit trail is full. (FAU_STG.4.1-2)

ER Gateway (ER GW) Manage User Access Function	
ER-MUA-1	ER Gateway maintains the following information for each user: user name, hash of the password, and roles. (FIA_ATD.1.1-2)

ER Gateway (ER GW) Manage User Access Function	
ER-MUA-2	ER Gateway requires that user passwords be: • Minimum of 8 characters in the password • Maximum of 64 characters • At least one lower case character • At least one upper case character • At least one numeric character (FIA_SOS.1.1-2)
ER-MUA-3	ER Gateway enforces the SecurVantage™ ER User Access Policy which controls access of subjects to objects (see Table 5-3) within the TOE's scope of control. (FDP_ACC.2.1-2, FDP_ACC.2.2-2) (FDP_ACF.1.1-2, FDP_ACF.1.2-2)
ER-MUA-4	ER Gateway restricts the ability to determine the behavior of the functions listed in Table 5-5 to the authorized roles identified in Table 5-5. . (FMT_MOF.1-2)
ER-MUA-5	ER Gateway restricts the ability to query, modify, delete, and other operations as specified in Table 5-4 to the roles as specified in Table 5-4. (FMT_MSA.1.1-2)
ER-MUA-6	ER Gateway enforces the SecurVantage™ ER User Access Policy to provide restrictive default values for security attributes and allows the Account Manager to specify alternative initial values. (FMT_MSA.3.1-2, FMT_MSA.3.2-2)
ER-MUA-7	ER Gateway restricts the ability to access TSF data as specified in Table 5-5 Management of TSF Data. (FMT_MTD.1.1-2)
ER-MUA-8	ER Gateway is capable of providing the following security management functions: • Determine the behavior of the functions listed in Table 5-5 to the authorized roles identified in Table 5-5 (see FMT_MOF.1-2), • Query, modify, delete, and create as specified in Table 5-4 the security attributes as specified in Table 5-4 (see FMT_MSA.1-2), • Query, modify, delete, and create as specified in Table 5-5 and the TSF Data as specified in Table 5-5 (See FMT_MTD.1.1-2). (FMT_SMF.1.1-2)
ER-MUA-9	ER Gateway maintains the roles ER SV Manager and ER Account Manager. (FMT_SMR.1.1-2, FMT_SMR.1.2-2)
ER-MUA-10	ER Gateway ensures that the SecurVantage™ ER User Access Policy is invoked and succeeds before each function is allowed to proceed. (FPT_RVM_EXP.1.1-2)

ER Gateway (ER GW) Manage User Access Function	
ER-MUA-11	ER Gateway maintains a security domain for its own execution and enforces separation between security domains of users initiating actions through its own TSFI. (FPT_SEP_EXP.1.1-2 and FPT_SEP_EXP.1.2-2)
ER-MUA-12	ER Gateway provides management of the account lockout feature. (FMT_MTD.2.1-2, , FMT_MTD.2.2-2)

ER Gateway (ER GW) User Login Function	
ER-UL-1	ER Gateway requires each user to self identify before being allowed to perform any other actions. (FIA_UID.2.1-2)
ER -UL-2	ER Gateway requires each user to successfully authenticate with a password before being allowed any other actions. (FIA_UAU.2.1-2)
ER -UL-3	The hash of the given password must match the stored hash of the user password. (FIA_UAU.5.1-2, FIA_UAU.5.2-2)
ER-UL-4	ER Gateway uses X509 certificates to authenticate each machine in the system. It uses this authentication to enable connections between machines. ER Gateway authenticates any SecurVantage™ component's claimed identity according to the certificate fingerprint match. (FIA_UAU.5.1-2, FIA_UAU.5.2-2)
ER -UL-5	ER Gateway provides only confirmation of user name and asterisks for password when password authentication is used. (FIA_UAU.7.1-2
ER -UL-6	ER Gateway locks user accounts when consecutive failed login attempts are performed on a given account (FIA_AFL.1-2) (FTA_TSE.1-2)
ER -UL-7	Users need to reauthenticate before changing their own passwords (FIA_UAU.6.1-2)
ER -UL-8	Users session is terminated after 30 minutes of inactivity (FTA_SSL.3.1-2)

6.2 Assurance Measures

SecurVantage™ satisfies the assurance requirements for Evaluation Assurance Level EAL3. Table 8-13 in Section 8.3.2 shows how the assurance measures are satisfied by the TOE.

6.3 Strength of Function

The M-MUA-2, E-MUA-2 and ER_MUA-2 security functions are realized by a probabilistic mechanism (passwords). These security functions implement a strength-of-function level of SOF-Basic.

7 PP Claims

The SecurVantage™ Security Target was not written to address any existing Protection Profile.

8 Rationale

8.1 Security Objectives Rationale

8.1.1 Organizational Security Policies

Table 8-1 shows that Organizational Security Policies are covered by Security Objectives for the TOE.

Table 8-1 Mapping of Organizational Security Policies to Security Objectives for the TOE

No.	Organizational Security Policy	Objective Name
1	P.Accact	O.IDAuth O.Audit
2	P.Access	O.Access O.IDAuth
3	P.Analyz	O.IDAnlz
4	P.Detect	O.IDSens O.Audit
5	P.Manage	O.Admin O.Access O.IDAuth

P.Accact: Users of the TOE shall be accountable for their actions within the system. **P.Accact** is countered by:

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE function access.

O.Audit: The TOE must record audit records for data accesses and use of the system functions. This objective requires the TOE to audit attempts for data accesses and use of TOE functions.

P.Access: All data collected and produced by the TOE shall only be used for authorized purposes. **P.Access** is countered by:

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This is provided by access controls that limit the actions an individual is authorized to perform.

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE function access.

P.Analyz: Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to system data and appropriate response actions taken. **P.Analyz** is countered by:

O.IDAnlz: The TOE must accept data and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future). This objective requires the TOE to analyze system data, which includes attempts to halt the TOE.

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

O.IDSens: The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, unauthorized access, or malicious activity of IT System assets and the IDS. This objective addresses this assumption by requiring the TOE to collect system data, which includes attempts to halt the TOE.

O.Audit: The TOE must record audit records for data accesses and use of the system functions. This objective requires the TOE to audit attempts for data accesses and use of TOE functions.

P.Manage: The TOE shall only be managed by authorized users. P.Manage is countered by:

O.Admin: The TOE must provide the functionality to enable an authorized user toeffectively manage the TOE and its security functions. This objective ensures the TOE has all the necessary administrator functions to manage the product.

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This is provided by access controls that limit the actions an individual is authorized to perform. .

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE function access.

8.1.2 Threats to Security

Table 8-2 shows that all identified threats to security are countered by Security Objectives for the TOE.

Table 8-2 All Threats to Security Countered

No	TOE Threat Name	Threat Description	Security Objective
1	T.Abuse	An undetected compromise of the TOE may occur as a result of an authorized user of the TOE (intentionally or otherwise) performing actions the individual is authorized to perform.	O.Access O.Audit OE.Time
2	T.Access	An authorized user of the TOE may access information or resources without having permission from the person who owns, or is responsible for, the information or resource.	O.Access
3	T.BadPassword	Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorized access to the TOE.	O.PasswordQual O.BruteForce
4	T.Bypass	An attacker may attempt to bypass TSF security functions	O.PartialDomainSep O.NonBypass O.Reauthenticate OE.NonBypass
5	T.BypassDisclosure	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.	O.Access O.PartialDomainSep O.IDAuth O.MultipleAuthen O.NonBypass O.Revoke OE.Confidentiality OE.PartialDomainSep OE.NonBypass
6	T.BypassIntegrity	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.	O.Access O.PartialDomainSep O.IDAuth O.NonBypass O.Revoke OE.PartialDomainSep OE.NonBypass
7	T.DataLoss	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.	O.Access O.DataIntegrity O.PartialDomainSep O.IDAuth O.Revoke OE.PartialDomainSep
8	T.Halt	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.	O.Access O.IDAnlz O.IDAuth O.IDSens

No	TOE Threat Name	Threat Description	Security Objective
9	T.ImpConfig	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.	O.Access O.Admin O.IDAuth O.Revoke
10	T.OFlows	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.	O.OFlows
11	T.Mismanage	Administrators may make errors in the management of security functions and TSF data, if administrative tools are not provided. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.	O.Admin O.ManageData O.Roles
12	T.Privil	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data	O.Access O.PartialDomainSep O.IDAuth O.MultipleAuthen O.ProtectAuth OE.PartialDomainSep
13	T.RemoteAttack	A threat agent may be able to view, modify, and/or delete security-related information that is sent between a remotely located Authorized Administrator and the TOE.	OE.ComIntegrity OE.Confidentiality
14	T.Tamper	An attacker may attempt to modify TSF programs and data.	O.PartialDomainSep OE.PartialDomainSep
15	T.Transmit	TSF data may be disclosed or modified by an attacker while being transmitted between TOE components.	OE.ComIntegrity OE.Confidentiality
16	T.Undetect	Attempts by an attacker to violate the security policy may go undetected.	O.Audit OE.Time

T.Abuse: An undetected compromise of the TOE may occur as a result of an authorized user of the TOE (intentionally or otherwise) performing actions the individual is authorized to perform. **T.Abuse** is countered by:

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This is provided by access controls that limit the actions an individual is authorized to perform.

O.Audit: The TOE must log audit records for data accesses and use of the system functions. This objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

OE.Time: The IT environment must provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

T.Access: An authorized user of the TOE may access information or resources without having permission from the person who owns, or is responsible for, the information or resource. **T.Access** is countered by:

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This is provided by access controls that limit the actions an individual is authorized to perform.

T.BadPassword: Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorized access to the TOE. **T.BadPassword** is countered by:

O.BruteForce: The TOE must lock user accounts after a number of consecutive failed attempts in a given window of time.

O.PasswordQual: The TOE must be able to specify password rules strong enough to deter password guessing. Enforcing these rules will force the user to create a better password.

T.Bypass: An attacker may attempt to bypass TSF security functions. **T.Bypass** is countered by:

O.PartialDomainSep: The TOE must maintain its own domain for execution and ensure that it cannot be interfered or tampered with by a user. The TOE must maintain separation between codes executing on behalf of different users. This objective addresses this threat by providing TOE self-protection and separation between users.

O.NonBypass: The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. As a result, an attacker would not be able to bypass the TSF security functions.

O.Reauthenticate: The TOE requires reauthentication to change users' own password

OE.NonBypass: The IT environment must ensure that its protection mechanisms cannot be bypassed. As a result, an attacker would not be able to bypass the TSF security functions by using the IT environment.

T.BypassDisclosure: An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. **T.BypassDisclosure** is countered by:

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This is provided by access controls that limit the actions an individual is authorized to perform. This objective builds upon the **O.IDAuth** objective by permitting only authorized users to access TOE data.

O.PartialDomainSep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing TOE self-protection and separation between users.

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE data access.

O.MultipleAuthen: The TOE must provide multiple authentication mechanisms. This allows users to authenticate themselves by either ID and password or ID and certificate. Having multiple authentication mechanisms, such as certificates, will make it difficult for an unauthorized user to impersonate a valid user.

O.NonBypass: The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. As a result, an attacker would not be able to bypass the TSF security functions.

O.Revoke: The TOE will allow authorized users to revoke security attributes within the TSC. Administrators will be allowed to revoke the privileges of users. This will limit the access of users.

OE.Confidentiality: The IT environment must protect the confidentiality of data transmitted within the TOE via the use of encryption. Additionally, the IT environment must protect the confidentiality of its dialogue with an authorized administrator, either locally or remotely, via encryption. This objective ensures that confidentiality of TOE dialogs and data will be maintained and protected from disclosure via encryption.. TOE data is encrypted, which protects it from disclosure.

OE.PartialDomainSep: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by protecting the TOE and its data.

OE.NonBypass: The IT environment must ensure that its protection mechanisms cannot be bypassed. As a result, an attacker would not be able to bypass the TOE security functions.

T.BypassIntegrity: An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. **T.BypassIntegrity** is countered by:

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the **O.IDAuth** objective by permitting only authorized users access to TOE data.

O.PartialDomainSep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing TOE self-protection and separation between users.

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE data access.

O.NonBypass: The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. As a result, an attacker would not be able to bypass the TSF security functions.

O.Revoke: The TOE will allow authorized users to revoke security attributes within the TSC. Administrators will be allowed to revoke the privileges of users. This will limit the access of users.

OE.PartialDomainSep: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by protecting the TOE and its data.

OE.NonBypass: The IT environment must ensure that its protection mechanisms cannot be bypassed. As a result, an attacker would not be able to bypass the TOE security functions.

T.DataLoss: An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. **T.DataLoss** is countered by:

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the O.IDAuth objective by permitting only authorized users access to TOE data.

O.DataIntegrity: The TOE must ensure the integrity of all audit and System data. This objective ensures no TOE data will be deleted.

O.PartialDomainSep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing TOE self-protection and separation between users.

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE data access.

O.Revoke: The TOE will allow authorized users to revoke security attributes within the TSC. Administrators will be allowed to revoke the privileges of users. This will limit the access of users.

OE.PartialDomainSep: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by protecting the TOE and its data.

T.Halt: An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. **T.Halt** is countered by:

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the **O.IDAuth** objective by permitting only authorized users access to TOE functions.

O.IDAnlz: The TOE must accept data from IDS Sensors and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future). This objective addresses this threat by requiring the TOE to analyze system data, including attempts to halt the TOE.

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE function access.

O.IDSens: The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, unauthorized access, or malicious activity of IT System assets and the IDS. This objective addresses this threat by requiring the TOE to collect system data, which includes attempts to halt the TOE.

T.ImpConfig: An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. **T.ImpConfig** is countered by:

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the **O.IDAuth** objective by permitting only authorized users access to TOE functions.

O.Admin: The TOE must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions. This objective ensures the TOE has all the necessary administrator functions to manage the product.

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE function access.

O.Revoke: The TOE will allow authorized users to revoke security attributes within the TSC. Administrators will be allowed to revoke the privileges of users. This will limit the access of users.

T.OFlows: An unauthorized user may cause a malfunction of the TOE by creating an influx of data that the TOE cannot handle. **T.OFlows** is countered by:

O.OFlows: The TOE must appropriately handle potential audit and system data storage overflows. This objective counters this threat by requiring the TOE to handle data storage overflows.

T.Mismanage: Administrators may make errors in the management of security functions and TSF data, if administrative tools are not provided. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE. **T.Mismanage** is countered by:

O.Admin: The TOE must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions. This objective ensures the TOE has all the necessary administrator functions to manage the product.

O.ManageData: The TOE must be able to store and maintain properties of users and resources including information to support primary and application authentication. This will assist administrators in managing the TOE.

O.Roles: The TOE must support multiple administrative roles. Multiple administrative roles can be used to enforce separation of duty, so that one administrator can catch errors made by another administrator.

T.Privil: An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data **T.Privil** is countered by:

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data. This objective builds upon the **O.IDAuth** objective by permitting only authorized users access to TOE functions.

O.PartialDomainSep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing TOE self-protection and separation between users.

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of users prior to any TOE function access.

O.MultipleAuthen: The TOE must provide multiple authentication mechanisms. This allows users to authenticate themselves by either ID and password or ID and certificate. Having multiple authentication mechanisms, such as certificates, makes it difficult for an unauthorized user to gain access to the TOE.

O.ProtectAuth: The TOE will provide protected authentication feedback. When an authorized user is typing in their password only asterisks will be seen on the screen. This will limit the ability to see what an authorized user's password is.

OE.PartialDomainSep: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by protecting the TOE and its data.

T.RemoteAttack: A threat agent may be able to view, modify, and/or delete security-related information that is sent between a remotely located Authorized Administrator and the TOE. **T.RemoteAttack** is countered by:

OE.ComIntegrity: The IT environment must protect the integrity of data transmitted within the TOE via digital signature. Upon receipt of data from another component (Studio, Monitor, Monitor LE, and Enterprise) of the TOE, the IT environment must verify that the received data accurately represents the data that was originally transmitted. This objective ensures the integrity of data in transit.

OE.Confidentiality: The IT environment must protect the confidentiality of data transmitted between the major components (Studio, Monitor, Monitor LE, and Enterprise) of the TOE via the use of encryption. Communication, either locally or remotely, must be protected from disclosure. When communication occurs over a network, it must be encrypted by the environment. Additionally, the IT environment must protect the confidentiality of its dialogue with an authorized administrator, either locally or remotely, via encryption. This objective ensures that confidentiality of TOE data will be maintained and protected from disclosure, via encryption. TOE data is encrypted, which protects it from disclosure.

T.Tamper: An attacker may attempt to modify TSF programs and data. **T.Tamper** is countered by:

O.PartialDomainSep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing TOE self-protection and separation between users.

OE.PartialDomainSep: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by protecting the TOE and its data.

T.Transmit: TSF data may be disclosed or modified by an attacker while being transmitted between TOE components. **T.Transmit** is countered by:

OE.ComIntegrity: The IT environment must protect the integrity of data transmitted within the TOE via digital signature. Upon receipt of data from another component (Studio, Monitor, Monitor LE, and Enterprise) of the TOE, the IT environment must verify that the received data accurately represents the data that was originally transmitted. This objective ensures the integrity of data in transit.

OE.Confidentiality: The IT environment must protect the confidentiality of data transmitted between the major components (Studio, Monitor, Monitor LE and Enterprise) of the TOE via the use of encryption. Communication must be protected, either locally or remotely, from being revealed. When communication occurs over a network, it must be encrypted by the environment. Additionally, the IT environment must protect the confidentiality of its dialogue with an authorized administrator, either locally or remotely, via encryption. This objective ensures that confidentiality of TOE data will be maintained. TOE data is encrypted, which protects it from disclosure.

T.Undetect: Attempts by an attacker to violate the security policy may go undetected. **T.Undetect** is countered by:

O.Audit: The TOE must log audit records for data accesses and use of the system functions. This objective records attempts to violate the security policy.

OE.Time: The IT environment must provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

Table 8-3 shows that all Security Objectives for the TOE and IT Environment map to identified threats to security.

Table 8-3 Mapping Security Objectives for the TOE and IT Environment to Threats/Policies

No.	Objective Name	Threat
1	O.Access	T.Abuse T.Access T.BypassDisclosure T.BypassIntegrity T.DataLoss T.Halt T.ImpConfig T.Privil P.Access P.Manage
2	O.Admin	T.ImpConfig T.Mismanage P.Manage
3	O.Audit	T.Abuse T.Undetect P.Accact P.Detect
4	O.BruteForce	T.BadPassword
5	O.DataIntegrity	T.DataLoss
6	O.PartialDomainSep	T.Bypass T.BypassDisclosure T.BypassIntegrity T.DataLoss T.Tamper T.Privil
7	O.IDAnlz	T.Halt P.Analyz
8	O.IDAuth	T.BypassDisclosure T.BypassIntegrity T.DataLoss T.Halt T.Privil T.ImpConfig P.Accact P.Access P.Manage
9	O.IDSens	T.Halt P.Detect

No.	Objective Name	Threat
10	O.ManageData	T.Mismanage
11	O.MultipleAuthen	T.BypassDisclosure T.Privil
12	O.NonBypass	T.Bypass T.BypassDisclosure T.BypassIntegrity
13	O.OFlows	T.OFlows
14	O.PasswordQual	T.BadPassword
15	O.ProtectAuth	T.Privil
16	O.Reauthenticate	T.Bypass
17	O.Revoke	T.BypassDisclosure T.BypassIntegrity T.DataLoss T.ImpConfig
18	O.Roles	T.Mismanage
1	OE.ComIntegrity	T.RemoteAttack T.Transmit
2	OE.Confidentiality	T.BypassDisclosure T.RemoteAttack T.Transmit
3	OE.PartialDomainSep	T.BypassDisclosure T.BypassIntegrity T.DataLoss T.Privil T.Tamper
4	OE.NonBypass	T.Bypass T.BypassDisclosure T.BypassIntegrity
5	OE.Time	T.Abuse T.Undetect

8.1.3 Assumptions

Table 8-4 is included as a consistency check that all security objectives for the non-IT security objectives map to corresponding threats and assumptions.

Table 8-4 Reverse Mapping of Non-IT Security Objectives for the Environment to Threats/Policies/ Assumptions

No.	Objective Name	Threat/Policy/Assumption
1	ON.Creden	A.NoEvil
2	ON.Install	A.Admin A.NoEvil T.ImpConfig
3	ON.Operations	A.Admin A.NoEvil
4	ON.Person	A.Dynmic A.Manage
5	ON.Password	A.Password
6	ON.Phycal	A.Protct A.Locate A.NoEvil
7	ON.NoUntrusted	A.Trusted

Table 8-5 shows that all secure usage assumptions are addressed by either security objectives for the IT environment or non-IT security objectives.

Table 8-5 All assumptions addressed

No	Name	Assumption	Objective
1	A.Admin	The administrator is trusted to correctly configure the TOE.	ON.Install ON.Operations
2	A.Dynmic	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.	ON.Person
3	A.Trusted	There will be no untrusted users of the TOE and no un-trusted software loaded on the TOE host platforms.	ON.NoUntrusted
4	A.Protct	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	ON.Phycal

No	Name	Assumption	Objective
5	A.Locate	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	ON.Phycal
6	A.Manage	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	ON.Person
7	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.	ON.Install ON.Operations ON.Phycal ON.Creden
8	A.Password	Administrators and users will follow the guidance provided by the TOE documentation for choosing good passwords.	ON.Password

A.Admin: The administrator is trusted to correctly configure the TOE. **A.Admin** is covered by:

ON.Install: Those responsible for the TOE must ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes correctly configuring the TOE.

ON.Operations: Procedures must be enacted which ensure that the TOE will be managed and operated in a secure manner. These procedures will provide guidance to the administrator on how to configure the TOE.

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.Dynmic** is covered by:

ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System. This objective ensures that the TOE will be managed appropriately.

A.Trusted: There will be no untrusted users of the TOE and no untrusted software loaded on the TOE host platforms. **A.Trusted** is covered by:

ON.NoUntrusted: The authorized administrator will ensure that there are no untrusted users and no untrusted software on the SecurVantage™ Server hosts.

A.Protct: The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. **A.Protct** is covered by:

ON.Phycal: Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack. This objective provides for the physical protection of the TOE hardware and software.

A.Locate: The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. **A.Locate** is covered by:

ON.Phycal: Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack. This objective provides for the physical protection of the TOE.

A.Manage: There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. **A.Manage** is covered by:

ON.Person: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System. This objective ensures all authorized administrators are qualified and trained to manage the TOE.

A.NoEvil: The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. **A.NoEvil** is covered by:

ON.Install: Those responsible for the TOE must ensure that the TOE is delivered and installed in a manner that maintains IT security. This objective ensures that the TOE is properly installed and operated.

ON.Operations: Procedures must be in place which ensure the TOE will be managed and operated in a secure manner. These procedures will provide guidance to the administrator on how to securely operate the TOE.

ON.Phycal: Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack. This objective provides for physical protection of the TOE by authorized administrators.

ON.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. This objective supports this assumption by requiring protection of all authentication data.

A.Password: Administrators and users will follow the guidance provided by the TOE documentation for choosing good passwords.

ON.Password: Personnel working as authorized administrators and users must follow the TOE guidance about choosing good passwords.

8.2 Security Requirements Rationale

8.2.1 Requirements for the TOE

Table 8-6 demonstrates that all of the security objectives of the TOE are satisfied.

Table 8-6 All Objectives Met by Functional Components

No	Objective	Objective Description	Security Functional or Assurance Requirement
1	O.Access	The TOE must allow authorized users to access only appropriate TOE functions and data.	FAU_SAR.2* FAU_STG.2* FDP_ACC.2* FDP_ACF.1* FIA_UAU.2* FIA_UID.2* FMT_MTD.1* FMT_MTD.2* FMT_SMF.1*
2	O.Admin	The TOE must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions.	FAU_SAR.1* FAU_SAR.3 FAU_SEL.1 FMT_MOF.1* FMT_MSA.1* FMT_MSA.3* FMT_MTD.1* FMT_MTD.2* FMT_SMF.1*
3	O.Audit	The TOE must record audit records for data accesses and use of the system functions.	FAU_GEN.1* FAU_SEL.1 FPT_ITA.1
4	O.BruteForce	The TOE must lock user account after a number of consecutive failed attempts in a given window of time	FIA_AFL.1* FTA_TSE.1*
5	O.DataIntegrity	The TOE must ensure the integrity of all audit data.	FAU_STG.2* FMT_MTD.1*
6	O.PartialDomainSep	The TOE must maintain its own domain for execution and ensure that it cannot be interfered with or tampered with by a user. The TOE must maintain separation between code executing on behalf of different users.	FPT_SEP_EXP.1.1-1 FPT_SEP_EXP.1.2-1 FPT_SEP_EXP.1.1-2 FPT_SEP_EXP.1.2-2

No	Objective	Objective Description	Security Functional or Assurance Requirement
7	O.IDAnlz	The TOE must accept data and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).	FAU_SAA.3
8	O.IDAuth	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	FIA_UAU.2* FIA_UID.2*
9	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.	FAU_ARP.1
10	O.ManageData	The TOE must be able to store and maintain properties of users and resources including information to support primary and application authentication.	FIA_ATD.1* FMT_MTD.1*
11	O.MultipleAuthen	The TOE must provide multiple authentication mechanisms.	FIA_UAU.5*
12	O.NonBypass	The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.	FPT_RVM_EXP.1.1-1 FPT_RVM_EXP.1.1-2 FTA_SSL.3*
13	O.OFlows	The TOE must prevent audit and System data storage overflows.	FAU_STG.4*
14	O.PasswordQual	The TOE must be able to specify password rules strong enough to deter password guessing.	FIA_SOS.1*
15	O.ProtectAuth	The TOE will provide protected authentication feedback.	FIA_UAU.7*
16	O.Reauthenticate	The TOE requires reauthentication to change users own password	FIA_UAU.6*
17	O.Revoke	The TOE will allow authorized users to revoke security attributes within the TSC.	FMT_REV.1
18	O.Roles	The TOE must support multiple administrative roles.	FMT_SMR.1*

O.Access: The TOE must allow authorized users to access only appropriate TOE functions and data.
O.Access is addressed by:

FAU_SAR.2* Restricted audit review, which requires that access to audit data be restricted to authorized users.

FAU_STG.2* Guarantees audit data availability, which requires the TOE to protect the audit data from deletion and modification as well as guarantee the availability of the audit data in the event of storage exhaustion, failure, or attack.

FDP_ACC.2* Complete access control; requires that the TSF enforce access controls on all operations between any subject in the TSC and any object within the TSC.

FDP_ACF.1* Security attribute based access control; requires the TSF enforce access controls based on specified security attributes. In addition, the TSF can explicitly authorize and deny access to specified subjects.

FIA_UAU.2* User authentication before any action; requires each user to be successfully authenticated before allowing access to the TOE.

FIA_UID.2* User identification before any action; requires that users be successfully identified before allowing access to the TOE.

FMT_MTD.1* Management of TSF data; requires that only authorized administrators of the system may query network event data and can delete alert data.

FMT_MTD.2* Managements of limits on TSF data; requires that certain security functions have limits configurable by the administrator of the application.

FMT_SMF.1* Specification of management functions; requires that the TSF provide specific management functions.

O.Admin: The TOE must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions. **O.Admin** is addressed by:

FAU_SAR.1* Audit review; requires that the auditor be able to read audit records.

FAU_SAR.3 Selectable audit review; requires that the TSF will provide the ability to search, sort, and order audit data.

FAU_SEL.1 Selective audit; requires the TOE to provide authorized users with the ability to include or exclude auditable events from the set of audited events.

FMT_MOF.1* Management of security functions; requires the TSF to provide configuration properties on certain security functions.

FMT_MSA.1* Management of security attributes; permits only authorized users to query, modify, and delete specified security attributes.

FMT_MSA.3* Static attribute initialization, which requires that the TSF enforce access control for specified default values of security attributes.

FMT_MTD.1* Management of TSF data, which permits only authorized administrators of the system to query network event data and to delete alert data.

FMT_MTD.2* Managements of limits on TSF data; requires that certain security functions have limits configurable by the administrator of the application.

FMT_SMF.1* Specification of management functions; requires that the TSF provide specific management functions.

O.Audit: The TOE must log audit records for data accesses and use of the system functions. **O.Audit** is addressed by:

FAU_GEN.1* Audit data generation; requires the ability to audit specified events.

FAU_SEL.1 Selective audit; provides the TOE with the capability to select which security-relevant events to audit.

FPT_ITA.1 Inter TSF availability within a defined available metric, which requires the TOE to keep alerting to a trusted system in a specific window of time even when TOE access data interface is not available.

O.BruteForce: The TOE must lock user account after a number of consecutive failed attempts in a given window of time. **O.BruteForce** is addressed by:

FIA_AFL.1* Helps preventing brute force attacks on user accounts, which requires the TSF to keep count of consecutive failed login attempts and lock user account when a specific threshold is reached.

FTA_TSE.1* Prevents users from establishing a session with the TOE; requires the TSF to recognize when a user account has been locked.

O.DataIntegrity: The TOE must ensure the integrity of all audit and System data. **O.DataIntegrity** is addressed by:

FAU_STG.2* Guarantees audit data availability, which requires the TSF to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack.

FMT_MTD.1* Management of TSF data, which permits only authorized administrators of the system to query or add audit and system data.

O.PartialDomainSep: The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces. **O.PartialDomainSep** is addressed by:

FPT_SEP_EXP.1.1-1, FPT_SEP_EXP.1.2-1, FPT_SEP_EXP.1.1-2, FPT_SEP_EXP.1.2-2 TSF domain separation; requires that the TSF maintain a security domain for its own execution that protects it from interference and tampering by untrusted users. The TSF must enforce separation between security domains of subjects in the TSC.

O.IDAnlz: The TOE must accept data and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future**). O.IDAnlz** is addressed by:

FAU_SAA.3 The TSF is required to perform intrusion analysis and generate conclusions.

O.IDAuth: The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. **O.IDAuth** is addressed by:

FIA_UAU.2* User authentication before any action; requires each user to be successfully authenticated before allowing access to the TOE.

FIA_UID.2* User identification before any action; requires that users be successfully identified before allowing access to the TOE.

O.IDSens: The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, unauthorized access, or malicious activity within IT System assets. **O.IDSens** is addressed by:

FAU_ARP.1 Security alarms, which requires the TSF to take specified action upon detection of a potential security violation.

O.ManageData: The TOE must be able to store and maintain properties of users and resources including information to support primary and application authentication. **O.ManageData** is addressed by:

FIA_ATD.1* User attribute definition, which requires that the TSF maintain security attributes of user.

FMT_MTD.1* Management of TSF data, which permits only authorized administrators of the system to query network event data and to delete alert data.

O.MultipleAuthen: The TOE must provide multiple authentication mechanisms. **O.MultipleAuthen** is addressed by:

FIA_UAU.5* Multiple authentication mechanisms; requires that the TSF provide multiple authentication mechanisms for user and component authentication.

O.NonBypass: The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. **O.NonBypass** is addressed by:

FPT_RVM_EXP.1.1-1, FPT_RVM_EXP.1.1-2 Non-bypassability of the TSP, which requires that the TSF ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FTA_SSL.3* TSF Initiated termination, which requires the TOE to terminate an inactive connection and mitigates the risk of attackers using a non-attended active session.

O.Oflows: The TOE must prevent audit and System data storage overflows. **O.Oflows** is addressed by:

FAU_STG.4* Prevention of audit data loss; requires that the TSF take action if the audit trail exceeds a specified limit.

O.PasswordQual: The TOE must be able to specify password rules strong enough to deter password guessing. **O.PasswordQual** is addressed by:

FIA_SOS.1* Verification of secrets; requires that the TSF provide a mechanism to verify that passwords meet the rules of the password policy.

O.ProtectAuth: The TOE will provide protected authentication feedback. **O.ProtectAuth** is addressed by:

FIA_UAU.7* Protected authentication feedback, the TSF shall provide only the confirmation of the user name and asterisks for the password for password authentication.

O.Reauthenticate: The TOE requires reauthentication to change users' own password. **O.Reauthenticate** is addressed by:

FIA_UAU.6* Reauthentication; requires the TSF to present users with a screen to provide valid password before changing it to a new one.

O.Revoke: The TOE will allow authorized users to revoke security attributes within the TSC. **O.Revoke** is addressed by:

FMT_REV.1 Revocation, which requires the TSF restrict the ability to revoke security attributes associated with users and objects to authorized users.

O.Roles: The TOE must support multiple administrative roles. **O.Roles** is addressed by:

FMT_SMR.1* Security roles; requires that the TSF be able to associate users with roles.

Table 8-7 All Objectives for the IT Environment Met by Requirements for IT Environment

IT Environment Objectives and Requirements				
No	**Objective**	**Objective Description**	**Requirement for the IT Environment**	**Component Title**
1	OE.ComIntegrity	The IT environment must protect the integrity of data transmitted within the TOE via digital signature. Upon receipt of data from another component (Studio, Monitor, Monitor LE, or Enterprise) of the TOE, the IT environment must verify that the received data accurately represents the data that was originally transmitted.	FPT_ITT.1	Basic internal TSF data transfer protection
2	OE.Confidentiality	The IT environment must protect the confidentiality of data transmitted between the major components (Studio, Monitor, Monitor LE, or Enterprise) of the TOE via the use of encryption.	FPT_ITT.1	Basic internal TSF data transfer protection

IT Environment Objectives and Requirements				
No	**Objective**	**Objective Description**	**Requirement for the IT Environment**	**Component Title**
		Communication must be protected, either locally or remotely, from being revealed. When communication occurs over a network, it must be encrypted by the environment. Additionally, the IT environment must protect the confidentiality of its dialogue with an authorized administrator, either locally or remotely, via encryption.	FTP_TRP.1	Trusted path
3	OE.PartialDomainSep	The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.	FPT_SEP_EXP.1-3	TSF domain separation
4	OE.NonBypass	The TOE must ensure that its protection mechanisms cannot be bypassed.	FPT_RVM_EXP.1-3	Non-bypassability of the TSP
5	OE.Time	The underlying the operating systems must provide reliable time stamps.	FPT_STM.1	Reliable time stamps

OE.ComIntegrity: The IT environment must protect the integrity of data transmitted within the TOE via digital signature. Upon receipt of data from another component (Studio, Monitor, Monitor LE, or Enterprise) of the TOE, the IT environment must verify that the received data accurately represents the data that was originally transmitted. **OE.ComIntegrity** is addressed by:

FPT_ITT.1: Basic internal TSF data transfer protection, which requires that TSF data be protected when transmitted between separate parts of the TOE.

OE.Confidentiality: The IT environment must protect the confidentiality of data transmitted between the major components (Studio, Monitor, Monitor LE, or Enterprise) of the TOE via the use of encryption. Communication, either locally or remotely, must be protected from disclosure. When communication occurs over a network, it must be encrypted by the environment. Additionally, the IT environment must protect the confidentiality of its dialogue with an authorized administrator, either locally or remotely, via encryption. **OE.Confidentiality** is addressed by:

FPT_ITT.1: Basic internal TSF data transfer protection, which requires that TSF data be protected when transmitted between separate parts of the TOE.

FTP_TRP.1: Trust path, which requires that a trusted path between the TSF and a user be provided.

OE.PartialDomainSep: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. **OE.PartialDomainSep** is addressed by:

FPT_SEP_EXP.1-3: TSF domain separation, which provides a distinct protected domain for the TSF and provides separation between subjects within the Operating System's Scope of Control.

OE.NonBypass: The TOE must ensure that its protection mechanisms cannot be bypassed. **OE.NonBypass** is addressed by:

FPT_RVM_EXP.1-3: Non-bypassability of the TSP, which requires non-bypassability of the TSP for all SFPs in the TSP.

OE.Time: The underlying the operating systems must provide reliable time stamps. **OE.Time** is addressed by:

FPT_STM.1: Reliable time stamps, which requires that the TSF provide reliable time stamps for TSF functions.

Table 8-8 shows the security functional requirements for the TOE map to the security objectives of the TOE.

Table 8-8 Mapping of IT Security Functional Requirements to Objectives for the TOE

IT Security Functional Requirements and TOE Objectives			
No.	**Requirement**	**Component Name**	**Objective**
1	FAU_ARP.1	Security alarms	O.IDSens
2	FAU_GEN.1*	Audit data generation	O.Audit
3	FAU_SAA.3	Simple attack heuristics	O.IDAnlz
4	FAU_SAR.1*	Audit review	O.Admin
5	FAU_SAR.2*	Restricted audit review	O.Access
6	FAU_SAR.3	Selectable audit review	O.Admin
7	FAU_SEL.1	Selective audit	O.Admin O.Audit
8	FAU_STG.2*	Guarantees of audit data availability	O.Access O.DataIntegrity
9	FAU_STG.4*	Prevention of audit data loss	O.OFlows
10	FDP_ACC.2*	Complete access control	O.Access
11	FDP_ACF.1*	Security attribute based access control	O.Access

IT Security Functional Requirements and TOE Objectives			
No.	**Requirement**	**Component Name**	**Objective**
12	FIA_AFL.1*	Authentication failure handling	O.BruteForce
13	FIA_ATD.1*	User attribute definition	O.ManageData
14	FIA_SOS.1*	Verification of secrets	O.PasswordQual
15	FIA_UAU.2*	User authentication before any action	O.Access O.IDAuth
16	FIA_UAU.5*	Multiple authentication mechanisms	O.MultipleAuthen
17	FIA_UAU.6*	Re-authenticating	O.Reauthenticate
18	FIA_UAU.7*	Protected authentication feedback	O.ProtectAuth
19	FIA_UID.2*	User identification before any action	O.Access O.IDAuth
20	FMT_MOF.1*	Management of security functions behavior	O.Admin
21	FMT_MSA.1*	Management of security attributes	O.Admin
22	FMT_MSA.3*	Static attribute initialization	O.Admin
23	FMT_MTD.1*	Management of TSF data	O.Access O.Admin O.DataIntegrity O.ManageData
24	FMT_MTD.2*	Management of limits on TSF data	O.Admin O.Access
25	FMT_REV.1	Revocation	O.Revoke
26	FMT_SMF.1*	Specification of management functions	O.Access O.Admin
27	FMT_SMR.1*	Security roles	O.Roles
28	FPT_ITA.1	Inter-TSF availability within a defined availability metric	O.Audit
29	FPT_RVM_EXP.1-1*	Non-bypassability of the TSP	O.NonBypass
30	FPT_SEP_EXP.1-1* FPT_SEP_EXP.1-2*	TSF domain separation	O.PartialDomainSep
31	FTA_SSL.3*	TSF-initiated termination	O.NonBypass
32	FTA_TSE.1*	TOE session establishment	O.BruteForce

8.2.2 Requirements for the IT Environment

Table 8-9 shows that all of the security objectives for the IT environment are satisfied.

Table 8-9 Mapping of Security Functional Requirements for the IT Environment to Objectives for the IT Environment

No.	Requirement	Objective
33	FPT_ITT.1	OE.ComIntegritiy OE.Confidentiality
34	FPT_RVM_EXP.1-3	OE.NonBypass
35	FPT_SEP_EXP.1-3	OE.PartialDomainSep
36	FPT_STM.1	OE.Time
37	FTP_TRP.1	OE.Confidentiality

8.2.3 Dependencies

Table 8-10 shows the dependencies for security functional requirements for the TOE. Table 8-11 shows the dependencies for security functional requirements for the IT Environment. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical requirement are denoted by an *(H)* following the dependency reference.

Table 8-10 Dependencies for TOE

TOE Dependencies					
No.	**Component**	**Component Name**	**Dependencies**	**Dependencies Met By**	**Reference**
1	FAU_ARP.1	Security alarms	FAU_SAA.1	FAU_SAA.1	3 (H)
2	FAU_GEN.1*	Audit data generation	FPT_STM.1	FPT_STM.1	Environment
3	FAU_SAA.3	Simple attack heuristics	None	None	None
4	FAU_SAR.1.1-1 [1] FAU_SAR.1.1-1 [2] FAU_SAR.1.1-1 [3] FAU_SAR.1.1-1 [4] FAU_SAR.1.2-1	Audit review	FAU_GEN.1 -1	FAU_GEN.1.1-1 FAU_GEN.1.2-1	2
	FAU_SAR.1.1-2 [1] FAU_SAR.1.1-2 [2] FAU_SAR.1.2-2	Audit review	FAU_GEN.1-2	FAU_GEN.1.1-2 FAU_GEN.1.2-2	

TOE Dependencies					
No.	**Component**	**Component Name**	**Dependencies**	**Dependencies Met By**	**Reference**
5	FAU_SAR.2.1-1	Restricted audit review	FAU_SAR.1	FAU_SAR.1.1-1 [1] FAU_SAR.1.1-1 [2] FAU_SAR.1.1-1 [3] FAU_SAR.1.1-1 [4] FAU_SAR.1.2-1	4
	FAU_SAR.2.1-2	Restricted audit review		FAU_SAR.1.1-2 [1] FAU_SAR.1.1-2 [2] FAU_SAR.1.2-2	
6	FAU_SAR.3	Selectable audit review	FAU_SAR.1	FAU_SAR.1	4
7	FAU_SEL.1	Security audit event selection	FAU_GEN.1	FAU_GEN.1*	2
			FMT_MTD.1	FMT_MTD.1	23
8	FAU_STG.2.1-1 FAU_STG.2.2-1 FAU_STG.2.3-1	Guarantees of audit data availability	FAU_GEN.1	FAU_GEN.1.1-1 FAU_GEN.1.2-1	2
	FAU_STG.2.1-2 FAU_STG.2.2-2 FAU_STG.2.3-2	Guarantees of audit data availability	FAU_GEN.1	FAU_GEN.1.1-2 FAU_GEN.1.2-2	
9	FAU_STG.4.1-1	Prevention of audit data loss	FAU_STG.2	FAU_STG.2.1-1 FAU_STG.2.2-1 FAU_STG.2.3-1	8 (H)
	FAU_STG.4.1-2	Prevention of audit data loss	FAU_STG.2	FAU_STG.2.1-2 FAU_STG.2.2-2 FAU_STG.2.3-2	
10	FDP_ACC.2.1-1 FDP_ACC.2.2-1	Complete access control	FDP_ACF.1	FDP_ACF.1.1-1 FDP_ACF.1.2-1 FDP_ACF.1.3-1 FDP_ACF.1.4-1	11
	FDP_ACC.2.1-2 FDP_ACC.2.2-2	Complete access control	FDP_ACF.1	FDP_ACF.1.1-2 FDP_ACF.1.2-2 FDP_ACF.1.3-2 FDP_ACF.1.4-2	
11	FDP_ACF.1.1-1 FDP_ACF.1.2-1	Security attribute based access	FDP_ACC.1	FDP_ACC.2.1-1 FDP_ACC.2.2-1	10 (H)

TOE Dependencies					
No.	**Component**	**Component Name**	**Dependencies**	**Dependencies Met By**	**Reference**
	FDP_ACF.1.3-1 FDP_ACF.1.4-1	control	FMT_MSA.3	FMT_MSA.3.1-1 FMT_MSA.3.2-1	22
	FDP_ACF.1.1-2 FDP_ACF.1.2-2 FDP_ACF.1.3-2 FDP_ACF.1.4-2	Security attribute based access control	FDP_ACC.1	FDP_ACC.2.1-2 FDP_ACC.2.2-2	
			FMT_MSA.3	FMT_MSA.3.1-2 FMT_MSA.3.2-2	
12	FIA_AFL.1.1-1 FIA_AFL.1.2-1	Authentication failure handling	FIA_UAU.1	FIA_UAU.2-1	15(H)
	FIA_AFL.1.1-1 FIA_AFL.1.2-1	Authentication failure handling	FIA_UAU.1	FIA_UAU.2-2	
13	FIA_ATD.1*	User attribute definition	None	None	None
14	FIA_SOS.1*	Verification of secrets	None	None	None
15	FIA_UAU.2.1-1	User authentication before any action	FIA_UID.1	FIA_UID.2-1	19 (H)
	FIA_UAU.2.1-2	User authentication before any action	FIA_UID.1	FIA_UID.2-2	
16	FIA_UAU.6	Re-authenticating	None	None	None
17	FIA_UAU.5	Multiple authentication mechanisms	None	None	None
18	FIA_UAU.7.1-1 [1] FIA_UAU.7.1-1 [2]	Protected authentication feedback	FIA_UAU.1	FIA_UAU.2.1-1	15 (H)
	FIA_UAU.7.1-2	Protected authentication feedback	FIA_UAU.1	FIA_UAU.2.1-2	
19	FIA_UID.2	User identification before any action	None	None	None
20	FMT_MOF.1.1-1 [1]	Management of security functions behavior	FMT_SMF.1	FMT_SMF.1.1-1	26 27
			FMT_SMR.1	FMT_SMR.1.1-1 FMT_SMR.1.2-1	
	FMT_MOF.1.1-1 [2]	Management of security functions behavior	FMT_SMF.1	FMT_SMF.1.1-1	
			FMT_SMR.1	FMT_SMR.1.1-1 FMT_SMR.1.2-1	

TOE Dependencies					
No.	**Component**	**Component Name**	**Dependencies**	**Dependencies Met By**	**Reference**
	FMT_MOF.1.1 -2	Management of security functions behavior	FMT_SMF.1	FMT_SMF.1.1-1	
			FMT_SMR.1	FMT_SMR.1.1-2 FMT_SMR.1.2-2	
21	FMT_MSA.1.1-1	Management of security attributes	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2.1-1 FDP_ACC.2.2-1	10 (H) 26 27
			FMT_SMF.1	FMT_SMF.1.1-1	
			FMT_SMR.1	FMT_SMR.1.1-1 FMT_SMR.1.2-1	
	FMT_MSA.1.1-2	Management of security attributes	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.2.1-2 FDP_ACC.2.2-2	
			FMT_SMF.1	FMT_SMF.1.1-2	
			FMT_SMR.1	FMT_SMR.1.1-2 FMT_SMR.1.2-2	
22	FMT_MSA.3.1-1 FMT_MSA.3.2-1	Static attribute initialization	FMT_MSA.1	FMT_MSA.1.1-1	21 27
			FMT_SMR.1	FMT_SMR.1.1-1 FMT_SMR.1.2-1	
	FMT_MSA.3.1-2 FMT_MSA.3.2-2	Static attribute initialization	FMT_MSA.1	FMT_MSA.1.1-2	
			FMT_SMR.1	FMT_SMR.1.1-2 FMT_SMR.1.2-2	
23	FMT_MTD.1.1-1 [1] FMT_MTD.1.1-1 [2] FMT_MTD.1.1-1 [3] FMT_MTD.1.1-1 [4] FMT_MTD.1.1-1 [5] FMT_MTD.1.1-1 [6] FMT_MTD.1.1-1 [7] FMT_MTD.1.1-1 [8] FMT_MTD.1.1-1 [9] FMT_MTD.1.1-1 [10] FMT_MTD.1.1-1 [11]	Management of TSF data	FMT_SMF.1	FMT_SMF.1.1-1	26 27
			FMT_SMR.1	FMT_SMR.1.1-1 FMT_SMR.1.2-1	
	FMT_MTD.1.1-2	Management of TSF data	FMT_SMF.1	FMT_SMF.1.1-2	
			FMT_SMR.1	FMT_SMR.1.1-2 FMT_SMR.1.2-2	

TOE Dependencies					
No.	**Component**	**Component Name**	**Dependencies**	**Dependencies Met By**	**Reference**
24	FMT_MTD.2.1-1 [1] FMT_MTD.2.1-1 [2] FMT_MTD.2.2-1	Management of limits on TSF data	FMT_MTD.1	FMT_MTD.1.1-1 [1] FMT_MTD.1.1-1 [2] FMT_MTD.1.1-1 [3] FMT_MTD.1.1-1 [4] FMT_MTD.1.1-1 [5] FMT_MTD.1.1-1 [6] FMT_MTD.1.1-1 [7] FMT_MTD.1.1-1 [8] FMT_MTD.1.1-1 [9] FMT_MTD.1.1-1 [10] FMT_MTD.1.1-1 [11]	23 27
			FMT_SMR.1	FMT_SMR.1.1-1 FMT_SMR.1.2-1	
	FMT_MTD.2.1-2 FMT_MTD.2.2-2	Management of limits on TSF data	FMT_MTD.1	FMT_MTD.1.1-2	
			FMT_SMR.1	FMT_SMR.1.1-2 FMT_SMR.1.2-2	
25	FMT_REV.1	Revocation	FMT_SMR.1	FMT_SMR.1.1-1 FMT_SMR.1.2-1	27
26	FMT_SMF.1	Specification of management functions	None	None	None
27	FMT_SMR.1.1-1 FMT_SMR.1.2-1	Security roles	FIA_UID.1	FIA_UID.2.1-1	19 (H)
	FMT_SMR.1.1-2 FMT_SMR.1.2-2	Security roles	FIA_UID.1	FIA_UID.2.1-2	
28	FPT_ITA.1	Inter-TSF availability within a defined availability metric	None	None	None
29	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	None	None	None
30	FMT_SEP_EXP.1-1	TSF domain separation	None	None	None

TOE Dependencies					
No.	**Component**	**Component Name**	**Dependencies**	**Dependencies Met By**	**Reference**
31	FTA_SSL.3	TSF-initiated termination	None	None	None
32	FTA_TSE.1	TOE session establishment	None	None	None

Table 8-11 Dependencies for IT Environment

No.	Component	Component Name	Dependencies	Reference
33	FPT_ITT.1	Basic internal TSF data transfer protection	None	None
34	FPT_RVM_EXP.1-2	Non-bypassability of the TSP	None	None
35	FPT_SEP_EXP.1-2	TSF domain separation	None	None
36	FPT_STM.1	Reliable time stamps	None	None
37	FTP_TRP.1	Trusted path	None	None

8.2.4 Strength of Function Rationale

A strength-of-function level of SOF-Basic counters an attack level of low. The environment is one where there are no untrusted users of the TOE and no untrusted software loaded on the TOE platforms.

8.2.5 Assurance Requirements Rationale

Evaluation Assurance Level EAL3 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks against the TOE.

8.2.6 Explicitly Stated Requirements Rationale

A refinement adds additional detail and narrows the scope, but has to be iterated to meet the original scope of the SFR. FPT_RVM_EXP.1 and FPT_SEP_EXP.1 had to be explicitly stated because they all provide partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection. Accordingly, CCIMB RI#19 states the following:

> "Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE."

Since the iterations of FPT_RVM_EXP.1 and FPT_SEP_EXP.1 span both the TOE requirements and IT Environment, they must be explicitly stated.

8.3 TOE Summary Specification Rationale

8.3.1 IT Security Functions

Table 8-12 shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-12 Mapping of Functional Requirements to TOE Summary Specification

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
1	FAU_ARP.1	Security alarms	M-CD-1 E-CD-2	Monitor sends an email or SNMP message if a critical event is generated even when web interface component is down. Enterprise sends an SMTP or SNMP trap when compliance thresholds are crossed. This implements the FAU_ARP.1 SFR.

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
2	FAU_GEN.1* (Continued)	Audit data generation (Continued)	M-CD-2 ER-AU-1	Monitor records based on the following conditions: • Legal IPv4 datagrams • Ethernet 2 encapsulation (length <= 1514 bytes) • Gigabit Ethernet Jumbo frames are not supported Monitor does not check IP, UDP and TCP checksums Reassembly of IP fragment and TCP segments is based on a first-received-is-used rule. A high performance Monitor captures 100% of data: • at a rate between 150 - 325 Mbits per second • for a typical policy that yields around 4% violations; • in a network with a typical network traffic distribution ranging from transaction processing (150Mbits/s) to service networks (325Mbits/s). Monitor can handle higher data rates and more complex policies by sampling the observed network traffic. A Monitor LE captures 100% of data: • at a rate less than 100 Mbits per second ; • for a typical policy that yields around 4% violations; • in a network with a typical network traffic distribution.

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
2	FAU_GEN.1* (Continued)	Audit data generation (Continued)	M-CD-2 ER-AU-1	ER Gateway generates the following auditable events: • Start-up and shutdown of the audit functions • Login/logout of users • Create, edit, and delete user accounts • Add, edit, or remove Enterprises • Change user's password This implements the FAU_GEN.1* SFRs.
3	FAU_SAA.3	Simple attack heuristics	M-CD-3	Monitor maintains an internal representation of signature events as defined in the customer-specified policy that may indicate a violation of the policy. Monitor is able to indicate an imminent violation of the policy when an event is found to match a signature event. This implements the FAU_SAA.3 SFR

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
4	FAU_SAR.1*	Audit review	S-AD-1 S-AD-4 M-AD-1 E-CD-1 E-AD-1 ER-AU-2	Studio, Monitor, and Enterprise provides users with the capability to read information from the audit records according to the Table 5-2 SecurVantageTM User Access Policy. • Operator, Analyst, and Developer can read Event Data (DME and live data for Studio and Live data for Monitor and Enterprise) • Operator, Analyst, and Developer can read Alerts (Only Studio can read DME data) • SV Manager can read Application Log data (Monitor and Enterprise) • Account Manager can read User Log data (Monitor and Enterprise) Studio provides the audit records in a manner suitable for the user to interpret the information. Studio provides users with the capability to read event data and alerts from the local audit record as DME files. ER Gateway provides the ER Account Manager with the capability to read the user activity log information from the audit records. ER Gateway provides the ER SV Manager with the capability to read the Gateway log information and user logs from the audit records. This implements the FAU_SAR.1* SFRs.

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
5	FAU_SAR.2	Restricted audit review	S-AD-2 M-AD-2 E-AD-2	Studio, Monitor, Enterprise, and ER Gateway prohibit all users read access to the audit records, except those that have been granted explicit read access. This implements the FAU_SAR.2* SFRs.
6	FAU_SAR.3	Selectable audit review	S-AD-3 M-AD-3 E-UL-3	Studio, Monitor and Enterprise provide the ability to perform searches, sorting, and ordering of the audit data based on event severity and event type. This implements the FAU_SAR.3 SFR.

7	FAU_SEL.1	Selective audit	S-P-1
			M-CD-4
				Studio provides users with the capability of select what type of events to audit and what severity to be assigned when such events occurred in the network.
				
				Monitor is able to include or exclude auditable events from the set of audited events based on specific attributes.
				
				These attributes include the following:
				• Host identity
				• Event type (network or protocol event)
				• Service
				• Protocol
				• Protocol attributes
				• Customer-specified policy attributes:
				  ○ Hostname
				  ○ Service name
				  ○ Outcome name
				  ○ Event severity
				  ○ Owner
				
				This implements the FAU_SEL.1 SFR.

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
8	FAU_STG.2*	Guarantees of audit data availability	M-CD-5 ER-AU-4	Monitor protects audit records from unauthorized deletion and modification. Monitor ensures that 4 gigabytes of audit records will be maintained when audit storage exhaustion occurs. ER Gateway protects audit records from unauthorized deletion and modification. Monitor ensures that 800 megabytes of audit records will be maintained until the audit file is full. This implements FAU_STG.2* SFRs
9	FAU_STG.4*	Prevention of audit data loss	M-CD-6 ER-AU-5	Monitor overwrites the oldest stored audit records if the audit trail is full. ER Gateway overwrites the oldest stored audit records if the audit trail is full. This implements FAU_STG.4* SFRs
10	FDP_ACC.2*	Complete access control	M-MUA-3 E-MUA-3 ER-MUA-3	Monitor and Enterprise enforces the SecurVantage™ User Access Policy (See Table 5-2 SecurVantageTM User Access Policy) ER Gateway enforce the SecurVantage™ ER User Access Policy which controls access of subjects to objects within the TOE's scope of control (See Table 5-3 SecurVantageTM ER User Access Policy). This implements FDP_ACC.2* SFRs

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
11	FDP_ACF.1*	Security attribute based access control	M-MUA-3 E-MUA-3 ER-MUA-3	Monitor and Enterprise enforces the SecurVantage™ User Access Policy (See Table 5-2 SecurVantageTM User Access Policy) ER Gateway enforces the SecurVantage™ ER User Access Policy which controls access of subjects to objects within the TOE's scope of control (See Table 5-3 SecurVantageTM ER User Access Policy). This implements FDP_ACF.1* SFRs
12	FIA_AFL.1*	Authentication failures	M-UL-5 E-UL-5 ER-UL-6	Monitor, Enterprise, and ER Gateway lock user accounts when consecutive failed login attempts are performed on a given account This implements FIA_AFL.1* SFRs
13	FIA_ATD.1 *	User attribute definition	M-MUA-1 E-MUA-1 ER-MUA-1	Monitor and Enterprise maintain the following information for each user: user name, hash of the password or certificate, roles, and whether authentication is password or certificate based. ER Gateway maintains the following information for each user: user name, hash of the password and roles. This implements FIA_ATD.1* SFRs

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
14	FIA_SOS.1*	Verification of secrets	M-MUA-2 E-MUA-2 ER-MUA-2	Monitor, Enterprise, and ER Gateway require that user passwords be: • Minimum of 8 characters • Maximum of 64 characters • At least one lower case character • At least one upper case character • At least one numeric character This implements FIA_SOS.1* SFRs
15	FIA_UAU.2*	User authentication before any action	M-UL-2 E-UL-2 ER-UL-2	Monitor and Enterprise requires each user to successfully authenticate with either a password or certificate before being allowed any other actions. ER Gateway requires each user to successfully authenticate with a password before being allowed any other actions. This implements FIA_UAU.2* SFRs
16	FIA_UAU.5*	Multiple authentication mechanisms	M-UL-3 M-UL-8 E-UL-3 ER-UL-3 ER-UL-4	The hash of the given password must match the stored hash of the user password. The given certificate (in the case of Enterprise and Monitor) must produce the same SHA-1 hash as the stored user hash. SecurVantage™ uses X509 certificates to authenticate each machine in the system. It uses this authentication to enable connections between machines. SecurVantage™ authenticates any SecurVantage™ component's claimed identity according to the certificate fingerprint match. This implements FIA_UAU.5* SFRs

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
17	FIA_UAU.6	Re-authenticating	M-UL-6 E-UL-6	Users need to reauthenticate before changing their own passwords This implements FIA_UAU.6 SFR
18	FIA_UAU.7*	Protected authentication feedback	S-UL-1 S-UL-2 M-UL-4 E-UL-4 ER-UL-5	Studio provides the certificate dialog box when certificate-based authentication is used. Studio, Monitor, Enterprise, and ER Gateway protect password display with asterisks when username/password authentication is used. This implements FIA_UAU.7* SFRs
19	FIA_UID.2*	User identification before any action	M-UL-1 E-UL-1 ER-UL-1	Monitor, Enterprise, and ER Gateway require each user to self identify before being allowed to perform any other actions. This implements FIA_UID.2* SFRs
20	FMT_MOF.1*	Management of security functions behaviour	M-MUA-12 M-CD-7 E-MUA-12 ER-MUA-4	Monitor allows SV Managers to set and configure the parameters of the account lockout feature. Monitor and Enterprise restrict the ability of changing the auditing events policy only to Developers. ER Gateway restricts the ability to determine the behavior of the functions listed in Table 5-5 to the authorized roles identified in Table 5-5. This implements FMT_MOF.1* SFRs

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
21	FMT_MSA.1*	Management of security attributes	M-MUA-4 E-MUA-4 ER-MUA-5	Monitor and Enterprise restrict the ability to query, modify, or delete the username, roles, and password- or certificate-based authentication security attributes to Account Manager. ER Gateway restricts the ability to query, modify, delete, and other operations as specified in Table 5-4 to the roles as specified in Table 5-4. This implements FMT_MSA.1* SFRs
22	FMT_MSA.3*	Static attribute initialization	M-MUA-5 E-MUA-5 ER-MUA-6	Monitor and Enterprise provide restrictive default values for security attributes as specified in Table 5-2 SecurVantageTM User Access Policy and allow the Account Manager to specify alternative initial values. ER Gateway enforces the SecurVantage™ ER User Access Policy to provide restrictive default values for security attributes and allows the ER Account Manager to specify alternative initial values. This implements FMT_MSA.3* SFRs

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
23	FMT_MTD.1	Management of TSF data	M-MUA-6 E-MUA-6 ER-MUA-7	Monitor and Enterprise restrict the ability to access data as specified in Table 5-2 SecurVantageTM User Access Policy. Monitor and Enterprise allow SV Managers to set and configure the parameters of the account lockout feature. • ER Gateway restricts the ability to access TSF data as specified in Table 5-5 Management of TSF Data. (FMT_MTD.1.1-2) This implements FMT_MTD.1* SFRs
24	FMT_MTD.2	Management of limits on TSF data	M-MUA-12 E-MUA-12 E-MUA-13 ER-MUA-12	Monitor and Enterprise allow SV Managers to set and configure the parameters of the account lockout feature. Enterprise allows SV Manager to set a threshold of violation compliance per domain. ER Gateway provides management of the account lockout feature. This implements FMT_MTD.2* SFRs
25	FMT_REV.1	Revocation	M-MUA-7 E-MUA-7	Monitor and Enterprise restrict the ability to revoke security attributes associated with users, subjects, and objects to Account Manager. This implements FMT_REV.1 SFR

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
26	FMT_SMF.1*	Specification of management functions	M-MUA-8 E-MUA-8	Monitor and Enterprise are capable of providing the security management functions as specified in Table 5-2 SecurVantageTM User Access Policy. ER Gateway is capable of providing the following security management functions: • Determining the behavior of the functions listed in Table 5-5 to the authorized roles identified in Table 5-5 (see FMT_MOF.1), • Query, modify, delete, and create as specified in Table 5-4 the security attributes as specified in Table 5-4 (see FMT_MSA.1), • Query, modify, delete, and create as specified in Table 5-4 and the TSF Data as specified in Table 5-4 (See FMT_MTD.1). This implements FMT_SMF.1* SFRs
27	FMT_SMR.1*	Security roles	M-MUA-9 E-MUA-9	Monitor and Enterprise maintain the roles Operator, Analyst, Developer, SV Manager, and Account Manager. ER Gateway maintains the roles ER SV Manager and ER Account Manager. (FMT_SMR.1.1-2, FMT_SMR.1.2-2) This implements FMT_SMR.1* SFRs
28	FPT_ITA.1	Inter-TSF availability within a defined available metric	M-CD-1	Monitor sends an email or SNMP message if a critical event is generated even when the web interface component is down This implements FPT_ITA.1 SFR

Mapping Functional Requirements to TOE Summary Specification				
No.	**Component**	**Component Name**	**TSS Ref. No**	**IT Security Function**
29	FPT_RVM_EXP.1.1-1 FPT_RVM_EXP.1.1-2	Non-bypassability of the TSP	M-MUA-10 E-MUA-10 ER-MUA-10	Monitor and Enterprise ensure that the Table 5-2 SecurVantageTM User Access Policy is invoked and succeeds before each function is allowed to proceed. ER Gateway ensures that the SecurVantage™ ER User Access Policy (See Table 5-3) is invoked and succeeds before each function is allowed to proceed. This implements FPT_RVM_EXP.1-1 SFR
30	FPT_SEP_EXP.1.1-1 FPT_SEP_EXP.1.2-1 FPT_SEP_EXP.1.1-2 FPT_SEP_EXP.1.2-2	TSF domain separation	M-MUA-11 E-MUA-11 ER-MUA-11	Monitor, Enterprise, and ER Gateway maintain a security domain for its own execution and enforce separation between security domains of users initiating actions through its own TSFI. This implements FPT_SEP_EXP.1.1-1, FPT_SEP_EXP.1.2-1, FPT_SEP_EXP.1.1-2, FPT_SEP_EXP.1.2-2 SFR
31	FTA_SSL.3*	TSF-initiated termination	M-UL-7 E-UL-7 ER-UL-8	Users session is terminated after 30 minutes of inactivity This implements FTA_SSL.3* SFRs
32	FTA_TSE.1	TOE session establishment	M-UL-5 E-UL-5 ER-UL-6	Monitor, Enterprise, and ER Gateway lock user accounts when consecutive failed login attempts are performed on a given account This implements FTA_TSE.1 SFR

8.3.2 Assurance Measures

Table 8-13 shows how the assurance measures are satisfied.

Table 8-13 Assurance Measures Rationale

Assurance Measures Rationale			
Component	**Evidence Requirements**	**How Satisfied**	**Rationale**

ACM_CAP.3	• CM Documentation
	  • CM Plan
	  • Configuration Item List
	  • CM Usage Evidence
		• Securify SecurVantage 5.0 Common Criteria Addendum
		• Securify SecurVantage 5.0 Manufacturing Procedures
		• Securify SecurVantage 5.0 Configuration Parameters
			• CM Plan
			  – describes the access controls used to control access to configuration items
			  – roles of individuals authorized to make changes to source code configuration items
			• Configuration Item List(s)
			  – is comprised of a list of the source code files and version numbers
			  – is comprised of a list of design documents with version numbers
			  – is comprised of test documents with version numbers
			  – user and administrator documentation with version numbers
			• CM Usage Evidence
			  – Shows that the CM system is operating in accordance with the CM plan. This includes samples of CM system records identifi ed in the CM plan and evidence that all CIs have been and are being effectively maintained under the CM system.

Assurance Measures Rationale			
Component	**Evidence Requirements**	**How Satisfied**	**Rationale**
ACM_SCP.1	TOE CM coverage	– Securify SecurVantage 5.0 CLI.xls - Securify SecurVantage 5.0 Lify Cycle Support Development Security.doc	Configuration Item List(s) − is comprised of a list of the source code files and version numbers − all evaluation evidence documentation required by evaluation with version numbers (Ex. design, test, user and administrator documents)
ADO_DEL.1	Delivery Procedures	The following document is provided to meet the ADO_DEL.1 requirements: − Manufacturing Procedures − Securify SecurVantage 5.0 EM Coversheet − Securify SecurVantage 5.0 Monitor Coversheet − Securify SecurVantage 5.0 Monitor LE Coversheet	Provides a description of all procedures that are necessary to maintain security when distributing TOE to the user's site. − Applicable across all phases of delivery from packaging, storage, distribution
ADO_IGS.1	Installation, generation, and start-up procedures	The following document is provided to meet the ADO_IGS.1 requirements: − SecurVantage™ Version 5.0 Installation Guide − SecurVantage™ 5.0 Deployment Guide − SecurVantage™ 5.0 Operations Guide − SecurVantage™ 5.0 Release Notes	Provides detailed instructions on how to install the TOE components.

Assurance Measures Rationale			
Component	**Evidence Requirements**	**How Satisfied**	**Rationale**
ADV_FSP.1	Functional Specification	Securify SecurVantage 5.0 Functional Specification-External Interfaces.xls	Provides rationale that TSF is fully represented
		The following documents are provided to meet the ADV_FSP.1 requirements: – SecurVantage™ Version 5.0 Installation Guide – SecurVantage™ Version 5.0 Operations Guide – Securify SecurVantage™ 5.0 Common Criteria Addendum – Securify SecurVantage™ 5.0 External Interfaces – Securify SecurVantage™ 5.0 Configuration Parameters – Securify SecurVantage™ 5.0 Database Functional Specification	Describes the TSF interfaces and TOE functionality
ADV_HLD.2	High-Level Design	Securify SecurVantage™ 5.0 HLD Securify SecurVantage™ 5.0 Common Criteria Addendum	Describes the TOE subsystems and their associated security functionality. Describe the sequences of actions that occur in each subsystem in response to stimulus at its interface.
ADV_RCR.1	Representation Correspondence	Securify SecurVantage™ 5.0 RCR	Provides the following two dimensional mappings: 1. TSS and functional specification; 2. Functional specification and high-level design.

Assurance Measures Rationale			
Component	**Evidence Requirements**	**How Satisfied**	**Rationale**
AGD_ADM.1	Administrator Guidance	– SecurVantage™ Version 5.0 WebUI Guide – SecurVantage™ Version 5.0 Studio Guide – SecurVantage™ Version 5.0 ER Guide - Securify SecurVantage™ 5.0 Common Criteria Addendum – Securify SecurVantage™ 5.0 Administrator Addendum	Describes how to administer the TOE securely.
AGD_USR.1	User Guidance	– SecurVantage™ Version 5.0 WebUI Guide – SecurVantage™ Version 5.0 Studio Guide – SecurVantage™ Version 5.0 ER Guide – Securify SecurVantage™ 5.0 Common Criteria Addendum – Securify SecurVantage™ 5.0 Administrator Addendum	Describes the secure use of the TOE.
ALC_DVS.1	Development Security Documentation	Securify Prodedures for Maintenance and Building of SecurVantage Systems.doc	Describes the physical, procedural, personnel, and other security measures necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ATE_COV.2	Test Coverage Analysis	Securify SecurVantage™ 5.0 Test Matrix.xls	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_DPT.1	Depth of Testing analysis	Securify SecurVantage™ 5.0 Test Matrix.xls	Demonstrates that the TSF operates in accordance with its High-Level Design.

Assurance Measures Rationale			
Component	**Evidence Requirements**	**How Satisfied**	**Rationale**
ATE_FUN.1	Test Documentation	Securify SecurVantage™ 5.0 Test Matrix.xls	Test documentation includes test plans and procedures and expected and actual results.
ATE_IND.2	TOE for Testing	– TOE for Testing – Sentinel tool	The TOE will be provided for testing.
AVA_MSU.1	Misuse Analysis	– SecurVantage™ Version 5.0 WebUI Guide – SecurVantage™ Version 5.0 Studio Guide – SecurVantage™ Version 5.0 ER Guide – Securify SecurVantage 5.0 Common Criteria Addendum – Securify SecurVantage 5.0 Administrator Addendum	The guidance documentation shall be analyzed and demonstrated to be complete.
AVA_SOF.1	SOF Analysis	– Securify SecurVantage™ 5.0 Common Criteria Addendum – Securify SecurVantage™ 5.0 Vulnerability 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	Vulnerability Analysis	Securify SecurVantage™ 5.0 Vulnerability Analysis	Provide an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.3.3 Strength of Function

The M-MUA-2 and E-MUA-2, and ER_MUA-2 security functions' strength of function level is SOF-Basic. These security functions implement the FIA_SOS.1*, Verification of secrets, security functional requirement, and the SOF-Basic level is consistent with the strength of function level for the FIA_SOS.1* functional requirement.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.

9 Acronyms

CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
IT	Information Technology
NTP	Network Time Protocol
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy