Securify

SecurVantage™ Version 3.1

Security Target V2.0

Robin Medlock

Debra Baker

January 26, 2004

Suite 100 West♦7927 Jones Branch Drive♦McLean, VA 22102-3305♦703 848-0883♦Fax 703 848-0960

Revision History:

Date:	Version:	Author:	Description
11/15/2002	0.1	Robin Medlock	First Draft for Securify SecurVantage™
01/10/2003	0.2	Robin Medlock	Second Draft
01/21/2003	1.0	Robin Medlock	NIAP Version
04/29/2003	1.1	Robin Medlock	Interim Version, contains responses to EORs
05/21/2003	1.2	Robin Medlock	Interim Version, contains responses to additional EORs
08/29/2003	1.3	Robin Medlock	Interim Version, contains responses to additional EORs
11/19/2003	1.4	Debra Baker	Interim Version, responses to EOR and validator comments
11/19/2003	1.5	Debra Baker	Interim Version, responses to EOR and validator comments
12/1/2003	1.6	Debra Baker	Responses to EOR and validator comments
1/16/2004	1.7	Debra Baker	Responses to validator comments
1/21/2004	1.8	Debra Baker	Responses to validator comments; TOE version number update
1/21/2004	1.9	Debra Baker	Reference section updated
1/26/2004	2.0	Debra Baker	Numbering corrected in section 2.2

TABLE OF CONTENTS

SECTION **PAGE**

Figures and Tables

Figure **Page**

Table **Page**

1 Security Target Introduction

1.1 *Security Target Identification*

TOE Identification:

Securify SecurVantage™ Studio: 3.1 (Tag V31-CC-110)

Securify SecurVantage™ Monitor (SM): 3.1 (Tag V31-CC-B-111) with patches

Managecert-v1

Txn-log-truncate-patch

Collected-patches2

Presence

Securify SecurVantage™ Monitor (Harvester): 3.1 (Tag V31-CC-B-111) with patches

Collected-patches2

Presence

Securify SecurVantage™ Monitor (LE): 3.1 (Tag V31-CC-B-111) with patches

Managecert-v1

Collected-patches2

LE533-Patch

Presence

Securify SecurVantage™ Enterprise: 3.1 (Tag V31-CC-110) with patches

Managecerts-v1

Txn-log-truncate-patch

Collected-patches2

ST Title:	Securify SecurVantage™ Version 3.1 Security Target
ST Version:	Version 2.0
ST Authors:	Robin Medlock, Debra Baker
ST Date:	January 26, 2004
Assurance level:	EAL2
Registration:	<To be filled in upon registration>
Keywords:	Network Security, Monitoring, Analysis, Identification, Authentication, Access Control, Audit, and Security Target

1.2 *Interpretations*

This Security Target incorporates the following International and National Interpretations:

Interpretation	Description
CCIMB 003	Unique identification of configuration items in the configuration list
CCIMB 051	Use of documentation without C & P elements
CCIMB 058	Confusion over refinement
CCIMB 065	No component to call out security function management
NIAP-0347	Including Sensitive Information In Audit Records
NIAP-0407	Empty Selections Or Assignments
NIAP-0409	Other Properties In FMT_MSA.3 Should Be Specified By Assignment
NIAP-0412	Configuration Items in The Absence Of Configuration Management
NIAP-0416	Association Of Access Control Attributes With Subjects And Objects
NIAP-0422	Clarification Of Audit Records
NIAP-0423	Some Modifications To The Audit Trail Are Authorized
NIAP-0429	Selecting One Or More

1.3 *Security Target Overview*

This Security Target (ST) defines the Information Technology (IT) security requirements for Securify SecurVantage™ Version 3.1. 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-specific policy that formally describes the desired operation of the network.

1.4 *Common Criteria Conformance*

The TOE is Part 2 conformant, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.1.

1.5 *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 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 the Appendices.

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 three major components:

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

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 limitation) 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.

Limitations:

SecurVantage Monitor audits IPv4 packets when transported over Ethernet frames with length less than 1518 bytes. Notice that this doesn't include IPv6 packet nor Ethernet Jumbo frames. These types of packets are discarded without logging.

Administrators are advised to configure any switch that maybe 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 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:

1. Source and destination IP addresses, the derived policy network objects, network object names, and services that those IP addresses resolve to

2. Outcome component assigned, including: protocol, outcome, protocol component, and criticality

3. Owner: either the outcome, service or reporting element owner in that order of precedence

4. Source and destination routing objects to provide IP routing information

5. 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 is one of the following options: Critical, High, Medium, Warning, Monitor, Informational, or Ok. All events other than 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 only 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 a severity associated to it. Monitor compares the event with a local copy of the Security Policy (previously uploaded by the user) and logs the events according to the assigned severity as specified in the Security Policy. Logged traffic and Critical events (Alerts) are stored in the Monitor database so it can be accessed via Monitor web interface or through Studio. Data is stored in the Monitor for a window of time (In 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 Enterprise and aggregates them 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 Studio application.

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

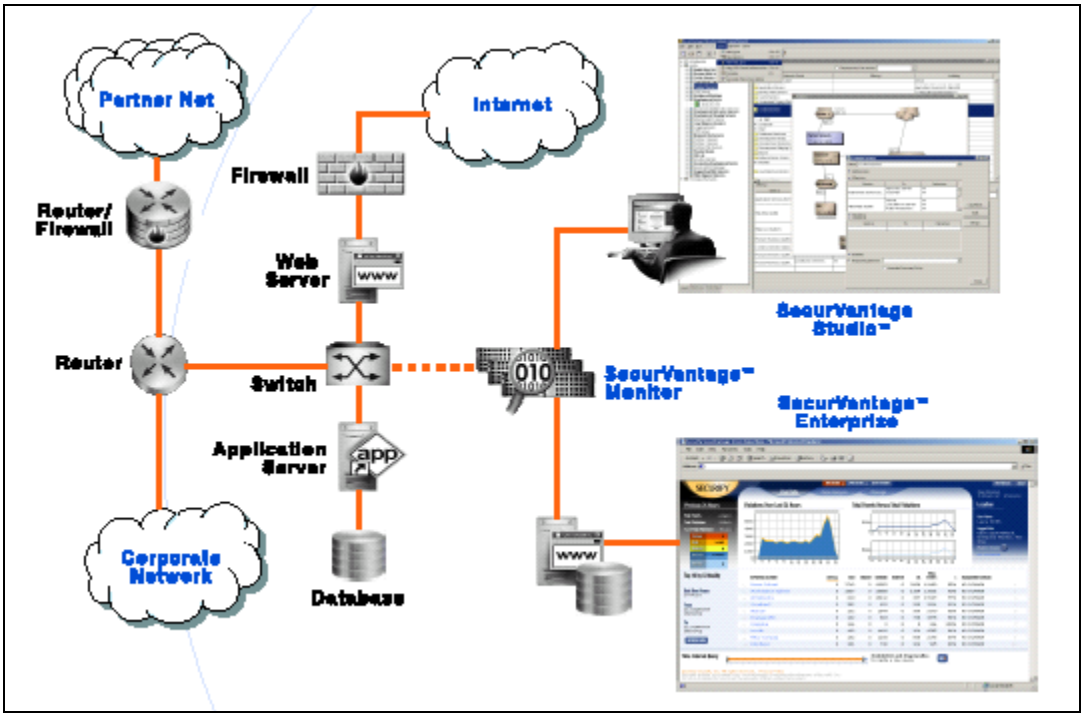

Figure 2-1 Typical SecurVantage™ Deployment

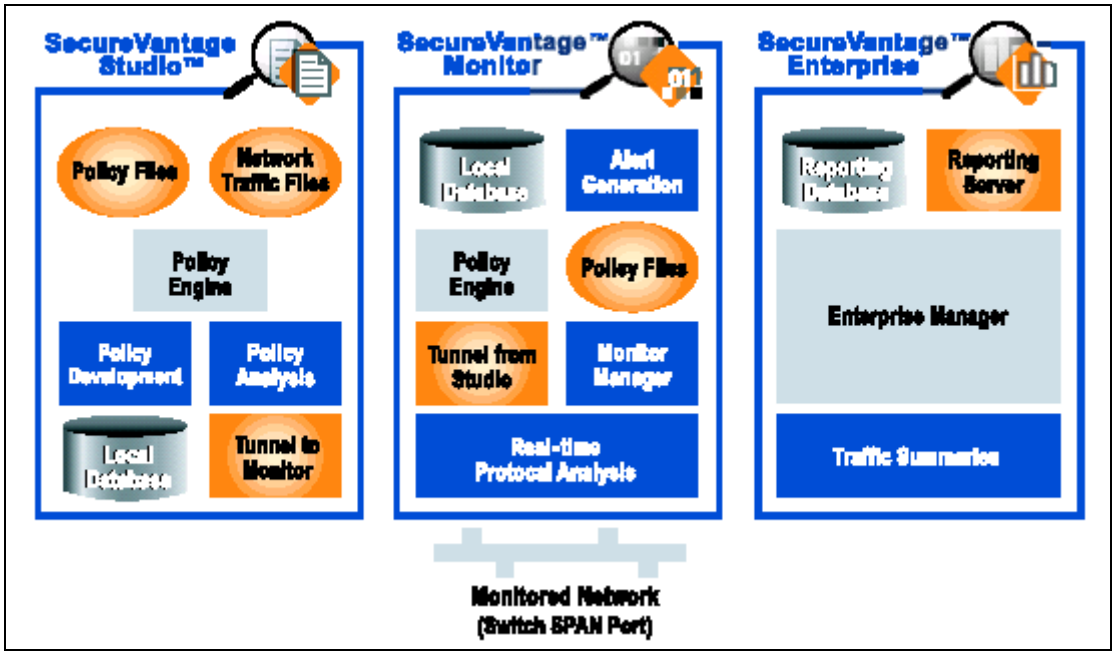

Figure 2-2 SecurVantage™ System Architecture

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 below in Figure 2-3. Network objects are functional groups of devices that exhibit a similar network function or behavior.

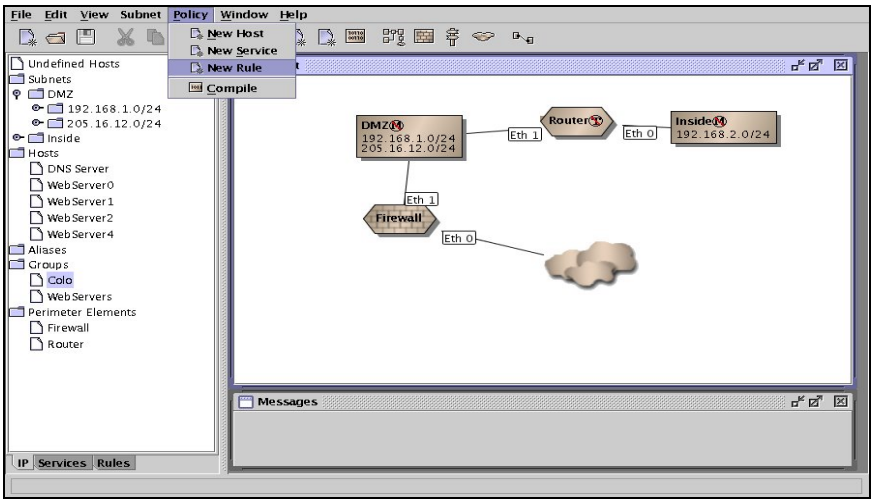

Figure 2-3 Defining Topology

Using Rules to Tie Together Network Objects: The Security Policy is a set of rules, which are used to create a set of relationships between network objects that 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 behavior 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 NetworkTraffic : The Monitor can be configured to capture (and make available to Studio) network traffic (in files) before policy evaluation occurs on the Monitor. These files are called DME files. The Studio can be made 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 are 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 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 NetworkTraffic : 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).

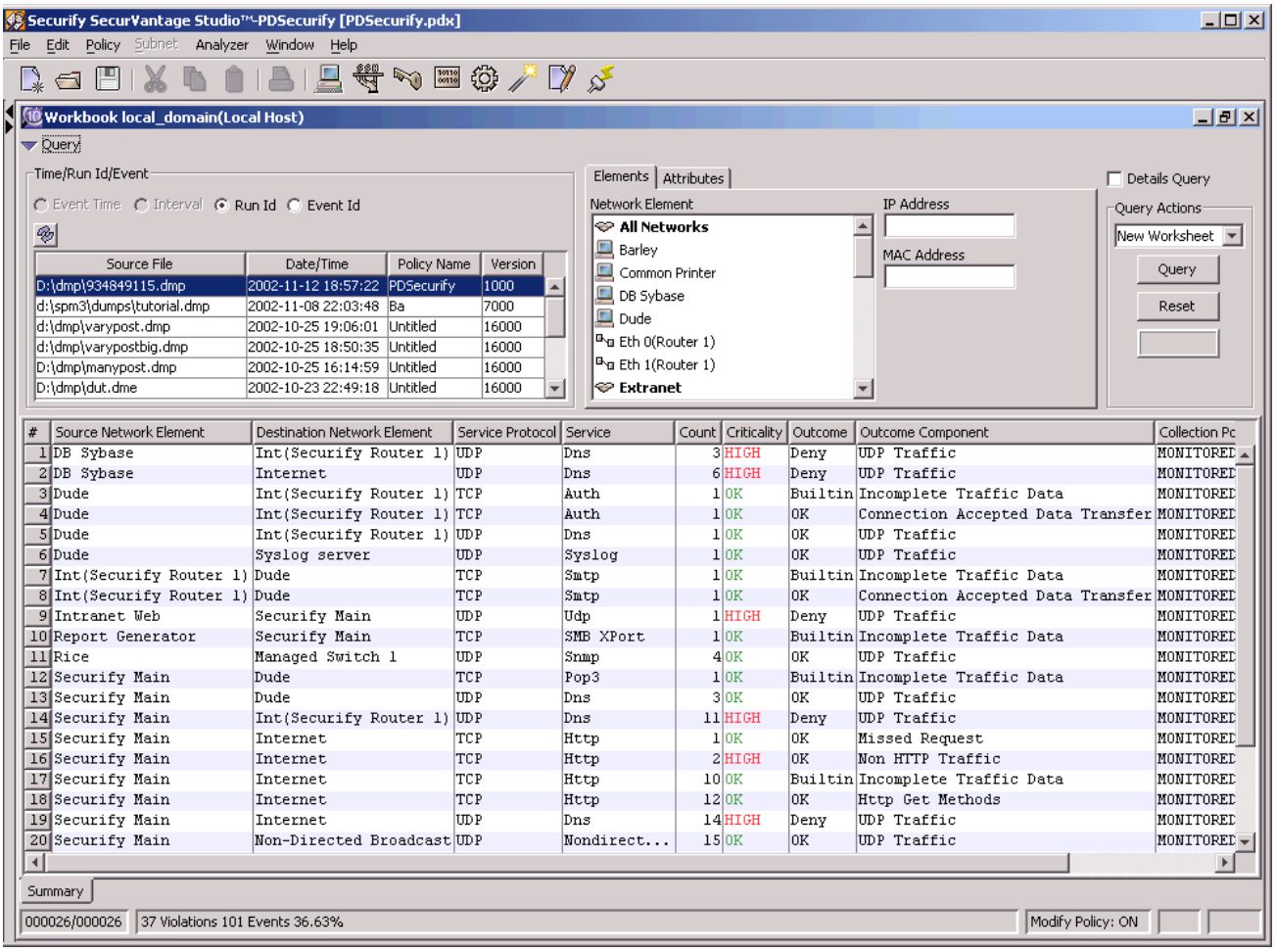

Figure 2-4 Policy Analysis

.

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. The Monitor is available in two forms: one form as a high bandwidth version consisting of two systems (Securify SecurVantage Monitor) and 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 that are specific to the business and actionable for 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; the Account Manager role to administer user accounts and a Super-user role with an “all roles” capability.

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. In addition, as mentioned before, users can access through Securify SecurVantage Studio a window of data of 4 weeks or more depending upon the density of the network events.

Auditing: SecurVantage Monitor and Monitor LE store in a local database the result of evaluating network traffic that is being monitored into the database. These records cannot be deleted or modified. A copy of events logged as critical are also kept in a different table called Alerts, to ease management of the 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 store in the database. That is to say that users can delete alerts but not the original data. In addition, SecurVantage Monitor and Monitor LE keep an auditing trail of every transaction that occur in the system. These audit trails are referred 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-timeweb 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, and 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 a group of Monitors. This is called a “Policy Domain”. A monitor can run only one policy, but a policy can run on multiple Monitors. The resulting network events can be viewed on the SecurVantage Enterprise by 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; the Account Manager role to administer user accounts and a Super-user role with an “all roles” capability.

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™ 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's Monitors 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. 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).

2.3 *TSF Boundary and Scope of the Evaluation*

The evaluated configuration includes the following:

- SecurVantage™ Studio 3.1 (Tag V31-CC-110) running on Microsoft Windows 2000
- SecurVantage™ Monitor 3.1 (Tag V31-CC-B-111) with Patches (specified in Section 1.1)(Security Master and Harvester) running on Linux Red Hat 7.2
- SecurVantage™ Monitor LE 3.1 (Tag V31-CC-B-111) with Patches (specified in Section 1.1) running on Linux Red Hat 7.2
- SecurVantage™ Enterprise 3.1 (Tag V31-CC-110) with Patches (specified in Section 1.1) running on Linux Red Hat 7.2

The TOE includes the SecurVantage™ Studio, Monitor, Monitor LE, and Enterprise software along with the underlying Sybase databases, but it does not include the underlying operating system software or hardware. The TOE also does not include the third-party encryption software that is used to provide protection of data transfer between the major TOE components, and to provide a trusted communication path between administrators and the TOE. The underlying operating system software and hardware, Tomcat, Apache, OpenSSL, and PureTLS encryption software are part of the TOE environment.

2.4 *TOE Functionality*

SecurVantage™ provides the following security functions:

- Security Audit
- Access Control
- User Identification and Authentication
- Security Management

2.5 *TOE 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 software to provide protection of data transfer between TOE components and for a trusted communication path between authorized administrators and the TOE.

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.

Intended Usage Assumptions

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.Trusted	There will be no untrusted users of the TOE and no untrusted software loaded on the TOE host platforms.

Physical Assumptions

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

Personnel Assumptions

A.Admin	The administrator is trusted to correctly configure 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.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.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 the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides.

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

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.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.BadPassword	Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorized access to the TOE.
T.Bypass	An attacker may attempt to bypass TSF security functions.

T.BypassDisclosure	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
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.DataLoss	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
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.ImpConfig	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.OFlows	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
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.Privil	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and 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.Tamper	An attacker may attempt to modify TSF programs and data.
T.Transmit	TSF data may be disclosed or modified by an attacker while being transmitted between TOE components.
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.

P.Accact	Users of the TOE shall be accountable for their actions within the system.
P.Access	All data collected and produced by the TOE shall only be used for authorized purposes.
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.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.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:

O.Access	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.Admin	The TOE must provide the functionality to enable an authorized user to effectively manage the TOE and its security functions.
O.Audit	The TOE must record audit records for data accesses and use of the system functions.
O.DataIntegrity	The TOE must ensure the integrity of all audit and system data.
O.IDAnlz	The TOE must accept data and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.IDAuth	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
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.
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.MultipleAuthen	The TOE must provide multiple authentication mechanisms.
O.NonBypass	The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.
O.OFlows	The TOE must appropriately handle potential audit and system data storage overflows.
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.PasswordQual	The TOE must be able to specify password rules strong enough to deter password guessing.
O.ProtectAuth	The TOE will provide protected authentication feedback.
O.Revoke	The TOE will allow authorized users to revoke security attributes within the TSC.
O.Roles	The TOE must support multiple administrative roles.

4.2 *Security Objectives for the Environment*

The TOEs 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 objective for the IT environment is as follows:

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.
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.
OE.NonBypass	The IT environment must ensure that its protection mechanisms cannot be bypassed.
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.Time	The IT environment must provide reliable time stamps.

4.2.2 Non-IT Security Objectives

The Non-IT security objectives are as follows:

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.
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.
ON.Operations	There must be procedures in place in order to ensure that the TOE will be managed and operated in a secure manner.
ON.Password	Personnel working as authorized administrators and users must follow the TOE guidance about choosing good passwords.
ON.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
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.

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

No.	Component	Component Name
1.	FAU_ARP.1	Security alarms
2.	FAU_GEN.1-NIAP_0347	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-NIAP-0407	Selective audit
8.	FAU_STG.2-NIAP-0429	Guarantees of audit data availability
9.	FAU_STG.4-NIAP-0429	Prevention of audit data loss
10.	FDP_ACC.2	Complete access control
11.	FDP_ACF.1-NIAP-0407	Security attribute based access control
12.	FIA_ATD.1	User attribute definition
13.	FIA_SOS.1	Verification of secrets
14.	FIA_UAU.2	User authentication before any action
15.	FIA_UAU.5	Multiple authentication mechanisms
16.	FIA_UAU.7	Protected authentication feedback
17.	FIA_UID.2	User identification before any action
18.	FMT_MSA.1	Management of security attributes
19.	FMT_MSA.3-NIAP-0429	Static attribute initialisation
20.	FMT_MTD.1	Management of TSF data
21.	FMT_REV.1	Revocation
22.	FMT_SMF.1	Specification of management functions
23.	FMT_SMR.1	Security roles

No.	Component	Component Name
24.	FPT_RVM.1-1	Non-bypassability of the TSP
25.	FPT_SEP.1-1	TSF domain separation

Operations on IT security requirements are identified as follows:

- Iteration – component number if distinguished by appending a number, preceded by a hyphen. Example: FIA_UAU.7.1-1
- 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.
- Interpretations – Full reference to CCIMB and NIAP interpretations is only used in Section 5, but not in Section 8 for readability.

5.1.1 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 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.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_GEN.1-NIAP-0347 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1-NIAP-0429 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;

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-NIAP-0347 The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***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 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 The TSF shall be able to maintain an internal representation of the following signature events [***customer-specified protocol and network events***] 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 data***].

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 Audit review

Hierarchical to: No other components.

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

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

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

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

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

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

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

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 [***customer-specified 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, Informational, or Ok.

FAU_SEL.1-NIAP-0407 Selective audit

Hierarchical to: No other components.

FAU_SEL.1.1-NIAP-0407 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, Informational, or Ok.

FAU_STG.2-NIAP-0429 Guarantees of audit data availability

Hierarchical to: FAU_STG.1

FAU_STG.2.1-NIAP-0422 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.2.2-NIAP-0429 The TSF shall be able to [***prevent***] unauthorized modifications to the audit records in the audit trail.

FAU_STG.2.3 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-NIAP-0429 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1-NIAP-0429 The TSF shall [***overwrite the oldest stored audit records***] and ***[take no other actions***] if the audit trail is full.

Dependencies: FAU_STG.1 Protected audit trail storage

5.1.2 Class FDP: User Data Protection

FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1

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

FDP_ACC.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 5-2 SecurVantage™ User Access Policy

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

FDP_ACF.1-NIAP-0407 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1-NIAP-0416 The TSF shall enforce the [***Table 5-2 SecurVantageTM User Access Policy***] to objects based on the following: [***See Table 5-2***].

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

FDP_ACF.1.3-NIAP-0407 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***no additional rules***].

FDP_ACF.1.4-0407 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 initialisation

5.1.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

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

Dependencies: No dependencies

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [***Minimum of 8 characters in the password;***

- ***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 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 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 Multiple authentication mechanisms

Hierarchical to: No other components.

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

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

Dependencies: No dependencies

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

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

FIA_UAU.7.1-2 The TSF shall provide only [***a X.509 or PKCS 12 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 User identification before any action

Hierarchical to: FIA_UID.1

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

Dependencies: No dependencies

5.1.4 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.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 and Super User***].

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 (CCIMB 065)

FMT_MSA.3-NIAP-0429 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1-NIAP-0429 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 *SF*P.

FMT_MSA.3.2 The TSF shall allow the [***Account Manager and Super User***] 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 Management of TSF data

Hierarchical to: No other components.

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

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

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

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

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

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

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

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

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

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

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

Dependencies: FMT_SMF.1 Specification of Management Functions

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 and Super User***].

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

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.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***]

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

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

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

Dependencies: FIA_UID.1 Timing of identification

5.1.5 Class FPT: Protection of the TSF

FPT_RVM.1-1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1-1 The TSF 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.1-1 TSF domain separation

Hierarchical to: No other components.

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

Dependencies: No dependencies

5.2 *TOE Security Assurance Requirements*

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components is refined. The assurance components are listed in Table 5-3.

Table 5-3 EAL2 Assurance Components

Component	Component Title
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

5.3 *Security requirements for the IT Environment*

SecureVantage™ Studio, Monitor, and Enterprise require that the operating systems provide non-bypassability of the TSP and TSF domain separation. SecureVantage™ Monitor and Enterprise require that a Network Time Protocol (NTP) Server provide reliable time stamps.

SecureVantage™ Studio, Monitor, and Enterprise require third party SSL or TLS software to provide basic internal TSF transfer protection. SecureVantage™ Monitor and Enterprise require this third party SSL or TLS software to provide a trusted path between the TSF and users.

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

FPT_RVM.1-2 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1-2 The ***IT environment*** 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.1-2 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1-2 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.1.2-2 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 requirement.

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

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) - Operator, Analyst, Developer, and Super User can read live Event Data - Operator, Analyst, Developer, and Super User can read Alerts 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)
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)

User Login function:

S-UL-1	Studio provides the certificate dialog box when certificate-based authentication is used. (FIA_UAU.7.1-2)

6.1.3 SecurVantage™ Monitor

Manage User Access function:

M-MUA-1	Monitor maintains the following information for each user: user name, e-mail address, hash of the password or certificate, roles, and whether authentication is password or certificate based. (FIA_ATD.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)
M-MUA-3	Monitor enforces the SecurVantage™ User Access Policy (See Table 5-2 SecurVantageTM User Access Policy) (FDP_ACC.2) (FDP_ACF.1)
M-MUA-4	Monitor restricts the ability to query, modify, or delete the user-name, roles, and password- or certificate-based authentication security attribute to Account Manager and Super User. (FMT_MSA.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 and Super User to specify alternative initial values. (FMT_MSA.3)
M-MUA-6	Monitor restricts the ability to access data as specified in Table 5-2 SecurVantageTM User Access Policy. (FMT_MTD.1)
M-MUA-7	Monitor restricts the ability to revoke security attributes associated with users, subjects, and objects to Account Manager and Super User. (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)
M-MUA-9	Monitor maintains the roles Operator, Analyst, Developer, SV Manager, Account Manager, and Super User. (FMT_SMR.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.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.1-1)

User Login function:

M-UL-1	Monitor requires each user to identify himself/herself before being allowed to perform any other actions. (FIA_UID.2)
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)
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)
M-UL-4	Monitor provides only confirmation of user name and asterisks for password when password authentication is used. (FIA_UAU.7.1-1)

Collect Data Function:

M-CD-1	Monitor sends an email or SNMP message if a critical event is generated. (FAU_ARP.1)

M-CD-2	Monitor is able to generate audit records. (FAU_GEN.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)

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)
M-CD-6	Monitor overwrites the oldest stored audit records if the audit trail is full. (FAU_STG.4)

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) - Operator, Analyst, Developer, and Super User can read Event Data - Operator, Analyst, Developer, and Super User can read Alerts - SV Manager and Super User can read Application Log data - Account Manager and Super User 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 that have been granted explicit read access. (FAU_SAR.2)
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

Manage User Access function:

E-MUA-1	Enterprise maintains the following information for each user: user name, e-mail address, hash of the password or certificate, roles, and whether authentication is password or certificate-based. (FIA_ATD.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)
E-MUA-3	Enterprise enforces the SecurVantage™ User Access Policy (See Table 5-2 SecurVantageTM User Access Policy) (FDP_ACC.2) (FDP_ACF.1)

E-MUA-4	Enterprise restricts the ability to query, modify, or delete the user-name, roles, and password- or certificate-based authentication security attribute to Account Manager and Super User. (FMT_MSA.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 and Super User to specify alternative initial values. (FMT_MSA.3)
E-MUA-6	Enterprise restricts the ability to access data as specified in Table 5-2 SecurVantageTM User Access Policy. (FMT_MTD.1)
E-MUA-7	Enterprise restricts the ability to revoke security attributes associated with users, subjects, and objects to Account Manager and Super User. (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)
E-MUA-9	Enterprise maintains the roles Operator, Analyst, Developer, SV Manager, Account Manager, and Super User. (FMT_SMR.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.1-1)
E-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.1-1)

User Login function:

E-UL-1	Enterprise requires each user to identify himself/herself before being allowed to perform any other actions. (FIA_UID.2)
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)
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)
E-UL-4	Enterprise provides only confirmation of user name and asterisks for password when password authentication is used. (FIA_UAU.7.1-1)

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)

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) - Operator, Analyst, Developer, and Super User can read Event Data - Operator, Analyst, Developer, and Super User can read Alerts - SV Manager and Super User can read Application Log data - Account Manager and Super User 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 that have been granted explicit read access. (FAU_SAR.2)
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)

6.2 Assurance Measures

SecurVantage™ satisfies the assurance requirements for Evaluation Assurance Level EAL2. 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 and E-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 all 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.	Organisational 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.IDAniz: 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 the identified threats to security are countered by Security Objectives for the TOE.

Table 8-2 All Threats to Security Countered

TOE Threat Name	Threat Description	Security Objective
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
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
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
T.Bypass	An attacker may attempt to bypass TSF security functions	O.PartialDomainSep O.NonBypass OE.NonBypass
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

TOE Threat Name	Threat Description	Security Objective
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
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
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
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
T.OFlows	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.	O.OFlows
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
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
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
T.Tamper	An attacker may attempt to modify TSF programs and data.	O.PartialDomainSep OE.PartialDomainSep
T.Transmit	TSF data may be disclosed or modified by an attacker while being transmitted between TOE components.	OE.ComIntegrity OE.Confidentiality
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 record 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 an 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.PasswordQual: The TOE must be able to specify password rules strong enough to deter password guessing. Forcing 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 with 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.
- 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 only permitting 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 will allow users to authenticate themselves by either id and password or id and certificate. By having multiple authentication mechanisms such as certificates it will make it difficult for an unauthorized user to impersonate another 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. This will allow administrators 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 data will be maintained. 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 only permitting 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.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. This will allow administrators 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 only permitting authorized users to access 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. This will allow administrators 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 only permitting authorized users to access 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 which includes 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 only permitting authorized users to access 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. This will allow administrators 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 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 toeffectively 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 only permitting authorized users to access 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 will allow users to authenticate themselves by either id and password or id and certificate. By having multiple authentication mechanisms such as certificates it will make 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 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.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 record 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 an 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

No.	Objective Name	Threat
1.	O.Access	T.Abuse T.Access T.BypassDisclosure T.BypassIntegrity T.DataLoss T.Halt T.ImpConfig T.Privil A.Trusted
2.	O.Admin	T.ImpConfig T.Mismanage
3.	O.Audit	T.Abuse T.Undetect
4.	O.DataIntegrity	T.DataLoss
5.	O.PartialDomainSep	T.Access T.Bypass T.BypassDisclosure T.BypassIntegrity T.DataLoss T.Tamper T.Privil
6.	O.IDAnlz	T.Halt

No.	Objective Name	Threat
7.	O.IDAuth	T.Abuse T.BypassDisclosure T.BypassIntegrity T.DataLoss T.Halt T.Privil T.ImpConfig
8.	O.IDSens	T.Halt
9.	O.ManageData	T.Mismanage
10.	O.MultipleAuthen	T.BypassDisclosure T.Privil
11.	O.NonBypass	T.Bypass T.BypassDisclosure T.BypassIntegrity
12.	O.OFlows	T.OFlows
13.	O.PasswordQual	T.BadPassword
14.	O.ProtectAuth	T.Privil
15.	O.Revoke	T.BypassDisclosure T.BypassIntegrity T.DataLoss T.ImpConfig
16.	O.Roles	T.Mismanage
17.	OE.ComIntegrity	T.RemoteAttack T.Transmit
18.	OE.Confidentiality	T.BypassDisclosure T.RemoteAttack T.Transmit
19.	OE.PartialDomainSep	T.BypassDisclosure T.BypassIntegrity T.DataLoss T.Privil T.Tamper
20.	OE.NonBypass	T.Bypass T.BypassDisclosure T.BypassIntegrity
21.	OE.Time	T.Abuse T.Undetect

8.1.3 Assumptions

Table 8-4 shows that all Security Objectives for the Environment map to identified secure usage assumptions.

Table 8-4 Mapping of Non-IT Security Objectives for the Environment to Assumptions

No.	Objective Name	Threat/Policy/Assumption
1.	ON.Creden	A.NoEvil

No.	Objective Name	Threat/Policy/Assumption
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

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

Table 8-5 All Assumptions Addressed

Name	Assumption	Objective
A.Admin	The administrator is trusted to correctly configure the TOE.	ON.Install ON.Operations
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
A.Trusted	There will be no untrusted users of the TOE and no un-trusted software loaded on the TOE host platforms.	O.Access
A.Protct	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	ON.Phycal
A.Locate	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	ON.Phycal
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
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
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: There must be procedures in place in order to ensure that the TOE will be managed and operated in a secure manner. The 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 O.Access:

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

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:

- OnInstall: 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: There must be procedures in place in order to ensure that the TOE will be managed and operated in a secure manner. The 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 shows that all of the security objectives of the TOE are satisfied.

Table 8-6 All Objectives Met by Functional Components

Objective	Objective Description	Security Functional or Assurance Requirement
O.Access	The TOE must allow authorized users to access only appropriate TOE functions and data.	FAU_SAR.2 FAU_STG.2-NIAP-0429 FDP_ACC.2 FDP_ACF.1 FIA_UAU.2 FIA_UID.2 FMT_MTD.1 FMT_SMF.1
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-NIAP-0407 FMT_MSA.1 FMT_MSA.3-NIAP-0429 FMT_MTD.1 FMT_SMF.1
O.Audit	The TOE must record audit records for data accesses and use of the system functions.	FAU_GEN.1-NIAP_0347 FAU_SEL.1-NIAP-0407
O.DataIntegrity	The TOE must ensure the integrity of all audit data.	FAU_STG.2-NIAP-0429 FMT_MTD.1
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.1-1
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
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
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
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
O.MultipleAuthen	The TOE must provide multiple authentication mechanisms.	FIA_UAU.5

Objective	Objective Description	Security Functional or Assurance Requirement
O.NonBypass	The TOE must ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.	FPT_RVM.1-1
O.OFlows	The TOE must prevent audit and System data storage overflows.	FAU_STG.4
O.PasswordQual	The TOE must be able to specify password rules strong enough to deter password guessing.	FIA_SOS.1
O.ProtectAuth	The TOE will provide protected authentication feedback.	FIA_UAU.7
O.Revoke	The TOE will allow authorized users to revoke security attributes within the TSC.	FMT_REV.1
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 of 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, which 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, which 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, which requires each user to be successfully authenticated before allowing access to the TOE.
- FIA_UID.2 User identification before any action, which requires that users be successfully identified before allowing access to the TOE.
- FMT_MTD.1 Management of TSF data, which requires that only authorized administrators of the system may query network event data and can delete alert data.
- FMT_SMF.1 Specification of management functions, which 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, which requires that the auditor be able to read audit records.
- FAU_SAR.3 Selectable audit review, which requires that the TSF will provide the ability to search, sort, and order audit data.
- FAU_SEL.1 Selective audit, which requires the TOE to provide authorized users with the ability to include or exclude auditable events from the set of audited events.
- FMT_MSA.1 Management of security attributes, which requires only authorized users can query, modify, and delete specified security attributes.
- FMT_MSA.3 Static attribute initialization, which requires the TSF enforce access control for specified default values of security attributes.

- FMT_MTD.1 Management of TSF data, which requires that only authorized administrators of the system may query network event data and can delete alert data.
- FMT_SMF.1 Specification of management functions, which requires that the TSF provide specific management functions.

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

- FAU_GEN.1 Audit data generation, which requires the ability to audit specified events.
- FAU_SEL.1 Selective audit, which provides the TOE with the capability to select which security-relevant events to audit.

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

- FAU_STG.2 Guarantees of 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 requires that only authorized administrators of the system may 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.1-1 TSF domain separation, which 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, which requires each user to be successfully authenticated before allowing access to the TOE.
- FIA_UID.2 User identification before any action, which 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 of 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 requires that only authorized administrators of the system may query network event data and can delete alert data.

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

- FIA_UAU.5 Multiple authentication mechanisms, which requires that the TSF provide multiple authentication mechanisms for user 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.1-1 Non-bypassability of the TSP, which required that the TSF ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

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, which 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, which 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 astericks for the password for password authentication.

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, which 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

Objective	Objective Description	Requirement for the IT Environment	Component Title
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.	FPT_ITT.1	Basic internal TSF data transfer protection
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.	FPT_ITT.1	Basic internal TSF data transfer protection

Objective	Objective Description	Requirement for the IT Environment	Component Title
		FTP_TRP.1	Trusted path
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.1-2	TSF domain separation
OE.NonBypass	The TOE must ensure that its protection mechanisms cannot be bypassed.	FPT_RVM.1-2	Non-bypassability of the TSP
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, and 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, 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. 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.1-2: 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.1-2: 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

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
12.	FIA_ATD.1	User attribute definition	O.ManageData
13.	FIA_SOS.1	Verification of secrets	O.PasswordQual
14.	FIA_UAU.2	User authentication before any action	O.Access O.IDAuth
15.	FIA_UAU.5	Multiple authentication mechanisms	O.MultipleAuthen
16.	FIA_UAU.7	Protected authentication feedback	O.ProtectAuth
17.	FIA_UID.2	User identification before any action	O.Access O.IDAuth
18.	FMT_MSA.1	Management of security attributes	O.Admin
19.	FMT_MSA.3	Static attribute initialisation	O.Admin
20.	FMT_MTD.1	Management of TSF data	O.Access O.Admin O.DataIntegrity O.ManageData
21.	FMT_REV.1	Revocation	O.Revoke
22.	FMT_SMF.1	Specification of management functions	O.Access O.Admin

No.	Requirement	Component Name	Objective
23.	FMT_SMR.1	Security roles	O.Roles
24.	FPT_RVM.1-1	Non-bypassability of the TSP	O.NonBypass
25.	FPT_SEP.1-1	TSF domain separation	O.PartialDomainSep

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 IT environment to Objectives for the IT environment

#	Requirement	Objective
1.	FPT_ITT.1	OE.ComIntegritiy OE.Confidentiality
2.	FPT_RVM.1-2	OE.NonBypass
3.	FPT_SEP.1-2	OE.PartialDomainSep
4.	FPT_STM.1	OE.Time
5.	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 denoted by an *(H)* following the dependency reference.

Table 8-10 Dependencies for TOE

No.	Component	Component Name	Dependencies	Reference
1.	FAU_ARP.1	Security alarms	FAU_SAA.1	3 (H)
2.	FAU_GEN.1	Audit data generation	FPT_STM.1	Environment
3.	FAU_SAA.3	Simple attack heuristics	None	None
4.	FAU_SAR.1	Audit review	FAU_GEN.1	2
5.	FAU_SAR.2	Restricted audit review	FAU_SAR.1	4
6.	FAU_SAR.3	Selectable audit review	FAU_SAR.1	4
7.	FAU_SEL.1	Security audit event selection	FAU_GEN.1	2
			FMT_MTD.1	20
8.	FAU_STG.2	Guarantees of audit data availability	FAU_GEN.1	2
9.	FAU_STG.4	Prevention of audit data loss	FAU_STG.1	8 (H)
10.	FDP_ACC.2	Complete access control	FDP_ACF.1	11
11.	FDP_ACF.1	Security attribute based access control	FDP_ACC.1	10 (H)
			FMT_MSA.3	19
12.	FIA_ATD.1	User attribute definition	None	None
13.	FIA_SOS.1	Verification of secrets	None	None

No.	Component	Component Name	Dependencies	Reference
14.	FIA_UAU.2	User authentication before any action	FIA_UID.1	17 (H)
15.	FIA_UAU.5	Multiple authentication mechanisms	None	None
16.	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	14 (H)
17.	FIA_UID.2	User identification before any action	None	None
18.	FMT_MSA.1	Management of security attributes	[FDP_ACC.1 or FDP_IFC.1]	10 (H)
			FMT_SMF.1	22
			FMT_SMR.1	23
19.	FMT_MSA.3	Static attribute initialisation	FMT_MSA.1	18
			FMT_SMR.1	23
20.	FMT_MTD.1	Management of TSF data	FMT_SMF.1	22
			FMT_SMR.1	23
21.	FMT_REV.1	Revocation	FMT_SMR.1	23
22.	FMT_SMF.1	Specification of management functions	None	None
23.	FMT_SMR.1	Security roles	FIA_UID.1	17 (H)
24.	FMT_RVM.1-1	Non-bypassability of the TSP	None	None
25.	FMT_SEP.1-1	TSF domain separation	None	None

Table 8-11 Dependencies for IT Environment

No.	Component	Component Name	Dependencies	Reference
1.	FPT_ITT.1	Basic internal TSF data transfer protection	None	None
2.	FPT_RVM.1-2	Non-bypassability of the TSP	None	None
3.	FPT_SEP.1-2	TSF domain separation	None	None
4.	FPT_STM.1	Reliable time stamps	None	None
5.	FTP_TRP.1	Trusted path	None	None

8.2.4 Strength of Function

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

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks against the TOE.

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

No.	Component	Component Name	TSS Ref. No	IT Security Function
1	FAU_ARP.1	Security alarms	M-CD-1	Monitor sends an email or SNMP message if a critical event is generated. This implements the FAU_ARP.1 SFR.
2	FAU_GEN.1	Audit data generation	M-CD-2	Monitor is able to generate audit records. (FAU_GEN.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 nameEvent 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. This implements the FAU_GEN.1-NIAP_0347 SFR.

No.	Component	Component Name	TSS Ref. No	IT Security Function
3	FAU_SAA.3	Simple attack heuristics	M-CD-3	Monitor maintain an internal representation of signature events as defined in the customer-specified policy that may indicate a violation of the policy. Monitor and Enterprise are 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.
4	FAU_SAR.1	Audit review	S-AD-1 M-AD-1 E-AD-1 S-AD-4	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. (FAU_SAR.1) - Operator, Analyst, Developer, and Super User can read Event Data (DME and live data for Studio and Live data for Monitor and Enterprise) - Operator, Analyst, Developer, and Super User can read Alerts (DME data for STUDIO and Live data for Monitor and Enterprise) - SV Manager and Super User can read Application Log data (Monitor and Enterprise) - Account Manager and Super User 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. This implements the FAU_SAR.1 SFR.
5	FAU_SAR.2	Restricted audit review	S-AD-2 M-AD-2 E-AD-2	Studio, Monitor and Enterprise prohibit all users read access to the audit records, except those that have been granted explicit read access. This implements the FAU_SAR.2 SFR.
6	FAU_SAR.3	Selectable audit review	S-AD-3 M-AD-3 E-AD-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	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 This implements the FAU_SEL.1- SFR.

No.	Component	Component Name	TSS Ref. No	IT Security Function
8	FAU_STG.2 -NIAP-0429	Guarantees of audit data availability	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. This implements the FAU_STG.2 SFR.
9	FAU_STG.4	Prevention of audit data loss	M-CD-6	Monitor overwrites the oldest stored audit records if the audit trail is full. This implements the FAU_STG.4 SFR.
10	FDP_ACC.2	Complete access control	M-MUA-3 E-MUA-3	Monitor and Enterprise enforce the SecurVantage™ User Access Policy (See Table 5-2 SecurVantageTM User Access Policy.) This implements the FDP_ACC.2 SFR.
11	FDP_ACF.1	Security attribute based access control	M-MUA-3 E-MUA-3	Monitor and Enterprise enforce the SecurVantage™ User Access Policy (See Table 5-2 SecurVantageTM User Access Policy.) This implements the FDP_ACF.1 SFR.
12	FIA_ATD.1	User attribute definition	M-MUA-1 E-MUA-1	Monitor and 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. This implements the FIA_ATD.1 SFR.
13	FIA_SOS.1	Verification of secrets	M-MUA-2 E-MUA-2	Monitor and Enterprise require 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. This implements the FIA_SOS.1 SFR.
14	FIA_UAU.2	User authentication before any action	M-UL-2 E-UL-2	Monitor and Enterprise require each user to successfully authenticate before being allowed any other actions. This implements the FIA_UAU.2 SFR.
15	FIA_UAU.5	Multiple authentication mechanisms	M-UL-3 E-UL-3	Monitor and Enterprise provide for either password- or certificate-based authentication of users. 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. This implements the FIA_UAU.5 SFR.
16	FIA_UAU.7. 1-1	Protected authentication feedback	M-UL-4 E-UL-4	Monitor and Enterprise provide only confirmation of user name and asterisks for password when password authentication is used. This implements the FIA_UAU.7.1-1 SFR.
17	FIA_UAU.7. 1-2	Protected authentication feedback	S-UL-1	Studio provides the certificate dialog box when certificate-based authentication is used. This implements the FIA_UAU.7.1-2 SFR.
18	FIA_UID.2	User identification before any action	M-UL-1 E-UL-1	Monitor and Enterprise require each user to identify himself/herself before being allowed to perform any other actions. This implements the FIA_UID.2 SFR.

No.	Component	Component Name	TSS Ref. No	IT Security Function
19	FMT_MSA.1	Management of security attributes	M-MUA-4 E-MUA-4	Monitor and Enterprise restrict the ability to query, modify, or delete the user-name, roles, and password- or certificate-based authentication security attributes to Account Manager and Super User. This implements the FMT_MSA.1 SFR.
20	FMT_MSA.3	Static attribute initialisation	M-MUA-5 E-MUA-5	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 and Super User to specify alternative initial values. This implements the FMT_MSA.3 SFR.
21	FMT_MTD.1	Management of TSF data	M-MUA-6 E-MUA-6	Monitor and Enterprise restrict the ability to access data as specified in Table 5-2 SecurVantageTM User Access Policy. This implements the FMT_MTD.1 SFR.
22	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 and Super User. This implements the FMT_REV.1 SFR.
23	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. This implements the FMT_SMF.1 SFR.
24	FMT_SMR.1	Security roles	M-MUA-9 E-MUA-9	Monitor and Enterprise maintain the roles Operator, Analyst, Developer, SV Manager, Account Manager, and Super User. This implements the FMT_SMR.1 SFR.
25	FPT_RVM.1-1	Non-bypassability of the TSP	M-MUA-10 E-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. This implements the FPT_RVM.1-1 SFR.
26	FPT_SEP.1-1	TSF domain separation	M-MUA-11 E-MUA-11	Monitor and Enterprise maintain a security domain for their own execution and enforce separation between security domains of users. This implements the FPT_SEP.1-1 SFR.

8.3.2 Assurance Measures

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

Table 8-13 Assurance Measures Rationale

Component	Evidence Requirements	How Satisfied
ACM_CAP.2	CM Documentation	The following documents are provided to meet the ACM_CAP.2 requirements: − Securify SecurVantage 3.1 Common Criteria Addendum − Securify SecurVantage 3.1 Manufacturing Procedures − Securify SecurVantage 3.1 Configuration Parameters
ADO_DEL.1	Delivery Procedures	The following document is provided to meet the ADO_DEL.1

Component	Evidence Requirements	How Satisfied
		requirements: − Manufacturing Procedures − Securify SecurVantage 3.1 EM Coversheet − Securify SecurVantage 3.1 Monitor Coversheet − Securify SecurVantage 3.1 Monitor LE Coversheet
ADO_IGS.1	Installation, generation, and start-up procedures	The following document is provided to meet the ADO_IGS.1 requirements: − SecurVantage™ Version 3.1 Installation Guide − SecurVantage 3.1 Deployment Guide − SecurVantage 3.1 Operations Guide − SecurVantage 3.1 Release Notes
ADV_FSP.1	Functional Specification	The following documents are provided to meet the ADV_FSP.1 requirements: − SecurVantage™ Version 3.1 Installation Guide − SecurVantage™ Version 3.1 Operations Guide − Securify SecurVantage 3.1 Common Criteria Addendum − Securify SecurVantage 3.1 External Interfaces − Securify SecurVantage 3.1 Configuration Parameters − − Securify SecurVantage 3.1 Database Functional Specification
ADV_HLD.1	High-Level Design	The following documents are provided to meet the ADV_HLD.1 requirements: − Securify SecurVantage 3.1 HLD − − Securify SecurVantage 3.1 Common Criteria Addendum
ADV_RCR.1	Representation Correspondence	The following document is provided to meet the ADV_RCR.1 requirements: − Securify SecurVantage 3.1 RCR
AGD_ADM.1	Administrator Guidance	The following document is provided to meet the AGD_ADM.1 requirements: − SecurVantage™ Version 3.1 Operations Guide − Securify SecurVantage 3.1 Common Criteria Addendum − Securify SecurVantage 3.1 Administrator Addendum
AGD_USR.1	User Guidance	The following document is provided to meet the AGD_USR.1 requirements: − SecurVantage™ Version 3.1 Operations Guide − Securify SecurVantage 3.1 Common Criteria Addendum − Securify SecurVantage 3.1 Administrator Addendum
ATE_COV.1	Test Coverage Analysis	The following document is provided to meet the ATE_COV.1 requirements: − SVS Matrix
ATE_FUN.1	Test Documentation	The following document is provided to meet the ATE_FUN.1 requirements:

Component	Evidence Requirements	How Satisfied
		− SV Functional Testing
ATE_IND.2	TOE for Testing	The following is provided to meet the ATE_IND.2 requirements: − TOE for Testing − Sentinel tool
AVA_SOF.1	SOF Analysis	The following document is provided to meet the AVA_SOF.1 requirements: − Common Criteria Addendum to Operations Guide − Securify SecurVantage 3.1 Vulnerability Analysis
AVA_VLA.1	Vulnerability Analysis	The following document is provided to meet the AVA_VLA.1 requirements: − Securify SecurVantage 3.1 Vulnerability Analysis

8.3.3 Strength of Function

The M-MUA-2 and E-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

10 References

• *Common Criteria for Information Technology Security Evaluation*, CCIB-98-026, Version 2.0, May 1998.
• Securify, *Securify SecurVantage™ Version 3.1 Deployment Guide, November 2002*
• Securify, *Securify SecurVantage™ Version 3.1 Installation Guide, November 2003*
• Securify, *Securify SecurVantage™ Version 3.1 Operations Guide, November 2002*
• Securify SecurVantage 3.1 Configuration Parameters.doc, December 2003
• Securify SecurVantage 3.1 Manufacturing Procedures.doc, December 2003
• Securify SecurVantage 3.1 Common Criteria Addendum.doc, January 2004
• Securify SecurVantage 3.1 Common Criteria Addendum.doc, January 2004
• Securify SecurVantage 3.1 HLD.doc, January 2004
• Securify SecurVantage 3.1 External Interfaces.xls, January 2004
• Securify SecurVantage 3.1 Test Matrix.xls, December 2003
• Securify SecurVantage 3.1 Vulnerability Analysis.doc, January 2004