Violin Memory 6000 Series Memory Arrays with Memory Gateways Security Target

Version 1.7

March 4, 2014

Violin Memory Inc.
685 Clyde Ave
Mountain View, CA 94043

DOCUMENT INTRODUCTION

Prepared By:

Common Criteria Consulting LLC
15804 Laughlin Lane
Silver Spring, MD 20906
http://www.consulting-cc.com

Prepared For:

Violin Memory Inc.
685 Clyde Ave
Mountain View, CA 94043
http://www.violin-memory.com/

REVISION HISTORY

Rev	Description
1.0	March 5, 2013 - Initial release
1.1	March 11, 2013 - Addressed lab comments
1.2	April 9, 2013 – Addressed lab Ors/CRs
1.3	July 4, 2013 – Updates for ADV consistency
1.4	July 22, 2013 – Updated the models included in the evaluation
1.5	October 16, 2013 – Inserted build information for the evaluated version
1.6	February 22, 2014 – Added the Unpriv role
1.7	March 4, 2014 – Corrected the build numbers in the TOE reference

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS LIST

CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAL	Evaluation Assurance Level
GPFS	General Parallel File System
HCA	Host Channel Adapter
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
IOPS	Input/output Operations Per Second
IP	Internet Protocol
I&A	Identification & Authentication
LUN	Logical Unit Number
MLC	Multi-Level Cell
NTP	Network Time Protocol
OS	Operating System
PCI	Peripheral Component Interconnect
PP	Protection Profile
RAID	Redundant Array of Independent Disks
RHEL	Red Hat Enterprise Linux
SAN	Storage Area Network
SCSI	Small Computer System Interface
SFP	Security Function Policy
SFR	Security Functional Requirement
SLC	Single Level Cell
SLES	SUSE Linux Enterprise Server
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VIMM	Violin Intelligent Memory Modules
vMem	Violin Memory
vMOS	Virtual Memory Operating System
VXM	Violin Switched Memory

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Violin Memory 6000 Series Memory Arrays with Memory Gateways. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4*. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Violin Memory 6000 Series Memory Arrays with Memory Gateways Security Target, Version 1.7, dated March 4, 2014

1.2 TOE Reference

Violin Memory 6000 Series Memory Arrays with Memory Gateways Version 5.5.2 (Build Number 1 for the Array Controllers and Build Number 7 for the Memory Gateways) .

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) augmented by ALC_FLR.2 from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 4.

1.4 Keywords

Memory array, Flash memory array, high performance storage, application acceleration, access control, Storage Area Network, SAN.

1.5 TOE Overview

1.5.1 Usage and Major Security Features

The Violin Memory (vMem) Memory Arrays are stand-alone purpose-built memory arrays designed to maximize the performance and value of flash memory and deliver a high-bandwidth, high IOPS, low latency and cost-effective storage system.

The primary operating modes for the vMem Memory Arrays are:

- SAN-attached Storage: connects to a storage area network (SAN) using Fibre Channel, InfiniBand or iSCSI/Ethernet. This configuration allows multiple servers, including clustered applications, to share the same storage.
- Direct-attached Storage: connects via PCI Express (PCIe) to one or two servers running Linux. This configuration provides low latency and high bandwidth. (This mode is not included in the evaluation.)

The vMem Memory Arrays enable thousands of flash devices to operate efficiently as a flash memory array and are intended for any application that requires active processing or rapid access to large amounts of data, including applications for transaction processing (Oracle, DB2, SQL Server, Sybase), analytics and data warehousing, messaging systems (e-mail), active file storage and metadata (GPFS, Lustre).

The flash memory may be configured as multiple Logical Unit Numbers (LUNs) and accessed from the servers using standard block access transport protocols over the SAN. Access to individual LUNs may be restricted by authorized administrators to a LUN-specific list of servers.

Memory Arrays provide multiple points of fault tolerance/hardware redundancy with hot-swap capabilities, including RAID storage configurations. These features are not evaluated.

Management of the TOE is performed via a serial connection using a CLI or via network connections using a CLI or web interface. The serial connection is used for initial installation only.

Management interfaces (both CLI and web interface) are provided by the appliance software. These interfaces are used for operational control and monitoring of the TOE. They support multiple roles (Admin and Monitor), enabling different users to have varying access to data and functions. Identification and Authentication may be performed locally or via integration with third party servers; only local I&A is included in the evaluation.

Auditing is performed for security-relevant events. The audit records are saved on the appliance and may be reviewed by users with the Admin role. Audit records may also be transmitted to one or more remote servers using the Syslog protocol.

Multiple appliance models are included in the evaluation. These models all provide the same security functionality; they differ in storage throughput, flash type and flash capacity only. The applicable models are listed in the following table.

Table 1 - 6000 Series Appliance Specifications

Model Item	6606	6611	6616	6212	6222	6232
Flash Type	Single Level Cell (SLC)			Multi-Level Cell (MLC)		
Raw Capacity (GiB/GB)	6TB/ 6.6TB	11TB/ 12.1TB	16TB/ 17.6TB	12TB/ 13.2TB	22TB/ 24.2TB	32TB/ 35.2TB
Max. 4KB IOPS	450K	800K	1000K	200K	350K	500K
Max. Bandwidth	3 GB/s	3.5 GB/s	4 GB/s	1.5 GB/s	2.5 GB/s	4 GB/s
Nominal Latency	< 250 µs	< 250 µs	< 250 µs	< 500 µs	< 500 µs	< 500 µs
Max VIMM Count	20 + 4	40 + 4	60 + 4	20 + 4	40 + 4	60 + 4
Connectivity Options	8x 4/8Gb/s Fibre Channel 8x 10GbE iSCSI 8x 40Gb/s QDR Infiniband					

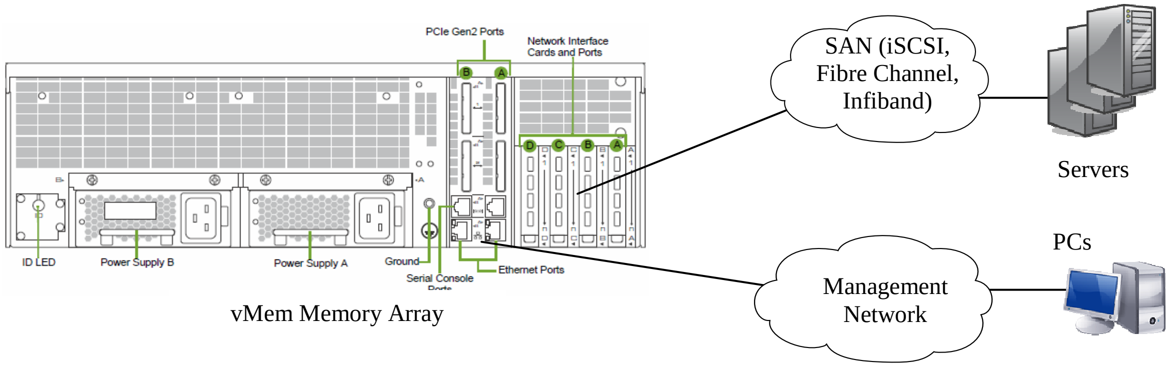
1.5.2 TOE Type

Other Devices and Systems

1.5.3 Required Non-TOE Hardware/Software/Firmware

A typical deployment of the vMem Memory Array is shown in the following diagram.

Figure 1 - Typical TOE Deployment



Multiple physical interfaces are used for data storage and retrieval from servers over a SAN. The server operating systems supported are RHEL, SLES, Windows, VMware, Hyper-V, Citrix, AIX, Solaris SPARC, Solaris x86, HP-UX, and OpenVMS. It is the responsibility of the operational environment to ensure that only authorized systems have access to the SAN.

Dedicated physical Ethernet interfaces are used for communication between remote management sessions and the appliance. It is the responsibility of the operational environment to protect the traffic on the management network from disclosure to or modification by unauthorized users. SSH is supported for CLI access. The browsers supported for HTTP access to the web interfaces are listed in the following table.

Table 2 - Supported Browsers

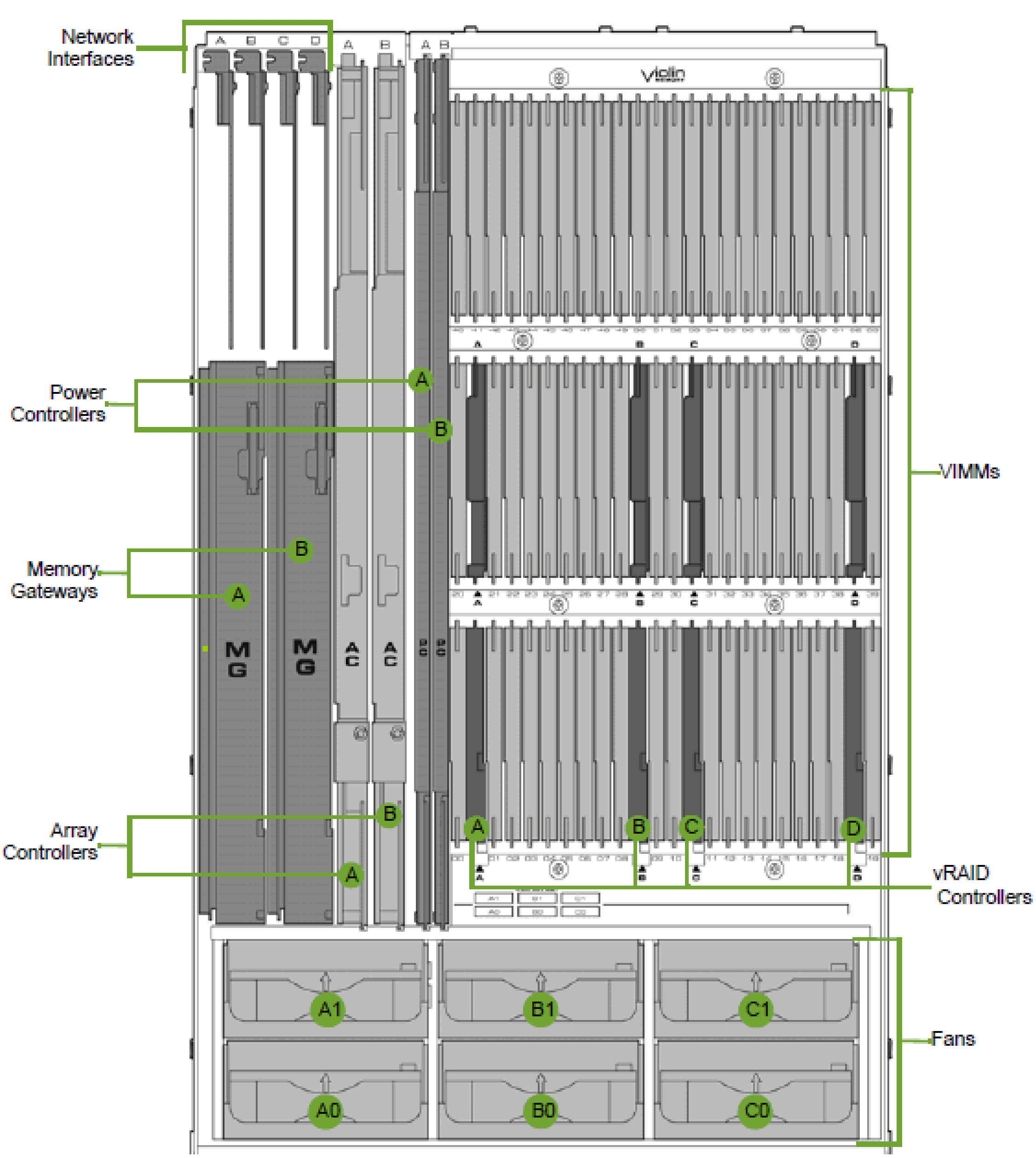
Operating System	Supported Browsers
Linux	• Mozilla Firefox 4 and above • Google Chrome 11 and above
Mac	• Apple Safari 4 and above • Mozilla Firefox 4 and above • Google Chrome 11 and above
Windows	• Windows Internet Explorer 9 and above • Apple Safari 4 and above • Mozilla Firefox 4 and above • Google Chrome 11 and above

JavaScript must be enabled, and Adobe Flash is required to view charts.

1.6 TOE Description

A Memory Array consists of multiple components, as shown in the following figure.

Figure 2 - vMem Memory Array Top View



The hardware components are:

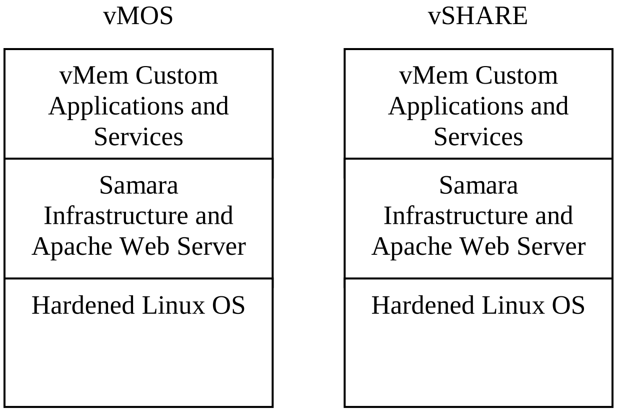
- Violin Intelligent Memory Modules (VIMMs) - VIMMs provide the flash capacity for the Memory Array. The number of VIMMs supported varies by model. Each VIMM includes a flash controller that manages the flash memory, including flash media errors and failures, flash wear, and the process of “grooming” for removing unused or obsolete memory blocks from the flash memory.
- Array Controllers - The Array Controllers provide PCIe interfaces, switching, and management services. vMOS software executes on the Array Controllers. In the

evaluated configuration, the Array Controllers are internally connected to the Memory Gateways via PCIe.

- Memory Gateways - Memory Gateways provide the control logic for the SAN protocols. vSHARE software executes on the Memory Gateways. In the evaluated configuration, Memory Gateways must be installed and vSHARE translates SAN requests into PCIe messages forwarded to the Array Controllers (and vice versa).
- Network Interfaces - The network interfaces provide the physical connectivity to the SAN via Fibre Channel, iSCSI or InfiniBand Host Channel Adapter (HCA) cards. Two Network Interface cards are attached to each of the Memory Gateways.
- vRAID Controllers – The vRAID controllers optimize key flash storage attributes including latency under load, bandwidth, storage efficiency and reliability. vRAID provides full RAID data protection across the array while simultaneously guaranteeing that any read will not be blocked by an erase providing for spike-free latency under load and sustained performance.
- Violin Switched Memory (VXM) – VXM is a switched memory network that combines the best attributes of a high-performance interconnect including sub-µsec latency, redundancy, scalability, and high availability. VXM connects the VIMMs to the vRAID Controllers and provides a high bandwidth, highly reliable data path.

Software is pre-installed on appliances by vMem. vMOS software executes on the Array Controllers, while vSHARE software executes on the Memory Gateways. vMOS mediates flash storage requests between Memory Gateways and VIMMs. vSHARE mediates access requests from servers, enabling servers to use standard block access transport protocols to access logical units of data (LUNs) stored within Memory Arrays. These components are described in more detail in the following diagram.

Figure 3 - Software Components


vMOS
vSHARE
vMem Custom Applications and Services
Samara Infrastructure and Apache Web Server
Hardened Linux OS
vMem Custom Applications and Services
Samara Infrastructure and Apache Web Server
Hardened Linux OS

The Samara infrastructure (third party software from Tall Maple Systems) provides the management infrastructure to process the CLI commands and maintain the configuration database for both CLI and web access. The vMem custom applications and services provide the functions to interpret the web messages, apply configuration changes made by administrators, monitor the operation of the hardware components, and satisfy the block data requests sent by servers to the TOE. vSHARE applies access control functionality to limit server access (referred to as initiators) to their authorized Logical Unit Numbers (LUNs).

All management access is via the CLI or web interface and is mediated by the Samara and vMem custom software. All data access is via the standard block access transport protocols and the requests are mediated by the vSHARE software. Operationally no shell access is provided to any Linux shell (there is no access to the underlying OS of the TOE).

All user data access is from the SAN, and is therefore processed by the Memory Gateways and vSHARE. In this configuration, the Array Processors and vMOS play a supporting role only. All of the security-relevant processing is performed on the Memory Gateways by vSHARE only.

1.6.1 Physical Boundary

The physical boundary of the TOE is the complete vMem Memory Array appliance.

The physical boundary includes the following guidance documentation:

1. *Violin Memory 6000 Series Memory Array Installation Guide For Release A5.5.2 and G5.5.2*
2. *Violin Memory 6000 Series Memory Array User's Guide For Release A5.5.2 and G5.5.2*
3. *Violin Memory Arrays Version 5.5.2 Common Criteria Supplement*

1.6.2 Logical Boundary

1.6.2.1 Audit

Audit records are generated for specific actions performed by administrators. All audit event record types have a pre-defined level; the minimum level of audit event record types to be saved may be configured. The audit records are stored on the appliance as multiple files that are periodically rolled. Audit records may be viewed by users with the Admin role. In the unlikely event audit storage space is exhausted, the oldest audit record file is discarded (the newest audit records are saved). Audit records are automatically deleted according to the retention policy configured by authorized administrators.

Audit records may also be sent to one or more configured remote destinations via Syslog.

1.6.2.2 Management

The TOE provides functionality for administrators to remotely configure and monitor the operation of the TOE via a CLI or web browser.

The security management functionality provided by the TOE includes:

- User
- Appliance
- LUN
- Audit
- Management

All TOE data is stored on the appliance.

1.6.2.3 Access Control

The TOE mediates all block data requests from servers (initiators) to prevent unauthorized access to LUNs. By default access to LUNs is unrestricted. Authorized administrators may configure an access control list for individual LUNs to restrict access to the configured initiators.

1.6.2.4 I&A

The TOE identifies and authenticates administrators before they are granted access to any TSF functions or data. When valid credentials are presented, security attributes for the user are bound to the session. .

1.6.3 TOE Data

The following table describes the TOE data.

Table 3 - TOE Data Descriptions

TOE Data	Description
Appliance Configuration	A set of configuration parameters for the appliance, including: • Memory Gateway IP Configuration • Memory Gateway Management IP Configuration • Clock Configuration (Internal or NTP Server) • Enabled SAN Interfaces • Initiators • Initiator Groups • Targets • Target Protocols
Audit Configuration	A set of configuration parameters for the audit function, including: • Local logging level • Remote Syslog destinations • Remote logging level
LUN Configuration	A set of configuration parameters for LUNs, including: • Size • Block Size • Name • Online • Read-only • Exported Target Ports • Authorized Initiators/Initiator Groups
Management Configuration	A set of configuration parameters for the CLI and web interface, including: • CLI Auto-logout Time • Web Auto-logout Time
User Accounts	A set of configuration parameters for user accounts, including: • Account name • Password • Role • Command Mode (applicable to CLI users only)

1.7 Evaluated Configuration

The evaluated configuration of the TOE includes one instance of a vMem Memory Array with Memory Gateways.

The following configuration restrictions apply to the evaluated configuration:

1. Only local users are defined. Remote user authentication (via third party servers) is not used.
2. Administrators configure passwords for user accounts in accordance with their policies.
3. No direct access to a Linux shell from remote management sessions is enabled.
4. SNMP support is not enabled.
5. Logging is enabled at all times. The local logging level is configured as INFO.
6. Telnet service is disabled; SSH is enabled because it is used for internal communication between Array Controllers and Memory Gateways.
7. Web Management on the Memory Gateways is enabled and the Web UI Inactivity Timeout parameter value is never set to 0 (disabled).
8. Web Management on the Array Controllers is disabled (no security-relevant actions may be performed via this GUI).

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Common Criteria (CC) for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012

Common Criteria conformance: Part 2 conformant and Part 3 conformant

2.2 Security Requirement Package Conformance

EAL2 augmented by ALC_FLR.2

The TOE does not claim conformance to any security functional requirement packages.

2.3 Protection Profile Conformance

The TOE does not claim conformance to any Protection Profiles.

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the Operational Environment.

Table 4 - Assumptions

A.Type	Description
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.MGMTNETWORK	The TOE components will be interconnected by a segregated management network that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users.
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.PROTCT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.

3.3 Threats

The threats identified in the following table are addressed by the TOE and the Operational Environment.

Table 5 - Threats

T.Type	Description
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential unauthorized data accesses to go undetected.
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.UNAUTH_ACCESS	A server may attempt to access user data (LUN) that it is not authorized to access.

3.4 Organisational Security Policies

The Organisational Security Policies identified in the following table are addressed by the TOE and the Operational Environment.

Table 6 - Organisational Security Policies

P.Type	Description
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.INTGTY	Audit data produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 7 - Security Objectives for the TOE

O.Type	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.AUDITREV	The TOE must provide a mechanism for authorized administrators to review audit records.
O.AUDITS	The TOE must record audit records for security relevant events.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.INTEGR	The TOE must prevent the modification of audit data records.
O.OFLOWS	The TOE must appropriately handle potential audit data storage overflows.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.TIME	The TOE will maintain reliable timestamps.

4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives.

Table 8 - Security Objectives of the Operational Environment

OE.Type	Description
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
OE.MGMTNET WORK	The operational environment will provide a segregated management network that protects the management traffic from disclosure to or modification by untrusted systems or users.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.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. Extended Components Definition

5.1 Extended Security Functional Components

None

5.2 Extended Security Assurance Components

None

6. Security Requirements

This section contains the security requirements that are provided by the TOE.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

6.1 TOE Security Functional Requirements

The functional requirements are described in detail in the following subsections. Additionally, these requirements are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation* and/or the previous chapter of this document with the exception of completed operations.

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

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

c) *The events in the following table*.

Table 9 - Auditable Events

SFR	Event	Additional Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_SAR.1	Accessing the audit records	Audit file accessed
FDP_ACC.1	Denied access attempts	Initiator, LUN
FDP_ACF.1	Denied access attempts	Initiator, LUN
FIA_UAU.2	Successful login	Remote IP address
	Failed login attempt	Remote IP address, Supplied username
FIA_UID.2	Successful login	Remote IP address
	Failed login attempt	Remote IP address, Supplied username
FMT_MSA.1	Modifications to LUN security attributes	Parameters, new parameter values
FMT_MSA.3	LUN creation	Parameters, parameter values
FMT_MTD.1	Modifications to the values of TSF data	Parameters, new parameter values
FTA_SSL.3	Logout due to inactivity	

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

a) Date and time of the event, type of event, subject identity (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, *the information in the Additional Details column in the table above*.

6.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *all authorised users with the Admin role* with the capability to read *all audit information* 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.

6.1.1.4 FAU_SAR.2 Restricted Audit Review

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

6.1.1.5 FAU_STG.2 Guarantees of Audit Data Availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that *the most recent but one file of* stored audit records will be maintained when the following conditions occur: audit storage exhaustion.

Application Note: Authorized deletion occurs indirectly when an admin role configures the retention and wrapping policy for audit record files.

Application Note: No modification of the stored audit records is authorized.

Application Note: In the unlikely event audit storage space is exhausted, new audit records are saved (the oldest rolled audit record file is deleted).

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the *LUN Access SFP* on

1. *Subjects: Initiators*
2. *Information: LUNs*
3. *Operations: Read, Write.*

6.1.2.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the *LUN Access SFP* to objects based on the following:

1. *Initiators: Presumed Initiator ID, Initiator Group Membership, Target Port from the access request*
2. *LUNs: Online status, Read-only status, Exported Target Ports, Authorized Initiators/Initiator Groups.*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

1. *Writes are allowed if all of the following conditions are true:*
    a. *The LUN is Online*
    b. *The LUN is not Read-only*
    c. *The Target Port from the access request is one of the Exported Target Ports*
    d. *The Presumed Initiator ID is one of the Authorized Initiators; or the Presumed Initiator ID is a member of any of the Authorized Initiator Groups; or no Authorized Initiators/Initiator Groups are configured for the LUN.*
2. *Reads are allowed if all of the following conditions are true:*
    a. *The LUN is Online*
    b. *The Target Port from the access request is one of the Exported Target Ports*
    c. *The Presumed Initiator ID is one of the Authorized Initiators; or the Presumed Initiator ID is a member of any of the Authorized Initiator Groups; or no Authorized Initiators/Initiator Groups are configured for the LUN.*

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *no additional rules*.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) *Account Name;*

b) *Password;*

c) *Role;*

d) *Command Mode.*

6.1.3.2 FIA_UAU.2 User Authentication Before Any Action

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.

6.1.3.3 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *obfuscated feedback for each character entered* to the user while the authentication is in progress.

6.1.3.4 FIA_UID.2 User Identification Before Any Action

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

6.1.3.5 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: *Account Name, Role, and Command Mode*.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *the attributes are associated upon successful completion of I&A.*

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

1. *The Account Name and Role attributes do not change during the session (through user logout).*
2. *The Command Mode attribute is initially set to Standard upon successful I&A and the following changes occur during a session:*
    a. *From Standard to Enable when the "enable" command is issued. All defined users may issue this command.*

    b. *From Enable to Config when the "configure terminal" command is issued. Only users with the Admin role may issue this command.*

    c. *From Config to Enable when the "exit" command is issued.*

    d. *From Enable to Standard when the "disable" command is issued.*

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the *LUN Access SFP* to restrict the ability to *modify* the security attributes *LUNs: Online status, Read-only status, Exported Target Ports, Authorized Initiators/Initiator Groups* to *the Admin role*.

6.1.4.2 FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the *LUN Access SFP* to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the *Admin role* to specify alternative initial values to override the default values when an object or information is created.

6.1.4.3 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, *create* the *data identified in the following table* to *the authorised identified roles identified in the following table*.

Table 10 - TSF Data Access Details

TSF Data	Web Interface		CLI		
	Admin	**Monitor**	**Admin**	**Monitor**	**Unpriv**
Appliance Configuration	Query, Modify	Query	Query, Modify	Query	None
Audit Configuration	Query, Modify	Query	Query, Modify	Query	None
LUN Configuration	Query, Modify, Delete, Create	Query	Query, Modify, Delete, Create	Query	None
Management Configuration	Query, Modify	Query	Query, Modify	Query	None
User Accounts	Query, Modify, Delete, Create	Query	Query, Modify, Delete, Create	Query	None

6.1.4.4 FMT_SMF.1 Specification of Management Functions

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

a) Appliance configuration;

b) Audit configuration;

c) LUN configuration;

d) Management configuration;

e) User Accounts configuration.

6.1.4.5 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles *Unpriv*, *Admin and Monitor*.

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

Application Note: The Unpriv role only applies to the CLI, and is the role assigned to a session upon initial login via the CLI. This role has no access to TSF data or functions. As soon as the user issues the CLI "enable" command, the Monitor role is assumed for the session.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time-stamps.

6.1.6 TOE Access (FTA)

6.1.6.1 FTA_SSL.3 TSF-Initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: *the configured auto-logout time for CLI or web interface sessions*].

6.2 TOE Security Assurance Requirements

The assurance requirements are identified in the following table. These requirements reference Part 3 of the *Common Criteria for Information Technology Security Evaluation*.

The TOE meets the assurance requirements for EAL2 augmented by ALC_FLR.2. These requirements are summarised in the following table.

Table 11 - EAL2+ Assurance Requirements

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 12 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied
FAU_GEN.2	No other components.	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied by FIA_UID.2
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components.	FAU_SAR.1	Satisfied
FAU_STG.2	FAU_STG.1	FAU_GEN.1	Satisfied
FDP_ACC.1	No other components.	FDP_ACF.1	Satisfied
FDP_ACF.1	No other components.	FDP_ACC.1, FMT_MSA.3	Satisfied Satisfied
FIA_ATD.1	No other components.	None	n/a
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UAU.7	No other components.	FIA_UAU.1	Satisfied by FIA_UAU,2
FIA_UID.2	FIA_UID.1	None	n/a
FIA_USB.1	No other components.	FIA_ATD.1	
FMT_MSA.1	No other components.	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied Satisfied
FMT_MSA.3	No other components.	FMT_MSA.1, FMT_SMR.1	Satisfied Satisfied
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by FIA_UID.2
FPT_STM.1	No other components.	None	n/a
FTA_SSL.3	No other components.	None	n/a

7. TOE Summary Specification

7.1 FAU_GEN.1, FAU_GEN.2

The TOE generates audit records for the events specified in the table included with the FAU_GEN.1, with the information specified in that table as well as in FAU_GEN.2. Audit records are generated as text records and are inserted into a rolling set of audit files. Files are rolled at a frequency or size configured by an administrator with the Admin role.

7.2 FAU_SAR.1, FAU_SAR.1

Audit records may be reviewed by any authorized user with the Admin role. The user may specify the audit file to be displayed. The display is a textual display. Users with the Monitor role may not view any audit records.

7.3 FAU_STG.2

The user access functionality of the TOE does not provide any mechanism to modify audit records. If no space is available when the TOE attempts to insert a new audit record, the oldest rolling audit file is automatically deleted, and then the new audit record is inserted. Audit files may also be automatically deleted when the retention period is exceeded (e.g. keep the 10 most recent audit files). Authorized administrators may also use the CLI “logging files delete oldest” command to delete one or more rolling audit files (starting with the oldest). The current audit file can not be deleted.

7.4 FDP_ACC.1, FDP_ACF.1

When a request for LUN access is received from any initiator, access controls are applied to determine if the access is granted. If the LUN is not online, access is denied. For write operations, access is denied if the LUN is read-only.

Each LUN is associated with one or more Target Ports. If the access is not performed on an Exported Target Port for the LUN, access is denied. Each request includes an initiator identifier; the form is dependent on the SAN type (e.g. Fibre Channel). The supplied identifier must either be included in the Authorized Initiators list for the LUN; be a member of one or more of the Authorized Initiator Groups list for the LUN; or no Authorized Initiators or Initiator Groups are configured for the LUN (implying all initiators may access it).

7.5 FIA_ATD.1

The TOE maintains the following information for each user account:

- Account Name;
- Password;
- Role;
- Command Mode.

User account information is maintained in the TOE.

7.6 FIA_UAU.2, FIA_UID.2, FIA_USB.1

The TOE requires all users of the CLI and web interface to successfully identify and authenticate themselves via a username and password before access is granted to any TSF data or functions. Validation of the supplied credentials is performed by the TOE.

Upon successful login, the security attributes for the User Account are bound to the session. The Account Name and Role attributes remain bound until the user logs out. For CLI users, the Command Mode attribute may be changed by issuing the "enable" and "configure terminal" commands. All users may issue the "enable" command, while only users with the Admin role may issue the "configure terminal" command.

7.7 FIA_UAU.7

When a password is being entered, either no input is echoed or asterisks are echoed.

7.8 FMT_MSA.1, FMT_MSA.3

The security attributes used in FDP_ACC.1/FDP_ACF.1 may only be configured (modified) by the Admin role. The default values are restrictive since no exports are associated with a newly created LUN.

7.9 FMT_MTD.1

The TOE grants access to TSF data for authorized administrators according to the roles specified in the table included with FMT_MTD.1(1). The CLI and web interface may only be used by authorized users. Access to TSF data other than that specified in the table is prevented.

7.10 FMT_SMF.1

The TOE provides functionality for authorized users to configure the following items via the CLI and/or web interface:

- appliance;
- audit operation;
- LUNs;
- management interfaces;
- user accounts.

7.11 FMT_SMR.1

All interactive users of the TOE are required to successfully complete I&A, at which time the role configured for the user account is associated with the user session. The role assigned to the user account determines the access permissions for the user. The roles that may be assigned to a user are Unpriv (CLI only), Admin and Monitor.

7.12 FPT_STM.1

The TOE maintains a reliable time stamp, either on its own or with input from an NTP server. The time stamps are inserted into audit records.

7.13 FTA_SSL.1

All CLI and web interface sessions are monitored for inactivity. If the configured inactivity time is exceeded, the session is automatically terminated. The inactivity times for CLI and web interface sessions are separate configuration parameters.

8. Protection Profile Claims

Conformance to a Protection Profile is not claimed.

9. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

9.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each organizational security policy, threat and assumption, the security objective(s) that address it.

Table 13 - Security Objectives Mapping

	O.ACCESS	O.AUDITREV	O.AUDITS	O.EADMIN	O.IDAUTH	O.INTEGR	O.OFLOWS	O.PROTCT	O.TIME	OE.CREDEN	OE.INSTAL	OE.MGMTNETWORK	OE.PERSON	OE.PHYCAL
A.MANAGE													X	
A.MGMTNETWORK												X		
A.NOEVIL										X	X			X
A.PROTCT														X
P.ACCACT		X	X		X				X					
P.INTGTY						X								
P.MANAGE	X			X	X			X		X	X		X	
P.PROTCT							X							X
T.IMPCON	X			X	X						X			
T.PRIVIL	X				X			X						
T.UNAUTH_ACCESS	X	X	X											

The following table describes the rationale for the security objectives mappings.

Table 14 - Rationale For Security Objectives Mappings

Item	Security Objectives Rationale
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

Item	Security Objectives Rationale
A.MGMTNETWORK	The TOE will be interconnected to remote administrators by a segregated management network that protects the traffic from disclosure to or modification by untrusted systems or users. The OE.MGMTNETWORK objective ensures that the management traffic will be protected by a segregated management network.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification. The OE.PHYCAL provides for the physical protection of the TOE software and the hardware on which it is installed.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.TIME objective supports this policy by providing a time stamp for insertion into the audit records. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The O.AUDITREV objective supports this policy by providing a mechanism for administrators to review the audit logs.
P.INTGTY	Audit data produced by the TOE shall be protected from modification. The O.INTEGR objective ensures the protection of audit data from modification.
P.MANAGE	The TOE shall only be managed by authorized users. The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTAL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions (overflows) of audit data storage. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.

Item	Security Objectives Rationale
T.UNAUTH_ACCESS	A server may attempt to access user data (LUN) that it is not authorized to access. The O.ACCESS objective only permits authorized access TOE data. The O.AUDITS objective supports O.ACCESS by requiring the TOE to record audit data for unauthorized access attempts, and O.AUDITREV requires the TOE to provide a mechanism for administrators to review the audit logs so that such attempts will be detected.

9.2 Security Requirements Rationale

9.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 15 - SFRs to Security Objectives Mapping

	O.ACCESS	O.AUDITREV	O.AUDITS	O.EADMIN	O.IDAUTH	O.INTEGR	O.OFLOWS	O.PROTCT	O.TIME
FAU_GEN.1			X						
FAU_GEN.2			X						
FAU_SAR.1	X	X						X	
FAU_SAR.2	X							X	
FAU_STG.2			X			X	X	X	
FDP_ACC.1								X	
FDP_ACF.1								X	
FIA_ATD.1					X				
FIA_UAU.2	X				X				
FIA_UAU.7	X				X				
FIA_UID.2	X				X				
FIA_USB.1	X								
FMT_MSA.1								X	
FMT_MSA.3								X	
FMT_MTD.1	X				X			X	
FMT_SMF.1	X			X		X			
FMT_SMR.1					X				
FPT_STM.1			X						X
FTA_SSL.3								X	

The following table provides the detail of TOE security objective(s).

Table 16 - Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. The TOE is required to restrict the review of audit data authorized administrators [FAU_SAR.1, FAU_SAR.2]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. Authorized users are granted access to data based upon their configured security attributes [FMT_MTD.1]. The security attributes are bound to the session upon successful I&A; only the Command Mode attribute may change during a session [FIA_USB.1]. The appropriate TOE management functions are identified [FMT_SMF.1]. Appropriate access is supported by not displaying passwords as they are entered [FIA_UAU.7].
O.AUDITREV	The TOE must provide a mechanism for authorized administrators to review audit records. The TOE provides a mechanism for authorized administrators to review audit records in human readable form [FAU_SAR.1].
O.AUDITS	The TOE must record audit records for security relevant events. Security-relevant events are defined for the TOE [FAU_GEN.1, FAU_GEN.2]. The audit records will contain reliable timestamps [FPT_STM.1]. The TOE must prevent unauthorized modification and deletion of audit data as well as the loss of collected data in the event the audit trail is full [FAU_STG.2].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The management functions provided by the TOE are specified [FMT_SMF.1].
O.IDAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. Authorized users are granted access to data based upon their configured security attributes [FMT_MTD.1]. The TOE must be able to recognize the different administrative roles that exist for the TOE [FMT_SMR.1]. Integrity of the I&A process is supported by not displaying passwords as they are entered [FIA_UAU.7].
O.INTEGR	The TOE must ensure the integrity of audit data records. The TOE is required to protect the audit trail from any modification and unauthorized deletion [FAU_STG.2]. The functions made available to users for management of the TOE are limited [FMT_SMF.1].
O.OFLOWS	The TOE must appropriately handle potential audit data storage overflows. The TOE must prevent unauthorized modifications and deletions and the loss of audit data in the event the audit trail is full [FAU_STG.2].
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data. The TOE is required to enforce the LUN Access SFP on all requests from Initiators [FDP_ACC.1, FDP_ACF.1]. Only authorized administrators may query audit data [FAU_SAR.1, FAU_SAR.2], and authorized administrators of the TOE may query and modify all other TOE data [FMT_MSA.1, FMT_MSA.3, FMT_MTD.1]. The TOE is required to protect the audit trail from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion [FAU_STG.2]. Idle management sessions are automatically logged out to guard against session hijacking [FTA_SSL.3].

Security Objective	SFR and Rationale
O.TIME	The TOE will maintain reliable timestamps. The TOE is required to maintain reliable timestamps [FPT_STM.1].

9.2.2 Security Assurance Requirements Rationale

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 augmented by ALC_FLR.2 from part 3 of the Common Criteria.