EMC® Corporation

EMC® VNX OE for Block v05.33 and File v8.1 with Unisphere™ v1.3 running on VNX Series Hardware Models VNX5200™, VNX5400™, VNX5600™, VNX5800™, VNX7600™, and VNX8000™

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.5

Prepared for:

EMC²
where information lives®

EMC® Corporation
176 South Street
Hopkinton, MA 01748
United States of America

Phone: +1 508 435 1000
http://www.emc.com

Prepared by:

Corsec®

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is EMC® VNX OE for Block v05.33 and File v8.1 with Unisphere™ v1.3 running on VNX Series Hardware Models VNX5200™, VNX5400™, VNX5600™, VNX5800™, VNX7600™, and VNX8000™, and will hereafter be referred to as the TOE. The TOE is a File and Block storage solution administered by Unified Management (Unisphere) and Command Line Interface (CLI) tools known as Navisphere CLI and Control Station CLI. The TOE provides access controls for internal storage provided by the TOE hardware. Internal file storage is accessed via Network Attached Storage (NAS) over a Local Area Network (LAN) and block storage is accessed via traditional Storage Area Network (SAN) based protocols.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 – ST and TOE References

ST Title	EMC® Corporation EMC® VNX OE for Block v05.33 and File v8.1 with Unisphere™ v1.3 running on VNX Series Hardware Models VNX5200™, VNX5400™, VNX5600™, VNX5800™, VNX7600™, and VNX8000™ Security Target
ST Version	Version 0.5
ST Author	Corsec Security, Inc.
ST Publication Date	2014-04-24
TOE Reference	Hardware: VNX Series Hardware Models VNX5200™, VNX5400™, VNX5600™, VNX5800™, VNX7600™, and VNX8000™ Software: VNX OE for Block v05.33.000.5.035 VNX OE for File v8.1.1.33 Unisphere v1.3.1.1.0033 Navisphere CLI v7.33.1.0.33
Keywords	VNX, Storage Area Network, SAN, storage array, data storage, Unisphere, Network Attached Storage, NAS, Navisphere CLI, Data Mover, Control Station, Storage Processor

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

EMC® VNX OE for Block v05.33 and File v8.1 with Unisphere™ v1.3 running on VNX Series Hardware Models VNX5200™, VNX5400™, VNX5600™, VNX5800™, VNX7600™, and VNX8000™ can be divided into three main components. VNX OE is the software portion of the product responsible for access controls and management of storage. Unisphere, Navisphere CLI, and Control Station CLI comprise the management software that allows administrators to maintain and configure the product. VNX is the hardware portion of the product. Together, these components provide Block and File access to internal storage for external entities:

1. Block: controls access to internal storage for devices on a SAN. These access controls allow administrators to determine which devices on a SAN have access to VNX storage, and also which areas of storage (disks or portions of disks) are available to each device. Storage is provided over Fibre Channel[1] (FC) and Internet Small Computer Systems Interface (iSCSI).
2. File: controls access to internal storage for devices on a LAN. While Block mode requires devices to access storage from a SAN using SAN-specific communications, VNX also provides NAS that allows traditional Internet Protocol (IP) - based devices to access internal storage over a LAN. NAS storage is provided over Network File System (NFS[2]), Server Message Block (SMB[3], also referred to as CIFS[4]), File Transfer Protocol (FTP), and Trivial File Transfer Protocol (TFTP).

Unisphere is a unified management suite presented through a Graphical User Interface (GUI) that allows administrators to configure the majority of VNX functionality from a single management console. In addition to Unisphere, VNX provides a CLI called Navisphere CLI and a second CLI available on the Control Station, referred to as Control Station CLI. Navisphere CLI provides a subset of the functionality available via the Unisphere GUI and is used to configure both Block and File functionality. Control Station CLI provides necessary functionality to configure File mode properties. Administrators can create shell scripts and batch files for CLI commands to automate management tasks. The Control Station CLI is accessed using a Secure Shell (SSH) interface that administrators can use for File-specific configuration management activities. The product includes an SSH server to provide this functionality.

VNX OE/Unisphere administrators can provision (make available) internal storage to devices on a LAN and devices on a SAN. Once storage has been provisioned to LAN users, it is no longer available to SAN users, and storage provisioned to SAN users is no longer available to LAN users. Storage can be re-provisioned as needed to suit the needs of users.

In File mode, VNX presents itself as one or more standard network-based file servers to client machines on a LAN. In Block mode, VNX presents itself as a series of block storage devices to client machines on a SAN. Administrators manage VNX and control the policies that govern access to storage with the Unisphere GUI and Navisphere CLI. Administrators may also have to use the Control Station CLI to manage the File portion of VNX.

[1] Fibre Channel is a serial data transfer interface that operates over copper wire and/or optical fibre at connection speeds currently supported up to 4 GB/s or 8 GB/s.
[2] NFS is a platform-independent file sharing system commonly used by UNIX and UNIX variants for file sharing. VNX support NFS versions 2, 3, and 4.
[3] SMB 1.0, 2.0, and 3.0 are supported
[4] CIFS – Common Internet File System

The product can run in Block mode, File mode, or Unified Block and File mode of operation. Block mode allows the product to provide only traditional SAN-based access and access controls to internal storage for devices on the SAN. File mode allows the product to control only LAN access to internal storage. Unified Block and File mode is a combination of the above two modes, allowing the product to provide and control access to internal storage from both typical SAN and LAN devices. Unisphere runs on the VNX hardware in the Unified Block and File mode of operation[5].

VNX/Unisphere allows an organization to manage its storage needs separately from its application and file servers. This allows greater control over storage allocation, fault tolerance, and backups versus storage that is directly attached to individual application or file servers. In a typical deployment scenario for VNX/Unisphere, individual client machines are attached to a SAN through a Fibre Channel or iSCSI switch. Client machines also connect to VNX/Unisphere over an IP-based LAN through standard networking equipment (IP routers and switches as needed). These client machines are then configured to use storage on VNX—in the form of Logical Units or file servers—for their applications.

VNX OE implements a Storage Operating Environment (SOE), which provides Redundant Array of Independent Disks (RAID) and storage provisioning capabilities. The product provides the ability to combine several individual drives into useful logical groups, provides fault tolerance for stored data, and manages access to stored data. The product is designed to allow customers to scale both system performance and storage capacity.

Hardware/software components called Data Movers[6] implement the NAS functionality. Data Movers are the VNX file-side components that perform the actual transfer of data between the internal storage and LAN clients. Each Data Mover provided by VNX can host one or more file servers that present shared services to client machines on a LAN.

Administrators can configure the type of server and protocols that are supported by that server per Data Mover. Client machines on the LAN, with the appropriate access privileges, can then use file-side VNX to store and access data as they would any other network-based file server. Additionally, shared file systems can be configured for FTP or TFTP access.

VNX is responsible for enforcing all access permissions for user data. In File mode, each file server on VNX can be configured to interface with a Microsoft Active Directory server or utilize local user authentication files. When a request for data access is made from an IP-based client machine, VNX utilizes the appropriate authentication mechanism, checks the Access Control List (ACL) of the requested file or directory, and either grants or denies access to the Data Mover User. User data can be stored directly on storage provided by VNX.

The VNX hardware includes internal storage (disk arrays). This internal storage is configured to provide a storage system where VNX users can store data. The block storage portion of VNX's SOE allows this storage system to store and retrieve block units of data for VNX users on a SAN. Each of these block units is associated with a Logical Unit, which is in turn associated with a Logical Unit Number (LUN). Individual elements of the storage system are presented to VNX as Logical Units. Each Logical Unit is a useable storage system volume that VNX can use to store user data.

The Unisphere, Navisphere CLI and Control Station CLI software contain utilities for installing and configuring VNX, maintaining the system, and monitoring system performance. Unisphere uses a Java-capable web browser as its platform, Navisphere CLI runs on an administrator's management workstation, and Control Station CLI sits directly on the Control Station appliance. The Data Mover operating system is

[5] Unified Block and File mode is the evaluated configuration.

[6] Data Movers are also called X-Blades and the two terms are used interchangeably throughout the product's documentation.

referred to as DART (Data Access in Real Time). VNX can have from 1 to 8 Data Movers. There are several different models of Data Movers; however, use and management of all Data Movers is identical. VNX/Unisphere can be monitored by an EMC ControlCenter Agent Server to collect information on the health or status of the product.

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the TOE, and defining the specific evaluated configuration.

The TOE is the EMC® VNX OE for Block v05.33 and File v8.1 with Unisphere™ v1.3 running on VNX Series Hardware Models VNX5200™, VNX5400™, VNX5600™, VNX5800™, VNX7600™, and VNX8000™. The TOE is a combination File (NAS) and Block (SAN) operating environment with Unified Management (Unisphere). It includes a SOE, which provides RAID and storage provisioning capabilities, one or more NAS servers that allow LAN clients to connect and use internal storage, and a set of interfaces administrators can use to manage the TOE and access controls for internal storage.

The TOE is managed by authorized users through the Unisphere Manager, Navisphere CLI, and Control Station CLI interfaces. Unisphere Manager is a Java-based applet that runs within a web browser. Administrators access Unisphere through a secure Hypertext Transfer Protocol Secure (HTTPS) connection to configure and view management tasks. The Unisphere GUI may be accessed through web addresses pointed at the Control Station and Storage Processor. A majority of the functionality is available through either address. However, specific file-side functionality is hosted on the Control Station. Specific block-side functionality is hosted on the Storage Processor. The functionality available is based on the web address provided when the administrator first enters the Unisphere GUI.

Navisphere CLI is the main CLI component of the storage system and communicates via the HTTPS protocol. Navisphere CLI provides access to common functions for monitoring and managing internal storage with a text-based interface that is usable in non-graphical operating environments. Navisphere CLI provides access to functions for storage provisioning, status and configuration information retrieval, and control. The CLI commands can also be used to automate management functions via shell scripts and batch files.

The Control Station CLI is used to manage, configure, and monitor information on the Data Movers. The Control Station CLI may be accessed locally from the console by providing a valid username and password. The Control Station CLI may be accessed remotely via SSH. The user specifies the IP address of the Control Station and then enters valid username and password.

In Block mode, the TOE software includes a SOE optimized for implementation of RAID storage architectures, providing fault detection, isolation, and diagnosis capabilities. It enables the use of logical storage elements (LUNs) to improve performance and capacity utilization. The TOE also implements a technology called Access Logix. Access Logix lets multiple hosts share a storage system by using Storage Groups. A Storage Group is one or more Logical Units within a storage system that are reserved for one or more hosts and is inaccessible to other hosts. Access Logix enforces the host-to-Storage Group permissions.

The TOE also performs event monitoring of system status and host registration of client machines. This is done through the TOE's SP Agent. The SP Agent collects information about the state of the system, including the operating environment, hardware components associated with the TOE, and the TOE's Logical Units, and reports this information to authorized TOE users. The SP Agents also communicate host registration information between the SP Agents and the client machines. These agents periodically

retrieve volume-mapping information from the client machines and forward it to Unisphere Manager for display.

In File mode, the TOE provides NAS Services that allow hosts on a LAN to access file systems via one of the supported file-based protocols (SMB, NFS, and FTP). The TOE presents this storage as one or more file servers on the customer's network. Client systems that attempt to access the file systems must pass VNX access controls before the TOE allows the access to occur.

Figure 1 shows the details of the deployment configuration of the TOE:

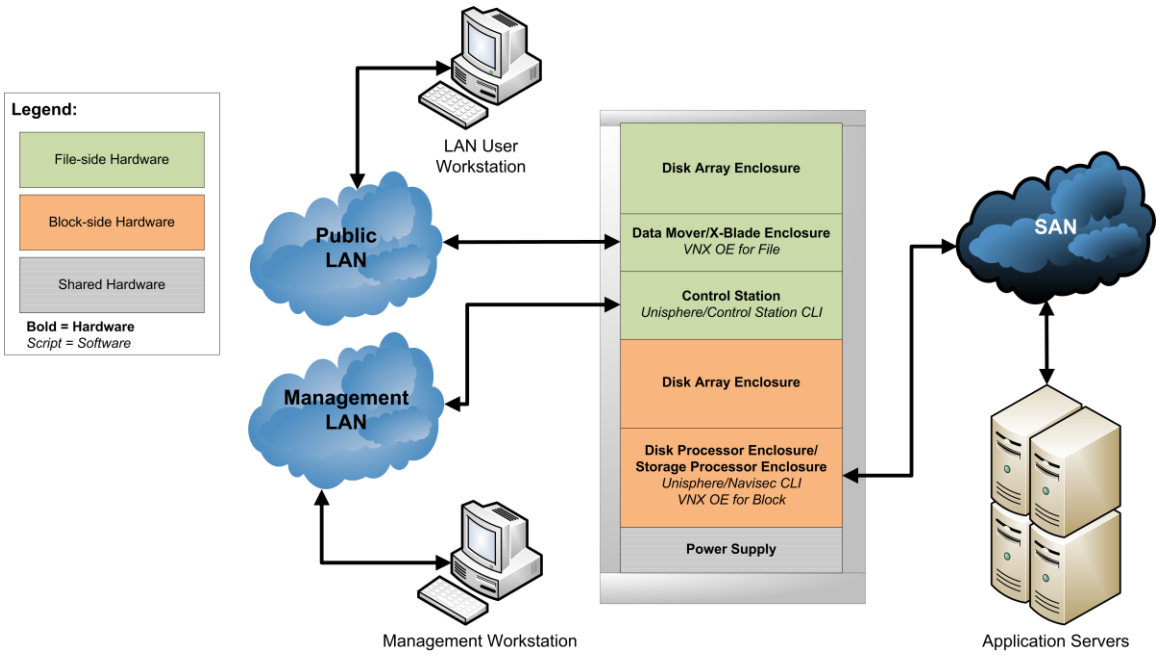

Figure 1 Deployment Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

The following sections describe the technologies and concepts related to the TOE.

1.4.1.1 Logical Units

The TOE works with storage entities called Logical Units. In Block mode, the TOE presents storage to client machines on the SAN in the form of Logical Units, and the TOE software provides for the management of Logical Units. Each Logical Unit represents a unit of storage to a client machine, analogous to a local disk drive. However, the Logical Unit provided by the TOE is not constrained to be a single individual disk. In fact, a typical deployment would have Logical Units that span multiple individual disks that are grouped into a RAID Group. Since IP-based client machines are presented storage as one or more file servers, Logical Units are not presented to IP-based clients.

1.4.1.2 File Servers

In File mode, the TOE presents storage to end users on a LAN through file server representations of that storage. File servers are hosted by the data movers. Each file server presents a portion of the internal storage to TOE users. TOE users access this storage as they would any NAS storage.

1.4.1.3 Storage Processors

The central component of the TOE in Block mode is the SP. The SP is responsible for interfacing with the SAN and with each of the individual disks within the VNX. There are two SPs in each TOE which logically operate as a single entity to provide increased performance and fault tolerance. The SP provides administrators with the ability to manage the TOE and establish Logical Units and RAID Groups.

1.4.1.4 RAID Groups

A RAID Group is a collection of individual disks. The TOE supports a variety of disk types and capacities (chosen by the customer when the product is purchased). In a RAID Group, disks of a similar type are typically grouped together. This RAID Group can then be configured by an administrator with various attributes, such as which RAID level to provide. In this manner, an administrator can manage the TOE through successive levels of abstraction.

1.4.1.5 Storage Groups

The TOE manages access to Logical Units through a component of the SP called Access Logix. Access Logix allows an administrator to group Logical Units together in Storage Groups. Each Storage Group can then be mapped to one or more client machines, identified by their Fibre Channel World Wide Name[7] (WWN) or iSCSI Qualified Name[8] (IQN). When this mechanism is used, a client machine can only access Logical Units that are present in a Storage Group that the client machine has been permitted to access.

It is also possible that multiple client machines are given access to the same Storage Group. This is used in cases where the client machine has been deployed in such a way as to manage multiple servers accessing the same Logical Unit, for example, in a clustered environment.

1.4.1.6 Management Software

Unisphere is the Java GUI used to manage the TOE. Administrators log into Unisphere in order to manage the TOE or the policies that control user access to storage. Management functionality is presented in the form of multiple screens that contain graphical elements, such as fields, buttons, and boxes. Unisphere also provides utilities to maintain and install the TOE. In addition to Unisphere, the TOE provides two CLI interfaces, Navisphere CLI and Control Station CLI, that administrators can use to manage the TOE.

[7] A World Wide Name is a unique identifier in a Fibre Channel.
[8] An iSCSI Qualified Name is a unique identifier in a Serial Attached SCSI storage network.

Navisphere CLI contains a subset of the Unisphere functionality, while Control Station CLI provides management functionality specific to File mode operations.

1.4.1.7 Data Movers

Hardware/software components called Data Movers implement NAS functionality. Data Movers transfer data between the internal storage and LAN clients. Each Data Mover can host one or more file servers that present shared services to client machines on a LAN. Data Movers leverage a secure private network with the Control Station to accept configuration information.

1.4.2 TOE Environment

The TOE is intended to be deployed in a secure data center that protects physical access to the TOE. The TOE is intended to be connected to a SAN with the constituent servers managed by administrators operating under a consistent security policy with the administrators that manage the TOE.

The TOE provides access control to individual Logical Units through its Access Logix component. For this to operate correctly, the WWN that is provided to the TOE must be accurate and must not be spoofed. The TOE Environment is required to provide this.

The TOE relies on secure access provided by the LAN and SAN to which it is attached. The purpose of the TOE is to mediate access to user data for client machines connected to an IP network or SAN. This functionality requires that the communications paths to the LAN and SAN be managed properly.

In a deployment where NFS is used, the systems accessing NFSv2 and v3 server shares are responsible for authenticating users. SMB, NFSv4, and FTP provide for authentication to be carried out by the TOE's file server against the data store configured by TOE administrators, which may be an external authentication server[9].

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

[9] Active Directory is the external authentication server used to identify and authenticate Data Mover users in the evaluated configuration.

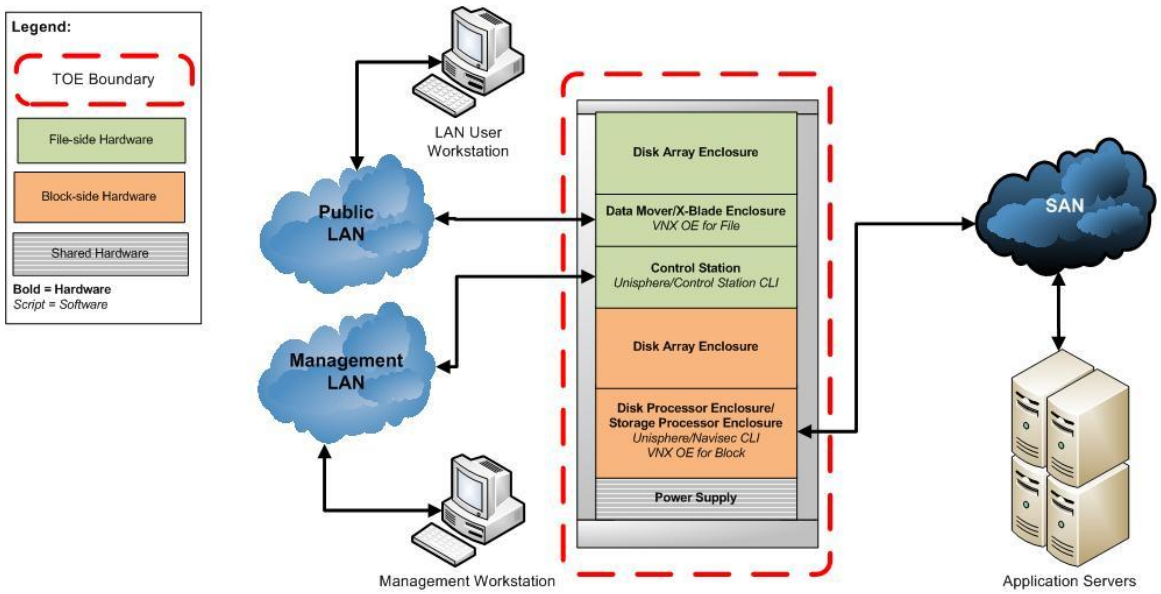

Figure 2 Physical TOE Boundary[10]

1.5.1.1 TOE Hardware

The TOE is comprised of the following VNX hardware components:

- Disk Array Enclosure (DAE)
- Data Mover, referred to as X-Blade
- Control Station
- Storage Processor or Disk Processor Enclosure
- Power Supply

Table 2 shows the hardware configuration for each VNX model being evaluated.

Table 2 – VNX Hardware Configuration

	5200	5400	5600	5800	7600	8000
Drive Count	4 – 125	4 – 250	4 – 500	4 – 750	4 – 1000	4 – 1000
Drive Types	Flash, SAS[11], NL-SAS[12]	Flash, SAS, NL-SAS	Flash, SAS, NL-SAS	Flash, SAS, NL-SAS	Flash, SAS, NL-SAS	Flash, SAS, NL-SAS
Data Mover Count	1 - 2	1 - 2	1 – 2	1 – 3	2 – 4	2 – 8
Control Station Count	1 - 2	1 - 2	1 - 2	1 - 2	1 - 2	1 - 2
File Protocols	NFS, SMB, MPFS[13], pNFS	NFS, SMB, MPFS, pNFS	NFS, SMB, MPFS, pNFS	NFS, SMB, MPFS, pNFS	NFS, SMB, MPFS, pNFS	NFS, SMB, MPFS, pNFS

[10] There are a possible 1 – 8 data movers supported per configuration. Refer to Table 2 for data mover configuration supported for each hardware model.
[11] SAS - Serial Attached SCSI
[12] NL-SAS – Nearline Serial Attached SCSI

	5200	5400	5600	5800	7600	8000
Array enclosure/SP Count	DPE[14]/2 SP	DPE/2 SP	DPE/2 SP	DPE/2 SP	DPE/2 SP	SPE[15]/2 SP
Block Protocols	FC, iSCSi, FCoE[16]	FC, iSCSi, FCoE	FC, iSCSi, FCoE	FC, iSCSi, FCoE	FC, iSCSi, FCoE	FC, iSCSi, FCoE
Power Supply Count	2	2	2	2	2	2

TOE Environment

The essential components of the TOE Environment are:

- Management workstation
- Active Directory domain controller to identify and authenticate LAN users
- Application servers to utilize the Block storage services provided by the TOE
- LAN users to utilize the File storage services provided by the TOE
- Cables, connectors, and switching and routing devices that allow all of the TOE and environmental components to communicate with each other

1.5.1.2 TOE Software

The essential software components for the proper operation of the TOE in the evaluated configuration are:

- VNX OE for File v8.1.1.33
- VNX OE for Block v05.33.000.5.035
- Unisphere v1.3.1.1.0033
- Navisphere CLI v7.33.1.0.33

1.5.1.3 Guidance Documentation

The following guides are required reading and part of the TOE:

- EMC, Setting up a Unisphere Management Station for the VNX Series, P/N 300-015-123, Rev 01
- EMC VNX, VNX5200 Unified Installation Guide, P/N 300-999-780, Rev 01
- EMC VNX, VNX5200 Block Installation Guide, P/N 300-999-786, Rev 01
- EMC VNX, VNX5200 File Installation Guide, P/N 300-999-792, Rev 01
- EMC VNX Family, VNX5200, Parts Location Guide, PN 300-015-012, Rev 01
- EMC VNX Family, VNX5200, Hardware Information Guide, P/N 300-014-323, Rev 01
- EMC VNX, VNX5400 Unified Installation Guide, P/N 300-999-781, Rev 03
- EMC VNX, VNX5400 Block Installation Guide, P/N 300-999-787, Rev 03
- EMC VNX, VNX5400 File Installation Guide, P/N 300-999-793, Rev 03
- EMC VNX Family, VNX5400, Parts Location Guide, PN 300-015-013, Rev 01
- EMC VNX Family, VNX5400, Hardware Information Guide, P/N 300-014-324, Rev 02
- EMC VNX, VNX5600 Unified Installation Guide, P/N 300-999-782, Rev 03
- EMC VNX, VNX5600 Block Installation Guide, P/N 300-999-788, Rev 03

[13] MPFS – Multi Path File System
[14] DPE – Disk-processor Enclosure
[15] SPE – Storage-processor Enclosure
[16] FCoE – Fibre Channel over Ethernet

- EMC VNX, VNX5600 File Installation Guide, P/N 300-999-794, Rev 03
- EMC VNX Family, VNX5600, Parts Location Guide, PN 300-015-014, Rev 01
- EMC VNX Family, VNX5600, Hardware Information Guide, P/N 300-014-325, Rev 01
- EMC VNX, VNX5800 Unified Installation Guide, P/N 300-999-783, Rev 03
- EMC VNX, VNX5800 Block Installation Guide, P/N 300-999-789, Rev 03
- EMC VNX, VNX5800 File Installation Guide, P/N 300-999-795, Rev 03
- EMC VNX Family, VNX5800, Parts Location Guide, PN 300-015-015, Rev 01
- EMC VNX Family, VNX5800, Hardware Information Guide, P/N 300-014-326, Rev 02
- EMC VNX, VNX7600 Unified Installation Guide, P/N 300-999-790, Rev 03
- EMC VNX, VNX7600 Block Installation Guide, P/N 300-999-784, Rev 03
- EMC VNX, VNX7600 File Installation Guide, P/N 300-999-796, Rev 03
- EMC VNX Family, VNX7600, Parts Location Guide, PN 300-015-016, Rev 01
- EMC VNX Family, VNX7600, Hardware Information Guide, P/N 300-014-327, Rev 02
- EMC VNX, VNX8000 Unified Installation Guide, P/N 300-999-791, Rev 03
- EMC VNX, VNX8000 Block Installation Guide, P/N 300-999-785, Rev 03
- EMC VNX, VNX8000 File Installation Guide, P/N 300-999-797, Rev 03
- EMC VNX Family, VNX8000, Parts Location Guide, PN 300-015-017, Rev 01
- EMC VNX Family, VNX8000, Hardware Information Guide, P/N 300-014-328, Rev 02
- EMC VNX Series, Release 5.33, Command Line Interface Reference for Block P/N 300-015-135 Rev 01
- EMC VNX Series, Release 8.1, Command Line Interface Reference for File P/N 300-014-338 Rev 01
- EMC VNX Series, Release 8.1, Security Configuration Guide for VNX, P/N 300-015-128, Rev 01
- EMC VNX Series, Release 8.1, System Operations, P/N 300-015-124, Rev 02
- EMC VNX Series, Release 8.1, Configuring NFS on VNX, P/N 300-014-336, Rev 01
- EMC VNX Series, Release 8.1, Configuring and Managing CIFS on VNX, P/N 300-014-332, Rev 01
- EMC VNX Series, Release 8.1, Controlling Access to VNX System Objects, P/N 300-015-106, Rev 01
- EMC VNX Series, Release 8.1, Using FTP, TFTP, and SFTP on VNX, P/N 300-015-134, Rev 01
- EMC VNX, Configuring Time Services on VNX, P/N 300-015-103, Rev 01
- EMC VNX, VNX Operating Environment for Block 05.33.000.5.035, VNX Operating Environment for File 8.1.1.33, EMC Unisphere 1.3.1.1.0033, Release Notes, P/N 32-000-403, Rev 02
- EMC VNX Unisphere Online Help 1.3

1.5.2 Logical Scope

The TOE logical boundary is defined by the security functions that it implements. The security functions implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Cryptographic Support
- Protection of the TSF
- Trusted Path/Channel

1.5.2.1 Security Audit

The TOE generates audit records for all administrator actions that result in a configuration change and all login attempts. Authorized administrators can view, sort, and filter the audit records.

1.5.2.2 User Data Protection

The User Data Protection function implements functionality necessary to protect user data which is entrusted to the TOE. In File mode, this functionality is primarily enforced by each of the Data Movers in the TOE. Users of the TOE are identified and authenticated, either by the TOE or the TOE Environment. These Data Mover users are then granted access to files and directories managed by the TOE. Each file and directory has an Access Control List (ACL) that contains the access privileges for Data Mover users of the TOE to that object.

In Block mode, Storage Processors govern access to storage by using Storage Groups. Individual devices on the SAN are assigned to Storage Groups, which allows them to access storage provided by the TOE. If a device is not a member of a Storage Group that grants access to a particular set of storage, then that device is not able to access that storage.

The TOE protects user data primarily in two additional ways. First, it ensures that only the client machines that have been granted access to a LUN have access to that LUN. Second, it ensures the integrity of the data entrusted to it through its use of RAID levels.

1.5.2.3 Identification and Authentication

This function of the TOE is used to identify and authenticate each operator of the TOE. In the case of Unisphere administrators, the TOE provides username and password verification functionality. Though administrators may be authenticated by LDAP, only local administrator authentication is considered for this evaluation. Data Mover Users of the TOE (e.g., LAN users) can be authenticated directly by the TOE or can be authenticated by a separate, external Active Directory, Kerberos, or NFS[17] server in the TOE environment. In the evaluated configuration, Data Mover Users of the TOE are authenticated by an Active Directory domain controller in the TOE environment, which provides the user identity as needed to enforce access control.

1.5.2.4 Security Management

The Security Management functionality of the TOE specifies several aspects of management of the TOE Security Function (TSF). Proper management of the TSF is required to properly mediate access to user data.

The TOE is managed by authorized administrators through the Unisphere Manager, Navisphere CLI, and Control Station CLI. Unisphere Manager is a Java applet that runs within a web browser. Navisphere CLI is a command line interface that provides access to common functions for monitoring and managing the TOE. The Control Station CLI contains management functionality specific to the File-side features of the TOE.

The Security Management function provides administrators with the ability to properly manage and configure the TOE to store user data. Administrators are assigned a role that governs what aspects of the TOE they are authorized to manage. Configuration of RAID settings, Storage Group membership, and administrator access is all supported through this security function.

1.5.2.5 Cryptographic Support

The TOE leverages two FIPS 140-2 validated modules (Cert. #1092 and #1051) to support cryptographic operations. These include: symmetric encryption/decryption using AES[18], signature generation/verification using RSA[19], hashing using SHA[20], and message authentication using HMAC[21]-SHA. Cryptographic keys

[17] Kerberos and NFS authentication are only available for File-side clients.
[18] AES – Advanced Encryption Standard
[19] RSA – Rivest, Shamir, Adleman
[20] SHA – Secure Hash Algorithm
[21] HMAC – Hash-Based Message Authentication Code

are generated using a NIST[22] Special Publication (SP) 800-90 random bit generator. Keys are zeroized when no longer needed by the application.

The TOE requires cryptographic support for the functionality discussed in section 1.5.2.7 below.

1.5.2.6 Protection of the TSF

Connection to a NTP[23] service and hardware clocks on the Control Station, Data Mover, and Storage Processor are used to ensure consistent time stamps across the TOE.

1.5.2.7 Trusted Path/Channels

The TOE leverages FIPS-validated cryptographic modules to establish a trusted path between itself and its users. Access to Unisphere and Navisphere CLI on the Control Station are established through a Secure Hypertext Transfer Protocol (HTTPS).

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- Remotely Anywhere
- Unisphere Analyzer
- Unisphere SnapView
- Unisphere MirrorView/Asynchronous
- Unisphere MirrorView/Synchronous
- Unisphere SAN Copy
- Unisphere Quality of Service Manager (UQM)
- iSCSI functionality
- Access Control Levels for Unisphere Administrators
- Multi-Path File System
- Replication Technologies
- VNX FileMover
- TFTP
- Use of DSA[24] keys for SSH
- Storage Processor service port
- Physical hard disks[25]

The TOE supports several File System Access Policies. For the purposes of this evaluation, only the "MIXED" Access Policy is to be evaluated. The "NATIVE", "NT", "UNIX", "SECURE", and "MIXED_COMPAT" Policies are excluded from the evaluation.

[22] NIST – National Institute of Standards and Technology
[23] NTP – Network Time Protocol
[24] DSA – Digital Signature Algorithm
[25] While these disks are not part of the TOE, the TOE does provide physical protection of the hard disks by fully enclosing them within the TOE's physical boundary.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM[26] as of 2013-07-29 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.2)

[26] CEM - Common Evaluation Methodology

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[27] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[28] and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 4 – Threats

Name	Description
T.DATA_CORRUPTION	Data could become corrupted due to hardware failure or incorrect system access by users of the TOE or attackers.
T.IMPROPER_SERVER	A system connected to the TOE could access data that it was not intended to gain access by bypassing the protection mechanisms of the TOE.
T.IMPROPER_CONFIG	The TOE could be misconfigured by an administrator to provide improper storage or enforce improper access to user data.
T.MEDIATE_ACCESS	Access to user data could be improperly granted by an administrator to users who should not have access to it.
T.UNAUTH	An unauthorized user could access data stored by the TOE by bypassing the protection mechanisms of the TOE.
T.CRYPTO	An attacker could attempt to exploit a weakness in a cryptographic algorithm to gain access to management communications.

[27] IT – Information Technology
[28] TSF – TOE Security Functionality

Name	Description
T.ACCESS	An attacker could attempt to gain access to the TOE by accessing the physical network and attempting to sniff data transmitted.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this ST.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 – Assumptions

Name	Description
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PHYSICAL	Physical security will be provided for the TOE and its environment.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.I&A	The TOE environment will provide identification and authentication of Application Server users before allowing any other TSF-mediated actions on behalf of those users.
A.PRIVATE	The IT environment will be configured in such a way as to ensure secure and private transmission of TOE management traffic on a separate LAN.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 6 – Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must record audit records for data accesses and use of the TOE functions on the management system.
O.AUDIT_REVIEW	The TOE must provide authorized administrators with the ability to review the audit trail.
O.ADMIN	The TOE must provide a method for administrative control of the TOE.
O.PROTECT	The TOE must protect data that it has been entrusted to protect.
O.I&A	The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.
O.CRYPTO	The TOE must be able to enforce FIPS validated algorithms to protect management communications.
O.ACCESS	There must be a secure path for communication between users and the TOE.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment:

Table 7 – IT Security Objectives

Name	Description
OE.I&A	The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.

Name	Description
OE.SECURE_COMMUNICATIONS	The TOE Environment must provide secure communications between systems connected to the Storage Area Network.
OE.SECURE_MGMT_COMMUNICATIONS	The TOE Environment must provide secure communications between systems connected to the Management LAN.
OE.SECURE_SERVERS	The TOE Environment must provide properly configured authentication servers and client machines to communicate with the TOE.
OE.TIME	The TOE environment must provide reliable time stamps to the TOE.
OE.PROPER_NAME_ASSIGNMENT	The TOE Environment must provide accurate World Wide Names for each system that communicates with the TOE.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 – Non-IT Security Objectives

Name	Description
NOE.MANAGE	Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.
NOE.NOEVIL	Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.
NOE.PHYSICAL	The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.

5 Extended Components

There are no extended SFRs and extended SARs for this evaluation of the TOE.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter following the component title. For example, FAU_GEN.1a Audit Data Generation would be the first iteration and FAU_GEN.1b Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_ACC.1a	Subset access control		✓		✓
FDP_ACC.1b	Subset access control		✓		✓
FDP_ACF.1a	Security attribute based access control		✓	✓	✓
FDP_ACF.1b	Security attribute based access control		✓		✓
FDP_SDI.2	Stored data integrity		✓	✓	
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.2	User authentication before any action				

Name	Description	S	A	R	I
FIA_UID.2	User identification before any action				
FMT_MSA.1a	Management of security attributes	✓	✓		✓
FMT_MSA.1b	Management of security attributes	✓	✓		✓
FMT_MSA.3a	Static attribute initialization	✓	✓		✓
FMT_MSA.3b	Static attribute initialization	✓	✓		✓
FMT_MTD.1a	Management of TSF data	✓	✓		✓
FMT_MTD.1b	Management of TSF data	✓	✓		✓
FMT_MTD.1c	Management of TSF data	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_STM.1	Time stamps				
FTP_TRP.1	Trusted path	✓	✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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) [*All administrator actions that result in a configuration change to the storage array, all administrators login attempts*].

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, [*no other audit relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*authorized administrators*] 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.

Dependencies: FAU_GEN.1 Audit data generation

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
FCS_CKM.1.1
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*defined in Table 10 below*] and specified cryptographic key sizes [*defined in Table 10 below*] that meet the following: [*standards defined in Table 10 below.*]
Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

Application note: The FIPS 140-2 validated cryptographic modules available on the Storage Processor and Control Station provide FIPS-Approved key generation algorithms.

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
FCS_CKM.4.1
The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2*].
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

Application note: The FIPS 140-2 validated cryptographic modules available on the Storage Processor and Control Station provide FIPS compliant zeroization.

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
FCS_COP.1.1
The TSF shall perform [*symmetric encryption/decryption, asymmetric encryption/decryption, key generation, random bit generation, signature generation/verification, hashing, and message authentication*] in accordance with a specified cryptographic algorithm [*defined in Table 10 below*] and cryptographic key sizes [*defined in Table 10 below*] that meet the following: [*standards defined in Table 10 below.*]
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Application note: The FIPS 140-2 validated cryptographic modules are available on the Storage Processor and Control Station.

Table 10 – Cryptographic Algorithms[29]

Algorithm	Key Size	Standard	CAVP[30] Certificate No.
AES	AES keys 128, 192, 256 bits	FIPS 197	860, 695, 1534, 1630, 1933, 2011

[29] Algorithm certification and key information taken from *OpenSSL Module v1.2.4 FIPS 140-2 Security Policy* and *RSA BSAFE Crypto-C Micro Edition Version 3.0.0.1 Security Policy*
[30] CAVP – Cryptographic Algorithm Validation Program

Algorithm	Key Size	Standard	CAVP[30] Certificate No.
Triple DES[31]	Triple-DES keys 168	NIST SP 800-67	707, 627, 1011, 1066, 1259, 1297
ANSI[32] X9.31PRNG[33]	PRNG seed value and seed key 128 bits	FIPS 186-2	492, 407, 826, 873, 1018, 1053
SHA-1	160-bit Digest	FIPS 180-4	855, 723, 1362, 1435, 1698, 1761
SHA-224	224-bit Digest	FIPS 180-4	855, 723, 1362, 1435, 1698, 1761
SHA-256	256-bit Digest	FIPS 180-4	855, 723, 1362, 1435, 1698, 1761
SHA-384	364-bit Digest	FIPS 180-4	855, 723, 1362, 1435, 1698, 1761
SHA-512	512-bit Digest	FIPS 180-4	855, 723, 1362, 1435, 1698, 1761
HMAC-SHA-1	160-bit Digest	FIPS 198-1	477, 373, 892, 957, 1167, 1216
HMAC-SHA224	224-bit Digest	FIPS 1981	477, 373, 892, 957, 1167, 1216
HMAC-SHA256	256-bit Digest	FIPS 198-1	477, 373, 892, 957, 1167, 1216
HMAC-SHA384	384-bit Digest	FIPS 198-1	477, 373, 892, 957, 1167, 1216
HMAC-SHA512	512-bit Digest	FIPS 198-1	477, 373, 892, 957, 1167, 1216
RSA sign, verify, and keygen	RSA keys 2048 and higher	X9.31, PKCS[34] #1.5, PSS[35]	412, 323, 745, 804, 999, 1040

[31] DES – Data Encryption Standard
[32] ANSI – American National Standards Institute
[33] PRNG – Pseudorandom Number Generator
[34] PKCS – Public Key Cryptography Standard
[35] PSS – Probabilistic Signature Scheme

6.2.3 Class FDP: User Data Protection

FDP_ACC.1a Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1a

The TSF shall enforce the [*Discretionary Access Control SFP*[36]] on
[
a) Subjects: Application servers
b) Objects: LUNs
c) Operations: Read and write
].

Application note: the Subjects are client machines connected to the SAN acting on behalf of an authorized user.

Dependencies: FDP_ACF.1a Security attribute based access control

FDP_ACF.1a Security attribute based access control
Hierarchical to: No other components.
FDP_ACF.1.1a

The TSF shall enforce the [*Discretionary Access Control SFP*] to objects based on the following:
[
Subject attributes:
1. *World Wide Name*
2. *Storage Group Membership*

Object Attributes:
1. *LUN ID*[37]
2. *Storage Group Membership*

].

FDP_ACF.1.2a

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[
A valid subject of the TOE is allowed to read and write to a LUN if the subject and the LUN are members of the same storage group
].

FDP_ACF.1.3a

The TSF shall explicitly authorize access of subjects to objects based on ~~the following~~ **no** additional rules: [~~assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*~~].

FDP_ACF.1.4a

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*]. ~~the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].~~

Dependencies: FDP_ACC.1a Subset access control
FMT_MSA.3a Static attribute initialization

[36] SFP – Security Functional Policy
[37] ID – Identifier

FDP_ACC.1b Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1b

The TSF shall enforce the [*File and Directory Access SFP*] on
[

a) Subjects: SMB, NFS, and FTP Users
b) Objects: Files and Directories
c) Operations: Create, Read, Write, Append, Execute, Delete, Change Ownership, Read Permissions, Change Permissions, Read Attributes, Write Attributes, Read Extended Attributes, and Write Extended Attributes].

Dependencies: FDP_ACF.1b Security attribute based access control

Application Note: The SMB naming convention has been used for operations. Equivalent operations are provided via NFS v4, but may be named slightly differently by NFS clients. FTP, NFS v2, and NFS v3 access supports a subset of these operations.

FDP_ACF.1b Security attribute based access control
Hierarchical to: No other components.
FDP_ACF.1.1b

The TSF shall enforce the [*File and Directory Access SFP*] to objects based on the following:
[
Subject attributes:

1. *UserID*
2. *GroupIDs*

Object attributes:

1. *UTF[38]-8 Filename*
2. *UTF-16 Filename*
3. *8.3 MS[39]-DOS[40] Filename*
4. *Access Control List*

].

FDP_ACF.1.2b

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*A valid subject of the TOE is allowed to perform an operation if the contents of the Access Control List for the object authorize the UserID or a GroupID of the Subject to perform the desired operation*].

FDP_ACF.1.3b

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:
[

1. *For SMB access, subjects that are members of the group Local Administrators shall be authorized to backup, restore, and take ownership of all objects*
2. *For NFS access, subjects that are authorized as superusers can perform all operations on all objects*

].

FDP_ACF.1.4b

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*A valid subject of the TOE is explicitly denied the ability to perform an operation if the contents of the Access Control List for the object explicitly deny the UserID or a GroupID of the Subject to perform the desired operation*].

[38] UTF – Unicode Transformation Format
[39] MS – Microsoft
[40] DOS – Disk Operating System

Dependencies: **FDP_ACC.1b Subset access control**
FMT_MSA.3b Static attribute initialization

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.2.1

The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all **user data** ~~objects~~, based on the following attributes: [*parity data for RAID 3, RAID 5, and RAID 6; mirrored data for RAID 1 and RAID 1+0*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [*reconstruct the user data for RAID 3, RAID 5, and RAID 6; replace erroneous data with the mirrored data for RAID 1, and RAID 1+0; and notify an administrator*].

Dependencies: **No dependencies**

6.2.4 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: [*UserID, one or more GroupIDs, and a password*].
Dependencies: No dependencies

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
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_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
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.
Dependencies: No dependencies

6.2.5 Class FMT: Security Management

FMT_MSA.1a Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1a
The TSF shall enforce the [*Discretionary Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*Storage Group Membership*] to [*the administrator, sanadmin, and storageadmin roles*].
Dependencies: FDP_ACC.1a Subset access control or
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1b Management; of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1b
The TSF shall enforce the [*File and Directory Access SFP*] to restrict the ability to [modify, delete, [*and add*]] the security attributes [*UserID and GroupID assignment*] to [*authorized roles*].
Dependencies: FDP_ACC.1b Subset access control or
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3a Static attribute initialization
Hierarchical to: No other components.
FMT_MSA.3.1a
The TSF shall enforce the [*Discretionary Access control SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2a
The TSF shall allow the [*administrator, sanadmin, and storageadmin roles*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies: FMT_MSA.1a Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3b Static attribute initialization
Hierarchical to: No other components.
FMT_MSA.3.1b
The TSF shall enforce the [*File and Directory Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2b
The TSF shall allow the [*Object Owner*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies: FMT_MSA.1b Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1a Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1a
The TSF shall restrict the ability to [query] the [*storage system information*] to [*all roles except securityadministrator*].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1b Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1b
The TSF shall restrict the ability to [query, modify, delete, [*create*]] the [*LUNs, RAID Groups, and Storage Groups*] to [*the administrator, sanadmin, and storageadmin roles*].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1c Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1c
The TSF shall restrict the ability to [query, modify, delete, [*create*]] the [*user accounts*] to [*the securityadministrator role*].
Dependencies: FMT_SMF.1 Specification of management functions
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 management functions:
[
a) Management of security functions behavior;
b) Management of TSF data;
c) Management of security attributes
].
Dependencies: No Dependencies

FMT_SMR.1 Security roles
Hierarchical to: No other components.
FMT_SMR.1.1
The TSF shall maintain the roles [*the authorized roles identified in* Table 11].
FMT_SMR.1.2
The TSF shall be able to associate users with roles.
Dependencies: FIA_UID.1 Timing of identification

Table 11 – Authorized Roles

Role	Description	GUI Name
Operator	Read only for storage and domain information. No security, not even read.	Operator
networkadmin	DNS[41]/IP settings for management path only. Routing/SNMP[42] + Operator	Network Administrator
Nasadmin	On File, NAS storage tasks only. Root role to configure Control Station network interfaces.	NAS administrator
Sanadmin	Block storage tasks only. Operator on File.	SAN administrator
storageadmin	nasadmin + sanadmin	Storage administrator

[41] DNS – Domain Name System
[42] SNMP – Simple Network Management Protocol

Role	Description	GUI Name
securityadministrator	Security and Domain tasks	Security administrator
administrator	Securityadministrator + storageadmin + networkadmin	Administrator
localdataprotection	Snap/Clone on Block. Checkpoints on File.	Local dataprotection
dataprotection	Localdataprotection + mirror on Block. Checkpoints on File	Dataprotection
datarecovery	On Block, localdataprotection + dataprotection. Additionally, recovery tasks, e.g. rollback. Replication Full Control and Checkpoints Full Control on File.	Datarecovery

6.2.6 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
FPT_STM.1
The TSF shall be able to provide reliable time stamps.
Dependencies: No dependencies

6.2.7 Class FTP: Trusted path/channels

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [remote] 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 and disclosure].

FTP_TRP.1.2

The TSF shall permit *[*remote users*]* to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for *[*initial authentication and functions modifying management configuration information*]*.

Dependencies: No dependencies

Application note: The TOE implements a trusted path on the Unisphere GUI and Navisphere CLI.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 12 – Assurance Requirements summarizes the requirements.

Table 12 – Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM[43] coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

[43] CM – Configuration Management

7 TOE Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 13 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
User Data Protection	FDP_ACC.1a	Subset access control
	FDP_ACC.1b	Subset access control
	FDP_ACF.1a	Security attribute based access control
	FDP_ACF.1b	Security attribute based access control
	FDP_SDI.2	Stored data integrity
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MSA.1a	Management of security attributes
	FMT_MSA.1b	Management of security attributes
	FMT_MSA.3a	Static attribute initialization
	FMT_MSA.3b	Static attribute initialization
	FMT_MTD.1a	Management of TSF data
	FMT_MTD.1b	Management of TSF data
	FMT_MTD.1c	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Cryptographic Support	FCS_CKM.1	Cryptographic key generation

TOE Security Functionality	SFR ID	Description
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Protection of the TSF	FPT_STM.1	Time stamps
Trusted Path/Channels	FTP_TRP.1	Trusted path

7.1.1 Security Audit

The TOE generates audit records for startup and shutdown of the audit function, all administrator actions that result in a configuration change and all login attempts. Audit records contain the date and time of the event, the type of event, subject identity (if applicable), and the outcome of the event. Authorized administrators can view the audit records from the CLI or GUI. Audit records are presented to administrators in a clearly understandable format.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1.

7.1.2 Cryptographic Support

The TOE utilizes two FIPS 140-2 validated cryptographic modules: OSSI[44] OpenSSL[45] (CMVP[46] Certificate #1051) running on the Control Station, and RSA BSAFE Crypto-C ME[47] (CMVP Certificate #1092) on the Control Station and Storage Processor. These modules implement the AES, 3DES, ANSI X9.31 PRNG, SHA, HMAC-SHA, and RSA algorithms. Certificates for these algorithms are listed in Table 10 in section *6.2.2 Class FCS: Cryptographic Support* above**.** The modules generate and zeroize cryptographic keys in accordance with FIPS 140-2 requirements. FIPS 140-2-required self-tests are performed on the cryptographic algorithms and the cryptographic modules as a whole to ensure their proper function.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

7.1.3 User Data Protection

This section describes the various User Data Protection SFRs claimed.

7.1.3.1 File and Directory Access SFP

The TOE enforces the File and Directory Access SFP[48] on each Data Mover User of the TOE based on the security attributes of that user. This is achieved by assigning access privileges to users based on their UserID and GroupIDs. The ability to perform operations on objects, which are governed by the File and Directory Access SFP, are granted to Data Mover Users by an object's owner. Thus, a Data Mover User is allowed to perform an operation on an object so long as permission is granted to the user within the object's ACL. A Data Mover User can also be denied the ability to perform an operation on an object if the contents of the object's ACL deny the desired operation based on the UserID or GroupID of the User.

[44] OSSI – Open Source Software Institute
[45] SSL – Secure Sockets Layer
[46] CMVP – Cryptographic Module Validation Program
[47] MES – Micro Edition
[48] SFP – Security Functional Policy

Under the SMB access protocol, Data Mover Users are allowed to backup, restore, and take ownership of all objects if they are member of the local Administrators group. For the NFS access protocol, Data Mover Users who are *superusers* can perform all operations on all objects.

The TOE is designed to mediate access to files and directories for authorized Data Mover Users. These files and directories are stored within internal storage. The TOE accesses the storage to provide Data Mover Users access to their data through several standard IP network file sharing mechanisms.

Identification and authentication of Data Mover Users is performed by the Identification and Authentication security function. Once a user has been successfully authenticated, the TOE is then in possession of the UserID and one or more GroupIDs for that User. These credentials are used to mediate access to files and directories.

Each file and directory managed by the TOE has an ACL associated with it. This ACL contains one or more Access Control Entries (ACEs). Each ACE contains a UserID or GroupID and a set of permissions that are granted or explicitly denied to that UserID or GroupID. Whenever a Data Mover User requests access to a file or directory, the TOE utilizes its File and Directory Access SFP to decide whether or not access is permitted. The TOE uses the UserID and GroupIDs of the user and the contents of the ACL to determine if the operation should be allowed to proceed.

7.1.3.2 Discretionary Access SFP

The TOE also provides the User Data Protection security function to manage access from client machines to configured Logical Units. The TOE provides this functionality for servers connected to the SAN.

Using the Security Management security function, Administrators of the TOE can configure Logical Units to provide storage to client machines. These Logical Units are then placed into Storage Groups, which allows an Administrator to limit access to each Logical Unit to one or more client machines. When a client machine requests a list of available Logical Units from the TOE, the TOE Environment provides a WWN. This WWN is used to identify the client machine to the TOE. The TOE then provides a list of Logical Units that the client machine has been granted access to. With each successive request to read or write information to or from a Logical Unit, the TOE ensures that only authorized client machines have access to the Logical Units to which they have been given access.

The TOE also provides for the integrity of user data. When creating RAID Groups from individual disk drives, an Administrator can configure RAID levels 0, 1, 1+0, 3, 5, or 6. Each of these, except RAID level 0, provides fault tolerance for integrity errors or individual disk drive failure. The TOE provides mechanisms to check data integrity continuously while reading and writing data to individual disks. Integrity errors or drive errors are fixed on-the-fly. Additionally, Administrators can configure “hot spare” disk drives. These “hot spares” are used when a disk failure has been detected by the system. Once a failure has been detected, the drive that has been lost will be recreated on the “hot spare”. The Administrator can then replace the failed drive and configure it as a new “hot spare”. This process is provided while real-time access to user data continues.

TOE Security Functional Requirements Satisfied: FDP_ACC.1a, FDP_ACF.1a, FDP_ACC.1b, FDP_ACF.1b, FDP_SDI.2.

7.1.4 Identification and Authentication

The TOE performs identification and authentication of both Administrators and Data Mover Users. The purpose of the identification and authentication function is to allow the TOE to restrict access to both administrative functions and to user data based upon the authenticated identity and associated attributes of a user.

7.1.4.1 Administrative I&A

Unisphere Administrators can access the TOE through a web browser or through a command line interface. The TOE supports internally enforced username and password-based authentication as well as authentication against an LDAP authentication server (LDAP authentication is not considered for the evaluated configuration). The first action that operators must take when attempting to interact with the TOE is to provide a username and password. Before identification and authentication, the TOE operator is not able to perform any TOE security functionality. Administrative accounts are maintained on both the Control Station and the Storage Processor.

7.1.4.2 User I&A

Data Mover Users of the TOE are defined as those subjects that wish to use the TOE to store and mediate access to data. Data Mover Users of the TOE would typically not be Administrators (although administrative access may be established with separate user credentials.).

The identification and authentication function on the TOE for Data Mover Users is configurable by an Administrator. This security function provides the ability for the TOE to internally identify and authenticate users, and manage their attributes. The TOE can also utilize an external authentication server to identify users.

Data Mover Users accessing SMB and NFSv4 filesystems may identified & authenticated by the TOE or in the TOE environment. For local user access, the TOE will validate the username and password with each request for access. If configured for local administration of Data Mover Users, the TOE will refer to its list of authorized users and groups. If the user can be authenticated, the function will allow the user access to the CIFS or SMB server shares. Access to individual files and directories is then governed by the User Data Protection security function using UserID, GroupID, and Access Control List as described in Section 7.1.3.1. In the evaluated configuration, the TOE is configured to use Active Directory. In this scenario, the TOE will communicate with the Active Directory server in the TOE environment using the Kerberos protocol to validate the user identity and retrieve a list of groups that the user is a member of. The authentication result is then accepted by the TOE.

For NFSv2 and NFSv3 File user access, the external system from which the request is coming (NFS client) has already identified and authenticated each Data Mover User (although this is not part of the evaluated functionality). For this configuration, the TOE relies on its environment to perform proper identification and authentication. The TOE also relies on the environment to provide a list of GroupIDs that have been assigned to the user.

Identification of client machines connecting to the TOE to access LUNs is provided by the TOE Environment through the proper assignment and use of WWNs.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.2, FIA_UID.2.

7.1.5 Security Management

Unisphere Administrators are primarily responsible for managing and configuring system objects. This includes managing the use of LUNs provided by the storage system, grouping those LUNs into useful storage groups called Volumes, and creating and managing individual file systems on those Volumes. The Administrator also manages individual Data Movers, creates and manages file servers, and maps shares on those file servers to configured file systems. The Administrator is responsible for configuring the access control mechanisms to be supported by each file server.

The TOE provides mechanisms to govern which client machines can access which LUNs. The Security Management function allows Administrators to properly configure this functionality.

Administrators of the TOE are assigned one of the ten roles described in Table 11 above.

TOE Security Functional Requirements Satisfied: FMT_MSA.1a, FMT_MSA.1b, FMT_MSA.3a, FMT_MSA.3b, FMT_MTD.1a, FMT_MTD.1b, FMT_MTD.1c, FMT_SMF.1, FMT_SMR.1.

7.1.6 Protection of the TSF

The TOE leverages a NTP service to ensure consistent time stamps across the TOE. A hardware clock on the Control Station, Data Mover, and Storage Processor is used to set this time. The clock may only be set by an authorized administrator.

TOE Security Functional Requirements Satisfied:FPT_STM.1.

7.1.7 Trusted Path/Channels

The Control Station is the main management component for the file-side components of the storage system. The main function of the Control Station is to support the Unisphere GUI and Navisphere CLI interfaces, which allow configuration and management of the system. The HTTPS secure protocol creates a trusted path to access these applications on the Control Station appliance.

TOE Security Functional Requirements Satisfied: FTP_TRP.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 revision 4.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 14 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.DATA_CORRUPTION Data could become corrupted due to hardware failure or incorrect system access by users of the TOE or attackers.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT counters this threat by providing mechanisms to protect the data that has been entrusted to the TOE.
T.IMPROPER_SERVER A system connected to the TOE could access data that it was not intended to gain access by bypassing the protection mechanisms of the TOE.	OE.SECURE_COMMUNICATIONS The TOE Environment must provide secure communications between systems connected to the Storage Area Network.	OE.SECURE_COMMUNICATIONS counters this threat by ensuring that all communications with the TOE are secure for administration of the TOE, internal TOE communications, and data sent to or from the TOE.
	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	OE.SECURE_MGMT_COMMUNICATIONS The TOE Environment must provide secure communications between systems connected to the Management LAN.	OE.SECURE_MGMT_COMMUNICATIONS counters this threat by ensuring that all management communications with the TOE are secure for management of the TOE.

Threats	Objectives	Rationale
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT counters this threat by providing adequate mechanisms to give only authorized servers access to the appropriately authorized data.
	OE.SECURE_SERVERS The TOE Environment must provide properly configured authentication servers and client machines to communicate with the TOE.	OE.SECURE_SERVERS counters this threat by ensuring that each server connected to the storage area network operates properly and does not intentionally compromise data.
	OE.PROPER_NAME_ASSIGNMENT The TOE Environment must provide accurate World Wide Names for each system that communicates with the TOE.	OE.PROPER_NAME_ASSIGNMENT counters this threat by ensuring that the World Wide Names provided to the TOE are accurate. This allows the mechanisms provided by O.PROTECT to properly protect data.
T.IMPROPER_CONFIG The TOE could be misconfigured by an administrator to provide improper storage or enforce improper access to user data.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.
	O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.	O.I&A counters this threat by ensuring that all authorized administrators are properly identified and authenticated.
T.MEDIATE_ACCESS Access to user data could be improperly granted by an administrator to users who should not have access to it.	OE.I&A The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.	O.I&A and OE.I&A (depending on TOE configuration) work together to counter this threat by ensuring that the TOE or the TOE environment has properly identified and authenticated a user prior to providing access to user data.
	OE.SECURE_COMMUNICATIONS The TOE Environment must provide secure communications between systems connected to the Storage Area Network.	OE.SECURE_COMMUNICATIONS counters this threat by ensuring that identification and authentication performed by the TOE Environment is done over a secure communications channel.
	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.

Threats	Objectives	Rationale
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT counters this threat by providing mechanisms to protect the data that has been entrusted to the TOE.
	OE.SECURE_SERVERS The TOE Environment must provide properly configured authentication servers and client machines to communicate with the TOE.	OE.SECURE_SERVERS counters this threat by ensuring that the servers that communicate with the TOE on behalf of a user are managed securely.
	O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.	O.I&A and OE.I&A (depending on TOE configuration) work together to counter this threat by ensuring that the TOE or the TOE environment have properly identified and authenticated a user prior to providing access to user data.
T.UNAUTH An unauthorized user could access data stored by the TOE by bypassing the protection mechanisms of the TOE.	O.AUDIT The TOE must record audit records for data accesses and use of the TOE functions on the management system.	O.AUDIT counters this threat by ensuring that the TOE tracks all management actions taken against the TOE.
	OE.I&A The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.	O.I&A and OE.I&A (depending on TOE configuration) work together to counter this threat by ensuring that the TOE or the TOE Environment has properly identified and authenticated a user prior to providing access to user data.
	O.AUDIT_REVIEW The TOE must provide authorized administrators with the ability to review the audit trail.	O.AUDIT_REVIEW counters this threat by ensuring that administrators can review the audited changes to the TOE configuration.
	OE.SECURE_COMMUNICATIONS The TOE Environment must provide secure communications between systems connected to the Storage Area Network.	OE.SECURE_COMMUNICATIONS counters this threat by ensuring that identification and authentication performed by the TOE Environment is done over a secure communications channel.
	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN counters this threat by allowing an administrator to properly configure the mechanisms of the TOE.

Threats	Objectives	Rationale
	O.PROTECT The TOE must protect data that it has been entrusted to protect.	O.PROTECT counters this threat by providing mechanisms to protect the data that has been entrusted to the TOE.
	OE.SECURE_SERVERS The TOE Environment must provide properly configured authentication servers and client machines to communicate with the TOE.	OE.SECURE_SERVERS counters this threat by ensuring that the servers that communicate with the TOE on behalf of a user are managed securely. Depending upon the access mechanism chosen, the TOE may depend upon these servers for identification and authentication of users.
	O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.	O.I&A and OE.I&A (depending on TOE configuration) work together to counter this threat by ensuring that the TOE or the TOE Environment has properly identified and authenticated a user prior to providing access to user data.
T.CRYPTO An attacker could attempt to exploit a weakness in a cryptographic algorithm to gain access to management communications.	O.CRYPTO The TOE must be able to enforce FIPS validated algorithms to protect management communications.	O.CRYPTO ensures that users accessing the TOE are validated using FIPS 140-2 validated algorithms or modules.
T.ACCESS An attacker could attempt to gain access to the TOE by accessing the physical network and attempting to sniff data transmitted.	O.ACCESS There must be a secure path for communication between users and the TOE.	O.ACCESS ensures that users are authenticated through a secure channel when accessing the TOE.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no OSPs defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 15 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	NOE.MANAGE Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.	NOE.MANAGE upholds this assumption by ensuring that those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use.
A.NOEVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	NOE.NOEVIL Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained, and follow all administrator guidance.	NOE.NOEVIL upholds this assumption by ensuring that administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.PHYSICAL Physical security will be provided for the TOE and its environment.	NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	NOE.PHYSICAL upholds this assumption by ensuring that physical security is provided within the domain for the value of the IT resources protected by the operating system and the value of the stored, processed, and transmitted information.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable time stamps to the TOE.	OE.TIME upholds this assumption by ensuring that the environment provides reliable time stamps to the TOE.
A.I&A The TOE environment will provide identification and authentication of Application Server users before allowing any other TSF-mediated actions on behalf of those users.	OE.I&A The TOE Environment will uniquely identify users and will authenticate the claimed identity when requested to do so by the TOE.	OE.I&A upholds this assumption by ensuring that the environment provides identification and authentication of client machine users.
A.PRIVATE The IT environment will be configured in such a way as to ensure secure and private transmission of TOE management traffic on a separate LAN.	OE.SECURE_MGMT_COMMUNICATIONS The TOE Environment must provide secure communications between systems connected to the Management LAN.	OE.SECURE_MGMT_COMMUNICATIONS upholds this assumption by ensuring the environment provides a separate LAN for TOE management traffic.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no extended functional requirements defined for this TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended assurance requirements defined for this TOE.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 16 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must record audit records for data accesses and use of the TOE functions on the management system.	FAU_GEN.1 Audit data generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security-related events, including relevant details about the event.
O.AUDIT_REVIEW The TOE must provide authorized administrators with the ability to review the audit trail.	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review the audit trail.
O.ADMIN The TOE must provide a method for administrative control of the TOE.	FIA_UAU.2 User authentication before any action	This SFR supports O.ADMIN by ensuring that the TOE shall successfully authenticate each administrator before allowing management of the TOE.
	FIA_UID.2 User identification before any action	This SFR supports O.ADMIN by ensuring that the TOE will properly identify and authenticate all administrators.
	FMT_MSA.1a Management of security attributes	This SFR supports O.ADMIN by ensuring that security attributes of the TOE can only be changed by authorized administrators.
	FMT_MSA.1b Management of security attributes	This SFR supports O.ADMIN by ensuring that security attributes of

Objective	Requirements Addressing the Objective	Rationale
		the TOE can only be changed by authorized administrators.
	FMT_MSA.3a Static attribute initialization	This SFR supports O.ADMIN by ensuring that permissive values for data access are provided and the TOE administrator can change them when a data object is created.
	FMT_MSA.3b Static attribute initialization	This SFR supports O.ADMIN by ensuring that restrictive values for data access are provided, and the Object Owner can change them when a data object is created.
	FMT_MTD.1a Management of TSF data	This SFR supports O.ADMIN by ensuring that the ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_MTD.1b Management of TSF data	This SFR supports O.ADMIN by ensuring that the ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_MTD.1c Management of TSF data	This SFR supports O.ADMIN by ensuring that the ability to modify TSF data is granted only to certain roles managed by the TOE.
	FMT_SMF.1 Specification of management functions	This SFR supports O.ADMIN by ensuring that each of the management functions are utilized to securely manage the TOE.
	FMT_SMR.1 Security roles	This SFR supports O.ADMIN by ensuring that specific roles are defined to govern management of the TOE.
O.PROTECT The TOE must protect data that it has been entrusted to protect.	FDP_ACC.1a Subset access control	This SFR supports O.PROTECT by ensuring that the TOE has an access control policy that ensures that only authorized servers can gain access to data within the TOE.
	FDP_ACC.1b Subset access control	This SFR supports O.PROTECT by ensuring that the TOE provides access control functionality to manage access to data protected by the TOE.

Objective	Requirements Addressing the Objective	Rationale
	FDP_ACF.1a Security attribute based access control	This SFR supports O.PROTECT by ensuring that the TOE provides access control functionality to manage access to data within the TOE.
	FDP_ACF.1b Security attribute based access control	This SFR supports O.PROTECT by ensuring that the TOE has an access control policy which ensures that only authorized users gain access to data protected by the TOE.
	FDP_SDI.2 Stored data integrity	This SFR supports O.PROTECT by ensuring that the TOE protects the stored user data from integrity errors.
	FPT_STM.1 Time stamps	This SFR supports O.PROTECT by ensuring an accurate time stamp across all components of the TOE.
O.I&A The TOE will uniquely identify users and will authenticate the claimed identity before granting a user access to the TSFs when local authentication is required.	FIA_ATD.1 User attribute definition	This SFR supports O.I&A by ensuring that the TOE, when configured for local user administration, maintains security attributes for each user.
	FIA_UAU.2 User authentication before any action	This SFR supports O.I&A by ensuring that the TOE authenticates each Administrator, and when configured for local user administration each user, prior to granting access to the TSF.
	FIA_UID.2 User identification before any action	This SFR supports O.I&A by ensuring that the TOE identifies each Administrator and when configured for local user administration, each user prior to granting access to the TSF>
O.CRYPTO The TOE must be able to enforce FIPS validated algorithms to protect management communications.	FCS_CKM.1 Cryptographic key generation	This SFR supports O.CRYPTO by ensuring the TOE uses secure cryptographic algorithms to protect management traffic.
	FCS_CKM.4 Cryptographic key destruction	This SFR supports O.CRYPTO by ensuring the TOE zeroizes cryptographic keys to prevent their compromise.

Objective	Requirements Addressing the Objective	Rationale
	FCS_COP.1 Cryptographic operation	This SFR supports O.CRYPTO by ensuring the TOE performs cryptographic operations in accordance with the FIPS 140-2 standard.
O.ACCESS There must be a secure path for communication between users and the TOE.	FTP_TRP.1 Trusted path	This SFR supports O.ACCESS by ensuring users access the TOE through a secure communication path.

8.5.2 Security Assurance Requirements Rationale

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

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Rationale for Refinements of Security Functional Requirements

The following refinements of SFRs from CC version 3.1 have been made to clarify the content of the SFRs, and make them easier to read:

The words "no additional rules" were added and others stricken, to FDP_ACF.1a.

The word "objects" was changed to "user data" to specify more precisely what is protected with FDP_SDI.2.

8.5.4 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 17 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 17 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_COP.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FDP_ACC.1a	FDP_ACF.1a	✓	
FDP_ACC.1b	FDP_ACF.1b	✓	
FDP_ACF.1a	FMT_MSA.3a	✓	
	FDP_ACC.1a	✓	
FDP_ACF.1b	FDP_ACC.1b	✓	
	FMT_MSA.3b	✓	
FDP_SDI.2	None	Not applicable	
FIA_ATD.1	None	Not applicable	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not claimed, FIA_UID.2 is claimed and is hierarchical to FIA_UID.1.
FIA_UID.2	None	Not applicable	
FMT_MSA.1a	FMT_SMR.1	✓	
	FDP_ACC.1a	✓	
	FMT_SMF.1	✓	
FMT_MSA.1b	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
	FDP_ACC.1b	✓	
FMT_MSA.3a	FMT_SMR.1	✓	
	FMT_MSA.1a	✓	
FMT_MSA.3b	FMT_MSA.1b	✓	
	FMT_SMR.1	✓	
FMT_MTD.1a	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1b	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1c	FMT_SMF.1	✓	
	FMT_SMR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FMT_SMF.1	None	Not applicable	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not claimed, FIA_UID.2 is claimed and is hierarchical to FIA_UID.1.
FPT_STM.1	No dependencies		
FTP_TRP.1	No dependencies		

9 Acronyms

This section describes the acronyms.

9.1 Acronyms

Table 18 – Acronyms and Terms

Acronym	Definition
ACE	Access Control Entry
ACL	Access Control List
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
CIFS	Common Internet File System
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CIM	Common Information Model
DART	Data Access in Real Time
DAE	Disk Array Enclosure
DES	Data Encryption Standard
DNS	Domain Name System
DOS	Disk Operating System
DPE	Disk-processor Enclosure
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
FC	Fibre Channel
FCoE	Fibre Channel over Ethernet
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol

Acronym	Definition
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IP	Internet Protocol
IQN	iSCSI Qualified Name
iSCSI	Internet Small Computer System Interface
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit
MA	Rivest, Shamir, Adleman
MD	Message Digest
ME	Micro Edition
MPFS	Multi Path File System
MS	Microsoft
NA	Not Applicable
NAS	Network Attached Storage
NFS	Network File System
NIST	National Institute of Standards and Technology
NL-SAS	Nearline Serial Attached SCSI
NTP	Network Time Protocol
OE	Operating Environment
OSP	Organizational Security Policy
OSSI	Open Source Software Institute
PKCS	Public Key Cryptography Standard
PP	Protection Profile
PRNG	Pseudorandom Number Generator
PSS	Probabilistic Signature Scheme
RAID	Redundant Array of Independent Disks
RSA	Rivest, Shamir, Adleman
SAN	Storage Area Network
SAR	Security Assurance Requirement
SAS	Serial Attached SCSI

Acronym	Definition
SCSI	Small Computer System Interface
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMB	Server Message Block
SNMP	Simple Management Network Protocol
SOE	Storage Operating Environment
SP	Storage Processor
SPE	Storage-processor Enclosure
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
UQM	Unisphere Quality of Service Manager
UTF	Unicode Transformation Format
WWN	World Wide Name

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
Email: info@corsec.com
http://www.corsec.com