EMC® Corporation

EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.2

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

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table of Figures

List of Tables

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware, and may be referred to as the TOE or "VNXe" throughout the remainder of this document. The TOE contains a combination File (IP[1]) and Block (iSCSI[2] over IP, and FC[3]) operating environment with Unified Management (Unisphere). The TOE provides storage and access controls for block services over IP and FC and standard IP-based file sharing 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 functionality 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), 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 Security 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 below shows the ST and TOE references.

Table 1 ST and TOE References

ST Title	EMC® Corporation EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware Security Target
ST Version	Version 1.2
ST Author	Corsec Security, Inc.
ST Publication Date	2015-07-08

[1] IP – Internet Protocol

[2] iSCSI – Internet Small Computer Systems Interface

[3] FC – Fibre Channel

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

ST Title	EMC® Corporation EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware Security Target
TOE Reference	**TOE Software:** EMC VNXe OE v3.1.1.5395470 EMC VNXe Unisphere v3.1.1.5395470 EMC VNXe Unisphere CLI[4] v3.0.0.1.16 **TOE Hardware:** EMC VNXe3200 DPE[5] V32D12AN2 P/N 100-542-455-11 EMC VNXe3200 DPE V32D12AN5QS25 P/N 100-542-441-01 EMC VNXe3200 DAE[6] V32-DAE-12 P/N 100-542-104-01 EMC VNXe3200 DAE V32-DAE-25 P/N 100-563-628 **Disk Drives:** EMC KSHWXG8J SAS[7] P/N 005049804PWR EMC SS162511 CLAR100 EFD[8] P/N 5050500 EMC Z1X1972R NL-SAS P/N 005050143PWR

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.

Figure 1 VNXe System

VNXe/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, hosts[9] connect to VNXe/Unisphere over an IP-based network through standard IP-based networking equipment (routers and switches as needed) or through a typical SAN architecture using FC equipment. These hosts are then configured to use storage on VNXe3200 hardware in the form of Logical Units or file systems for their applications.

VNXe includes the VNXe Operating Environment v3.1.1, which provides RAID[10] and storage capabilities. The product provides the ability to combine several individual drives into useful logical groups, provides

[4] CLI – Command Line Interface
[5] DPE – Disk Processor Enclosure
[6] DAE – Disk Array Enclosure
[7] SAS – Serial-Attached SCSI
[8] EFD – Enterprise Flash Drive
[9] Host – a host is a term used to generically define systems accessing storage on the TOE, whether that acces is Block-based access or File-based access
[10] RAID – Redundant Array of Independent Disks

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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.

VNXe Operating Environment v3.1.1 software includes the Unisphere management software that allows administrators to manage and configure the VNXe. The VNXe3200 is the hardware platform, which includes back-end disk arrays. Together these components provide three main features:

- Block services (iSCSI over IP, and FC)
- File services (Network File System (NFS) and Common Internet File System (CIFS)[11])
- A unified management suite that allows administrators to configure all parts of the VNXe from a single management console.

VNXe users access storage through traditional IP-based block and file protocols. VNXe can present itself as one or more standard network-based file servers to IP-based client machines (as a NAS[12]), or as a block storage device to application servers with iSCSI and FC. Administrators manage VNXe and control the policies that govern access to storage with VNXe Operating Environment v3.1.1 software.

The product runs Unified[13] Block and File protocols, allowing the product to provide and control access to storage from both IP-connected clients and clients connecting via FC.

CSX[14] implements the File and Block functionality. CSX is an execution environment built on a Linux kernel that processes and performs the actual transfer of data between the back-end disk drives and clients. Each CSX process provided by VNXe can host one or more "virtual servers" that present shared services to IP-based and FC-based hosts. Protocols that VNXe supports include:

- CIFS[15] versions 2 and 3
- NFS[16] versions 2 and 3
- iSCSI
- FC

Administrators can configure the type of protocols that are supported for that server per process. IP-connected hosts, with the appropriate access privileges, can then use VNXe to store and access data.

VNXe is responsible for enforcing all access permissions for user data. Each File-based "virtual server" on VNXe can be configured to interface with an LDAPv3-compatible or Network Information Service (NIS) server. When a request for data access is made from a File-based client machine, VNXe utilizes the LDAPv3-compatible server or NIS server for authentication, checks the Access Control List (ACL) of the requested file or directory, and either grants or denies access to the user. User data is stored directly on storage provided by VNXe3200.

The VNXe3200 platform includes disk drives and other hardware to run the system (such as memory and processor). The VNXe hardware offers options to choose the capacity and performance of storage by customizing the number and capacity of SSD, NL-SAS[17], and SAS[18] disks in the system.

The disk storage is configured to provide a storage system for use by VNXe users. The block storage portion of VNXe allows this storage system to store and retrieve block units of data for VNXe users. Each

[11] CIFS is the Microsoft implementation of System Message Block (SMB)
[12] NAS – Network Attached Storage
[13] Unified refers to both Block and File storage functionality being present on the same storage system.
[14] CSX – Common Software eXecution
[15] CIFS is a platform-independent file sharing system commonly used by Microsoft Windows network file sharing
[16] NFS is a platform-independent file sharing system commonly used by UNIX and UNIX variants for file sharing
[17] NL SAS – Near Line Serial Attached Small Computer System Interface (SCSI)
[18] SAS – Serial Attached SCSI

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 VNXe as Logical Units. Each Logical Unit is a useable storage system volume that VNXe can expose to the user.

The VNXe Operating Environment v3.1.1 software contains utilities and a user interface for installing and configuring VNXe, maintaining the system, and monitoring system performance.

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 product, and defining the specific evaluated configuration.

The hardware and software TOE is the EMC VNXe™ OE v3.1.1 with Unisphere and VNXe3200™ Hardware. The TOE is a mid-to-high capacity storage system. The VNXe Operating Environment v3.1.1 provides RAID and virtual storage capabilities, one or more NAS servers that allow IP-based clients to connect and use storage, an interface by which the TOE provides access controls for storage under management by VNXe. The VNXe3200 includes the hardware needed to access and provide storage and the disk storage itself.

The TOE is managed by authorized users through the UEMCLI[19] and the Unisphere GUI[20] interfaces. Unisphere GUI is an Adobe Flex application that runs within a web browser. To access the functions available via Unisphere GUI, an authorized user must open a web browser and enter the IP address or hostname of the VNXe management port. UEMCLI is a command line interface that provides access to common functions for monitoring and managing the TOE. The UEMCLI provides access to functions for storage provisioning, status and configuration information retrieval, and other TOE administrative functions. UEMCLI commands can also be used to automate management functions via shell scripts and batch files.

The TOE software provides RAID storage architectures, fault detection, isolation, and diagnosis capabilities. It enables the use of virtual storage elements (LUNs) to improve performance and capacity utilization.

The TOE provides NAS services that allow hosts on an IP network to access file systems via one of the supported file-based protocols (CIFS and NFS). 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 TOE access controls before the TOE allows the access to occur. The TOE provides Storage Area Network (SAN) services that allow hosts to access storage as Logical Units via iSCSI or FC.

The TOE also performs identification and authorization of TOE Administrators, and Users; discovery and monitoring of File-side and Block-side components; storage configuration and allocation; status and configuration information display; and event management. The TOE hardware provides the physical storage and processing resources necessary for the TOE to function.

Figure 2 shows the details of the deployment configuration of the TOE:

[19] UEMCLI – Unified Element Manager Command Line Interface

[20] GUI – Graphical User Interface

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

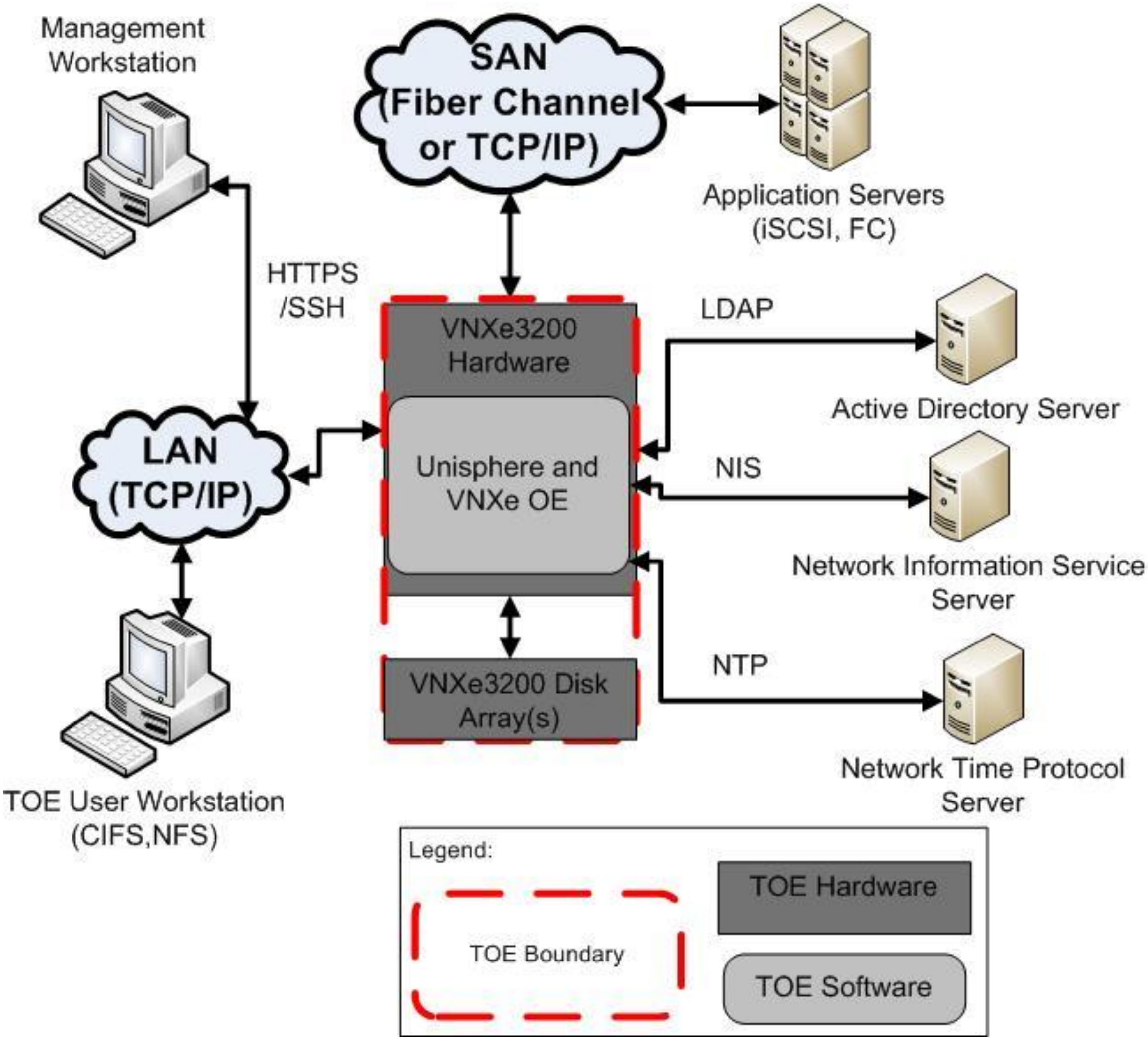

Figure 2 Deployment Configuration of the TOE

In the diagram above, Application Servers are shown to make use of the block protocols in order to access storage on the TOE. This is because users typically access storage via the file protocols. Application Servers, which can include any type of applications requiring the use of storage (such as database servers, web servers, trouble-ticket systems, custom applications, and more), typically use block protocols to store and retrieve data requested by users.

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 and File Systems

A central concept of the TOE is an abstraction called a Logical Unit. The TOE presents storage to hosts on the IP network in the form of Logical Units and File Systems. The TOE software provides for the management of Logical Units and File Systems. Each Logical Unit represents a unit of storage to a host, 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.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Each LUN can then be mounted by hosts. When this mechanism is used, a host can only access LUNs that the host has been permitted to access. It is also possible that multiple hosts are given access to the same LUNs. This is used in cases where the host has been deployed in such a way as to manage multiple servers accessing the same LUN, for example, in a clustered environment.

1.4.1.2 Storage Processors (SPs)

The SP hardware (with VNXe3200 Operating Environment v3.1.1 software) is responsible for interfacing with the front-end IP-based clients and the back-end disks within the VNXe3200. The SP provides administrators with the ability to manage the TOE and establish Logical Units and RAID Groups.

1.4.1.3 Disk Array Enclosures (DAEs)

The DAE hardware houses the disks in the storage array and provides connectivity to users attempting to access storage or stored data. The VNXe3200 storage system supports up to 150 drives on 25-disk 2.5" (SSD and SAS) enclosures or 12-disk 3.5" (SAS and NL SAS) enclosures[21].

1.4.1.4 Disk Processor Enclosure (DPE)

The DPE houses two SPs and can hold up to 25 2.5" SSD drives and SAS or 12 3.5" SAS and NL SAS drives.

1.4.1.5 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.

1.4.1.6 Unisphere

Unisphere is the Adobe Flex GUI used to manage the TOE. Administrators must log into Unisphere in order to manage the TOE or the policies that control user access. 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.

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 an IP network with the constituent servers managed by administrators operating under a consistent security policy with the administrators that manage the TOE. Management workstations need to meet the following requirements to run UEMCLI and Unisphere:

1.4.2.1 Unisphere CLI (UEMCLI)

- 32-bit Windows

1.4.2.2 Unisphere

- Adobe Flash Player v11
- Mozilla Firefox v28

The TOE relies on secure access provided by the network to which it is attached. The purpose of the TOE is to mediate access to user data for File-based users and Block-based application servers connected to an IP or FC network. Hosts connecting to the TOE to access storage must use CIFS, NFS, iSCSI, or FC.

[21] For a list of supported disk drives, please refer to *EMC VNXe Series Storage Systems Disk and OE Matrix*, available at https://support.emc.com/products/30951_VNXe3200/Documentation/.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

An LDAPv3-compliant Microsoft Active Directory Domain Controller is included within the TOE Environment in order to provide remote password-based authentication for the TOE for administrators and CIFS File-based users. A NIS Server is also included within the TOE environment for remote password-based authentication to the TOE for NFS File-based users. A Network Time Protocol Server is included within the TOE Environment in order to synchronize the system time of the TOE with the rest of the deployment environment.

1.5 TOE Description

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

1.5.1 Physical Scope

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

The essential physical components for the proper operation of the TOE in its minimal configuration are:

- **TOE:**
  - **Software:**
    - EMC VNXe Operating Environment v3.1.1 software (includes EMC VNXe Unisphere)
    - EMC VNXe Unisphere CLI (UEMCLI) v3.0
  - **Hardware:**
    - EMC VNXe3200 DPE – includes two SPs
    - EMC VNXe3200 DAE
    - EMC EFD and SAS disk drives
- **TOE Environment:**
  - Management workstation used to access the Unisphere GUI via a web browser or the UEMCLI (the workstation and web browser are not included within the TOE boundary)
  - LDAPv3-compatible Server (Active Directory)
  - NTP Server (Active Directory)
  - NIS Server
  - Application Servers accessing Block storage
  - Client Systems accessing File storage

1.5.1.1 Guidance Documentation

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

- EMC Unisphere for VNXe Online Help
- EMC VNXe Unisphere CLI[22] User Guide
- EMC VNXe Security Configuration Guide
- EMC VNXe Series Quick Start
- EMC VNXe Series Using a VNXe3200 System with Fibre Channel or iSCSI LUNs
- EMC VNXe Series Using a VNXe3200 System with NFS File Systems
- EMC VNXe Series Using a VNXe3200 System with CIFS File Systems
- EMC VNXe3200 Operating Environment v3.1.1.5395470 Release Notes
- VNXe Series VNXe3200 Hardware Information Guide
- EMC VNXe3200 Installation Guide

[22] CLI – Command Line Interface

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management

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 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. This functionality is primarily enforced by the storage management processes in the TOE. File-based users accessing the TOE are identified and authenticated by the TOE Environment. The TOE verifies that the identification and authentication is successful before granting these users 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 users of the TOE to that object. Files are accessed via CIFS and NFS.

The TOE protects user data primarily in two additional ways. First, it ensures that only the users or application servers that have been granted access to LUNs have access to those LUNs. 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 verify the successful identification and authentication of each administrator of the TOE and each File-based TOE user. (both user and administrator I&A are performed by the TOE environment). In the case of Unisphere administrators, the TOE provides username and password verification functionality via a remote LDAPv3-compatible server. Administrators are assigned a role to determine what aspects of the TOE they are allowed to manage. This functionality is configured by an Administrator. File users (CIFS or NFS) are also authenticated via a remote LDAPv3-compatible server or NIS server.

1.5.2.4 Security Management

The Security Management functionality of the TOE specifies several aspects of management of the TOE Security Functionality (TSF). Proper management of the TSF is required to properly mediate access to the storage that the TOE provides.

The TOE is managed by authorized users through the Unisphere GUI and the UEMCLI. Unisphere GUI is an Adobe Flex application that runs within a web browser. UEMCLI is a command line interface that provides access to common functions for monitoring and managing the TOE.

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

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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:

- Event Enabler
- REST interface
- SMI-S interface
- VASA interface
- File-level retention
- Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP) notification functionality

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2 Conformance Claims

This section and Table 2 provide 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 2 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2014-12-11 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Reporting Procedures (ALC_FLR.2)

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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[23] 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[24] 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. Table 3 below lists the applicable threats.

Table 3 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 to provide improper storage or enforce improper access to user data.
T.MEDIATE_ACCESS	Access to user data could be improperly granted 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.

[23] IT – Information Technology

[24] TSF – TOE Security Functionality

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 Organizational Security Policies defined for this evaluation.

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. Table 4 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 4 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. The TOE is on an internal network and the environment protects against all external access to the operating system.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 listed in Table 5 below.

Table 5 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 verify that users have been uniquely identified and authenticated before granting those users access to the TSFs where authentication is required.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 6 below lists the IT security objectives that are to be satisfied by the environment.

Table 6 IT Security Objectives

Name	Description
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.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4.2.2 Non-IT Security Objectives

Table 7 below lists the non-IT environment security objectives that 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 7 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.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

5 Extended Components

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

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 in parentheses 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 8 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 8 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FDP_ACC.1a	Subset access control		✓		✓
FDP_ACF.1a	Security attribute based access control		✓		✓
FDP_ACC.1b	Subset 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				
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 initialisation	✓	✓		✓

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	S	A	R	I
FMT_MSA.3b	Static attribute initialisation	✓	✓		✓
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		✓		

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

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

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 administrator 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*].

FAU_SAR.1 Audit review
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [*the Administrator, Storage Administrator, and Operator roles*] 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.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.3 Class FDP: User Data Protection

FDP_ACC.1a Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1a Security attribute based access control

FDP_ACC.1.1a

The TSF shall enforce the [*Block Storage Access Control SFP*[25]] on [

a) Subjects: Hosts (application servers)
b) Objects: LUNs
c) Operations: Read and write

].

Application note: the Subjects are application servers connected to the TOE acting on behalf of an authorized user.

FDP_ACF.1a Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1a Subset access control
FMT_MSA.3a Static attribute initialization

FDP_ACF.1.1a

The TSF shall enforce the [*Block Storage Access Control SFP*] to objects based on the following:
[

Subject attributes:

1. *iSCSI Qualified Name (IQN)*
2. *World Wide Name (WWN)*

Object attributes:

1. *IQN access list*
2. *WWN access list*

].

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 TOE storage if the IQN or WWN of the subject is included in the host list, the subject has been granted access to the LUN, and (for FC) the host list entry is mapped to an initiator with access to the LUN
].

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

FDP_ACC.1b Subset access control
Hierarchical to: No other components.
Dependencies: FDP_ACF.1b Security attribute based access control

FDP_ACC.1.1b

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

a) Subjects: Users (accessing storage from client machines)

[25] SFP – Security Functional Policy

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

b) *Objects: CIFS shares and NFS mounts*
c) *Operations: Read, Write, Execute*

].

Application Note: The CIFS naming convention has been used for operations. NFS v2 and NFS v3 access supports the following subset of commands: Create, Read, Write, Delete, Change Ownership, Read Permissions, Change Permissions, Read Attributes, Write Attributes.

FDP_ACF.1b Security attribute based access control
Hierarchical to: No other components.
Dependencies: FDP_ACC.1b Subset access control
FMT_MSA.3b Static attribute initialization

FDP_ACF.1.1b

The TSF shall enforce the [*File Storage Access Control SFP*] to objects based on the following:

[

Subject attributes:

1. *Username*
2. *Authentication status (success or failure)*
3. *IP address (for NFS access)*

Object attributes:

1. *NFS Mount permissions: Unix-style ACLs for each file and directory (Read, Write, and Execute).*
2. *CIFS Share* permissions*: NT-style DACLs*[26] for each file and directory *(No Access, Full Control, Modify, Read & Execute, List Folder Contents, Read, Write, Special Permissions).*

].

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 (containing permissions) for the object authorizes the Subject to perform the desired operation. A user must be successfully authenticated by the TOE Environment in order to be associated with the permissions and privileges configured for that user*].

FDP_ACF.1.3b

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

[

1. *For CIFS access subjects that are members of the group Domain Administrators shall be authorized to backup, restore, and take ownership of all objects and control over the overall share permissions for the entire domain*
2. *For NFS access, the user must access the NFS mount from a computer running an IP address listed in the allowed hosts configuration for the TOE*
3. *For NFS access, subjects that are authorized as superusers (root) can perform all operations on all objects*
4. *For root users accessing an NFS mount, access will be permitted if the host the root user is using to connect to the NFS mount is listed under the "trusted hosts" list in the TOE configuration.*

].

FDP_ACF.1.4b

The TSF shall explicitly deny access of subjects to objects based on the [*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 Subject to perform the desired operation. A user that has failed authentication is not granted access to any object*].

[26] DACL – Discretionary Access Control List

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies

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 5 and RAID 6; mirrored data for RAID 1+0*].

FDP_SDI.2.2

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

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.4 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
Dependencies: No dependencies

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual **Administrators** ~~users~~: [*role*].

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

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.

User Authentication applies to users accessing File-based storage on the TOE as well as administrators accessing management functionality via the management interfaces.

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

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.

User Identification applies to users accessing File-based storage on the TOE as well as administrators accessing management functionality via the management interfaces.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.5 Class FMT: Security Management

FMT_MSA.1a Management of security attributes
Hierarchical to: No other components.
Dependencies: FDP_ACC.1a Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1a

The TSF shall enforce the [*Block Storage Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*WWN and IQN access lists*] to [*the Administrator and Storage Administrator roles*].

Application Note: The Block Storage Access Control SFP does not actually control access to the security attributes; rather, these attributes are used in the enforcement of the Block Storage Access Control SFP and are restricted by role-based access control.

FMT_MSA.1b Management of security attributes
Hierarchical to: No other components.
Dependencies: FDP_ACC.1b Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1b

The TSF shall enforce the [*File Storage Access Control SFP*] to restrict the ability to [modify, delete, [*add*]] the security attributes [*the attributes listed under "Attributes" in Table 9*] to [*the roles listed under "Role/permissions required" in Table 9*].

Table 9 File Storage Access Control SFP Management

Access type	Attributes	Role/permissions required
CIFS share	Domain Administrator	Administrator or Storage Administrator
NFS mount	Host and Trusted Host access lists (IP addresses for each allowed system)	Administrator or Storage Administrator
CIFS file and directory permissions	CIFS file and directory DACLs	CIFS user with Domain Administrator membership, File Owner, or Change Permissions in DACL for the file, directory, or share
NFS file and directory permissions	NFS file and directory ACLs	NFS user with root, File Owner, or Change Permissions in the ACL for the file or directory

Application Note: The File Storage Access Control SFP does not actually control access to the security attributes; rather, these attributes are used in the enforcement of the File Storage Access Control SFP and are restricted by role-based access control.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

FMT_MSA.3a Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1a Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1a

The TSF shall enforce the [*Block Storage Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2a

The TSF shall allow the [*Administrator and Storage Administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3b Static attribute initialization

Hierarchical to: No other components.
Dependencies: FMT_MSA.1b Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1b

The TSF shall enforce the [*File Storage 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.

FMT_MTD.1a Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1a

The TSF shall restrict the ability to [query] the [*all administrative information for the TOE*] to [*the Administrator, Storage Administrator, and Operator roles*].

FMT_MTD.1b Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1b

The TSF shall restrict the ability to [modify, delete, [*create*]] the [*LUNs and RAID Groups*] to [*the Administrator and Storage Administrator roles*].

FMT_MTD.1c Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1c

The TSF shall restrict the ability to [modify, delete, [*create*]] the [*user accounts*] to [*the Administrator Role*].

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No Dependencies

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:
[

a) Management of Block Storage Access Control SFP attributes
b) Management of File Storage Access Control SFP attributes
c) Viewing administrative information

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

d) Manage storage
e) Manage users

].

FMT_SMR.1 Security roles

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [*the authorized roles identified in Table 10*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Table 10 Authorized Roles

Role	Description
Operator	Can only perform monitoring activities in Unisphere. Read-only access.
Storage Administrator	Can configure Unisphere and provision and reclaim storage.
Administrator	All administration capabilities.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.6 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 11 Assurance Requirements summarizes the requirements.

Table 11 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 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

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7 TOE Security 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 Functionality

Each of the security requirements and the associated descriptions correspond to security functionality. Hence, the security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 12 lists the security functionality and their associated SFRs.

Table 12 Mapping of TOE Security Functionality 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_ACF.1a	Security attribute based access control
	FDP_ACC.1b	Subset 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 initialisation
	FMT_MSA.3b	Static attribute initialisation
	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

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 User Data Protection

This section describes the various User Data Protection SFRs claimed.

7.1.2.1 File Storage Access Control SFP

The TOE enforces the File Storage Access Control SFP[27] on each user of the TOE based on the security attributes of that user. The TOE supports three different user types: File Users, who are controlled by the File Access Control SFP, Block Users, who are controlled by the Block Access SFP, and administrators who are constrained as described by the Security Management functionality. File Users are any users accessing data or storage on the TOE via one of the file protocols (CIFS or NFS). Block Users are any users accessing data or storage on the TOE via one of the block protocols (iSCSI, or FC) from a client machine. Block users are typically application servers and not actual human users. Administrators are any users accessing one of the management interfaces for the TOE.

File Storage Access Control SFP*:* All access to storage is performed via a CIFS or NFS client on behalf of the user. These clients are basic pieces of software (such as the CIFS client within Windows Explorer) used to map and access file-based storage. The TOE enforces the File Storage Access Control SFP on users connecting to the storage on the TOE for NFS and CIFS. After successful authentication for NFS users, the TOE checks user permissions for each file or directory's ACL on each user's access request to determine if the user has appropriate permissions to access the files or directories. After successful authentication for CIFS users, the TOE checks user permissions for each file or directory's DACL on each user's access request to determine if the user has appropriate permissions to access the files or directories. The ability to connect to an NFS mount or CIFS share is granted to users by Administrators or Storage Administrators. Users are associated with CIFS shares via an access list, while a list of IP addresses is associated with NFS mounts as an access list.

Individual file and directory access control management is granted to CIFS users with File Owner or Change Permissions set in the DACL for the user. NFS users with the root role can modify permissions for all files and directories, or users with the File Owner or Change Permissions for any given file or directory can manage access controls for those particular files and directories.

A Linux/Unix host can mount to the VNXe hosted NFS Shared Folder Server if the host has been explicitly authorized to the NFS Shared Folder Server. Similarly, a Windows user can map to the VNXe hosted CIFS Shared Folder Server if the user has been explicitly authorized to the CIFS Shared Folder.

The export of a CIFS Shared Folder Server is based off of the Server Configuration LDAP setting. The VNXe hosted CIFS Shared Folder Server must be in a Windows domain with an LDAPv3-compatible server set up. A Windows client machine can map to the share only if it is a member of the defined domain. For CIFS access, subjects that are members of the group Domain Administrators shall be authorized to backup, restore, and take ownership of all objects.

[27] SFP – Security Functional Policy

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Client machine access to the VNXe hosted NFS Shared Folder Server can be configured based on IP address or network host name, IP subnet range, or a Netgroup. For the NFS access protocol, users connecting to TOE storage who are *superusers* can perform all operations on all objects. Clients must be recognized as "trusted" by the system in order to submit a root request, otherwise it will be mapped to the "nobody" role.

Each file and directory has an ACL associated with it. Each ACL has a set of permissions that are granted or explicitly denied to that user. Whenever a user requests an access to a file or directory, the TOE utilizes its File Storage Access Control SFP (stored with each file and directory) to decide whether or not that access is permitted.

7.1.2.2 Block Storage Access Control SFP

The TOE also provides the User Data Protection security function to manage access from Block-based application servers to configured Logical Units. The purpose of the TOE's storage is to allow high speed, scalable, fault-tolerant storage separate from individual application servers. The TOE provides this functionality to IP-connected hosts.

Using the Security Management security function, Administrators of the TOE can configure Logical Units to provide storage to client machines. LUNs allow Administrators to limit access to one or more specified application servers. When an iSCSI application server requests a list of available LUNs from the TOE, the TOE Environment provides an IQN, or a WWN for FC application servers. This IQN or WWN is used to identify the application servers to the TOE. If the iSCSI application server has a host object created to represent itself on the TOE, the TOE then provides a list of LUNs that the application server has been granted access to. FC is slightly more complicated by requiring the physical adapters to be connected to the application server (either through the SAN fabric or otherwise). Once the host is connected to the proper Host Bus Adapter (HBA), the WWN for the host can be associated with a host object on the TOE as is done with iSCSI. After all of this, each successive request to read or write information to or from a LUN, the TOE ensures that only authorized application servers have access to the LUNs to which they have been given access.

7.1.2.3 RAID

The TOE also provides for the integrity of user data. When creating RAID Groups from individual disk drives, an Administrator can configure RAID levels 1/0, 5, or 6. Each of these 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.

When an integrity error occurs, the TOE notifies the administrator of the error. This notification is an alert that is placed in a log file. Administrators can view alerts via the Alerts page of Unisphere or from the UEMCLI.

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

7.1.3 Identification and Authentication

The TOE environment performs identification and authentication of both Administrators and File-based 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. Both user (File) as well as administrator access to the TOE is covered via the I&A claims. The TOE uses a NIS server or LDAPv3-compatible server in the TOE environment to provide

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

authentication services. Once the username and password has been verified, the TOE uses the message returned from the LDAP or NIS server to assign a role to users and administrators.

7.1.3.1 Administrative I&A

Unisphere Administrators can access the TOE through a web browser or through a command line interface. The TOE supports authentication against Active Directory or an LDAPv3-compatible authentication server. The first action that administrators must take when attempting to interact with the TOE is to provide a username and password. Before identification and authentication, the administrator is not able to access any TOE security functionality.

7.1.3.2 User I&A

Windows environments use an LDAPv3-compatible server or a NIS server for authentication. A Windows host can only map to a CIFS Shared Folder Server if the Windows host is on the same domain as the VNXe, and the Windows domain with an LDAPv3-compatble server is set up.

For NFSv2 and NFSv3, users are authenticated against a NIS server. The server from which the request is coming is identified and authenticated based on the username and password. If the user ID is "root" then the host must also be assigned as a "trusted host" within the TOE configuration.

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

7.1.4 Security Management

Unisphere Administrators are primarily responsible for managing and configuring system objects. This includes managing the use of storage and NFS mount and CIFS share access controls for Block and File. Storage management is primarily the tasks associated with LUNs provided by the storage system, grouping those LUNs into useful groupings called LUN groups. The Administrator creates and manages storage for the TOE, and (for file services) 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 "Storage Resource". All of this, in addition to managing users, user access to LUNs, and managing RAID groups, is accomplished via Unisphere and UEMCLI.

Administrators, storage administrators, and operators may use Unisphere or UEMCLI to query all administrative information on the TOE. This includes all TOE configuration settings, all storage information, and all user accounts on the system. Only users with the administrator role may manage users. User accounts can only be managed via UEMCLI or Unisphere.

Client machines accessing the TOE via CIFS and NFS protocols have restrictive default attributes and are not granted any access to data until the TOE verifies that each user has been identified and authenticated by the LDAPv3-compatible server or NIS server in the TOE Environment. Once authenticated, the user is granted access according to the DACL (CIFS) or ACL (NFS) associated with each file and directory. CIFS and NFS file and directory attributes that can be modified include read, write, and execute permissions. For CIFS users, the user is granted access to the share based on whether they have read and write permissions for the whole share, as granted by a Domain Administrator via a CIFS client (no permissions are set by default). For NFS, the IP address of the system accessing storage must be authorized before any access is allowed. In these ways, access to storage via the File Storage Access Control SFP are restrictive by default.

Unisphere and UEMCLI administrators with the Administrator or Storage Administrator role can modify the NFS access lists and CIFS Domain Administrator attributes. Domain Administrators can modify CIFS share permissions via a CIFS client, and users assigned file owner or change permissions rights for a file can modify the read, write, and execute settings for each file.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Application servers accessing the TOE via block protocols have restrictive default values and are required to be listed in the TOE configuration with a valid WWN or IQN in order access stored data. Additionally, the WWN must be mapped to a valid initiator in order to access the storage for FC.

The TOE provides mechanisms to govern which hosts can access which LUNs. The Security Management function allows Administrators to properly configure this functionality. Additionally, the storage management portion of Unisphere allows administrators to manage the RAID settings for storage, although this can also be managed via UEMCLI.

Administrators of the TOE are assigned one of the roles described in Table 10 above. Section 7.1.2 above describes how the Block and File Access Control SFPs are managed.

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.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Release 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 13 below provides a mapping of the objectives to the threats they counter.

Table 13 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.	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_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.
	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.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

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
		data.
T.IMPROPER_CONFIG The TOE could be misconfigured 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 verify that users have been uniquely identified and authenticated before granting those users access to the TSFs where authentication is required.	O.I&A counters this threat by ensuring that all authorized administrators are properly identified and authenticated by the TOE Environment and that the TOE has verified their successful identification and authentication.
T.MEDIATE_ACCESS Access to user data could be improperly granted to users who should not have access to it.	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_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.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.
	O.I&A The TOE will verify that users have been uniquely identified and authenticated before granting those users access to the TSFs where authentication is required.	O.I&A counters this threat by ensuring that all users have been properly identified and authenticated by the TOE Environment prior to the TOE 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.
	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.
	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_SERVERS	OE.SECURE_SERVERS counters

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
	The TOE Environment must provide properly configured authentication servers and client machines to communicate with the TOE.	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.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.
	O.I&A The TOE will verify that users have been uniquely identified and authenticated before granting those users access to the TSFs where authentication is required.	O.I&A counters this threat by ensuring that users have been properly identified and authenticated by the TOE Environment prior to the TOE providing access to user data.

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 Organizational Security Policies defined for this evaluation.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 14 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 14 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	NOE.PHYSICAL	NOE.PHYSICAL upholds this

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Assumptions	Objectives	Rationale
Physical security will be provided for the TOE and its environment. The TOE is on an internal network and the environment protects against all external access to the operating system.	The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	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.

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 evaluation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended assurance requirements defined for this evaluation.

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 15 below shows a mapping of the objectives and the SFRs that support them.

Table 15 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
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.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
	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 the TOE can only be changed by authorized administrators or users with the appropriate permissions.
	FMT_MSA.3a Static attribute initialisation	This SFR supports O.ADMIN by ensuring that restrictive values for data access are provided and the TOE administrator can change them when a data object is created.
	FMT_MSA.3b Static attribute initialisation	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 query 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.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.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
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.I&A The TOE will verify that users have been uniquely identified and authenticated before granting those users access to the TSFs where authentication is required.	FIA_ATD.1 User attribute definition	This SFR supports O.I&A by ensuring that the TOE maintains security attributes for administrative users.
	FIA_UAU.2 User authentication before any action	This SFR supports O.I&A by ensuring that the TOE verifies the successful authentication of each Administrator and 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 and TOE Environment identify each Administrator and user prior to granting access to the TSF.
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.
	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.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 reporting procedures.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 16 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 16 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Although FPT_STM.1 is not included, the TOE Environment provides reliable timestamps to the TOE. An environmental objective states that the TOE will receive reliable timestamps, thereby satisfying this dependency.
FAU_SAR.1	FAU_GEN.1	✓	
FDP_ACC.1a	FDP_ACF.1a	✓	
FDP_ACF.1a	FDP_ACC.1a	✓	
	FMT_MSA.3a	✓	
FDP_ACC.1b	FDP_ACF.1b	✓	
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.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UID.2	None	Not applicable	
FMT_MSA.1a	FMT_SMR.1	✓	
	FDP_ACC.1a	✓	
	FMT_SMF.1	✓	
FMT_MSA.1b	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1b	✓	
FMT_MSA.3a	FMT_MSA.1a	✓	
	FMT_SMR.1	✓	
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	✓	
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.

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

9 Acronyms

This section and Table 17 define the acronyms used throughout this document.

9.1 Acronyms

Table 17 Acronyms

Acronym	Definition
ACL	Access Control List
API	Application Programming Interface
CC	Common Criteria
CIFS	Common Internet File System
CLI	Command Line Interface
CPU	Central Processing Unit
CSX	Common Software eXecution
DPE	Disk Processor Enclosure
DRAM	Dynamic Random Access Memory
EAL	Evaluation Assurance Level
EFD	Enterprise Flash Drive
FAST	Fully Automated Storage Tiering
FC	Fibre Channel
GUI	Graphical User Interface
HBA	Host Bus Adapter
HDD	Hard Disk Drive
HIPAA	Health Insurance Portability and Accountability Act of 1996
ID	Identifier
IP	Internet Protocol
IQN	iSCSI Qualified Name
iSCSI	Internet Small Computer System Interface
IT	Information Technology
LUN	Logical Unit or Logical Unit Number
MCx	Multicore x
NAS	Network Attached Storage
NFS	Network File System
NIS	Network Information Service

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
NL SAS	Near Line Serial Attached SCSI
OSP	Organizational Security Policy
PP	Protection Profile
RAID	Redundant Array of Independent Disks
REST	Representational State Transfer
SAN	Storage Area Network
SAR	Security Assurance Requirement
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMB	System Message Block
SMI-S	Storage Management Initiative Specification
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOX	Sarbanes-Oxley Act of 2002
SP	Storage Processor
SSD	Solid State Drive
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UEMCLI	Unified Element Manager Command Line Interface
VASA	vStorage APIs for Storage Awareness
VP	Virtual Pool
WWN	World Wide Name

© 2015 EMC® Corporation
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Prepared by:
Corsec Security, Inc.

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

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