EMC Corporation

EMC® Symmetrix® VMAX^{TM} Series with Enginuity^{TM} Operating Environment 5875, Solutions Enabler 7.2.0, and Symmetrix Management Console 7.2.0

Security Target

Evaluation Assurance Level: 2+
Document Version: 0.7

Prepared for:

EMC² where information lives

EMC Corporation
171 South Street
Hopkinton, MA 01748

Phone: (508) 435-1000

http://www.emc.com

Prepared by:

Corsec®

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030

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

Table of Contents

TABLE OF CONTENTS **2**

TABLE OF FIGURES **3**

TABLE OF TABLES **3**

1 INTRODUCTION **4**
1.1 PURPOSE 4
1.2 SECURITY TARGET AND TOE REFERENCES 4
1.3 PRODUCT OVERVIEW 5
1.4 TOE OVERVIEW 6
1.4.1 TOE Environment *8*
1.5 TOE DESCRIPTION 11
1.5.1 Physical Scope *11*
1.5.2 Logical Scope *12*
1.5.3 Product Physical and Logical Features and Functionality not included in the TOE *13*

2 CONFORMANCE CLAIMS **14**

3 SECURITY PROBLEM **15**
3.1 THREATS TO SECURITY 15
3.2 ORGANIZATIONAL SECURITY POLICIES 15
3.3 ASSUMPTIONS 15

4 SECURITY OBJECTIVES **17**
4.1 SECURITY OBJECTIVES FOR THE TOE 17
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 17
4.2.1 IT Security Objectives *17*
4.2.2 Non-IT Security Objectives *18*

5 EXTENDED COMPONENTS **19**
5.1 EXTENDED TOE SECURITY FUNCTIONAL COMPONENTS 19
5.2 EXTENDED TOE SECURITY ASSURANCE COMPONENTS 19

6 SECURITY REQUIREMENTS **20**
6.1.1 Conventions *20*
6.2 SECURITY FUNCTIONAL REQUIREMENTS 20
6.2.1 Class FAU: Security Audit *22*
6.2.2 Class FDP: User Data Protection *23*
6.2.3 Class FIA: Identification and Authentication *27*
6.2.4 Class FMT: Security Management *28*
6.3 SECURITY ASSURANCE REQUIREMENTS 30

7 TOE SPECIFICATION **31**
7.1 TOE SECURITY FUNCTIONS 31
7.1.1 Security Audit *32*
7.1.2 User Data Protection *32*
7.1.3 Identification and Authentication *33*
7.1.4 Security Management *33*

8 RATIONALE **35**
8.1 CONFORMANCE CLAIMS RATIONALE 35
8.2 SECURITY OBJECTIVES RATIONALE 35
8.2.1 Security Objectives Rationale Relating to Threats *35*
8.2.2 Security Objectives Rationale Relating to Policies *37*

8.2.3 Security Objectives Rationale Relating to Assumptions ... 37
8.3 RATIONALE FOR EXTENDED SECURITY FUNCTIONAL REQUIREMENTS ... 38
8.4 RATIONALE FOR EXTENDED TOE SECURITY ASSURANCE REQUIREMENTS ... 38
8.5 SECURITY REQUIREMENTS RATIONALE ... 38
8.5.1 Rationale for Security Functional Requirements Relating to the TOE Objectives ... 38
8.5.2 Security Assurance Requirements Rationale ... 40
8.5.3 Dependency Rationale ... 40
9 ACRONYMS AND TERMS ... 42
9.1 ACRONYMS ... 42
9.2 TERMINOLOGY ... 43

Table of Figures

FIGURE 1 - DEPLOYMENT CONFIGURATION AND PHYSICAL BOUNDARY OF THE TOE ... 8

Table of Tables

TABLE 1 - ST AND TOE REFERENCES ... 4
TABLE 2 - SOLUTIONS ENABLER SUPPORTED PLATFORMS ... 9
TABLE 3 – CC AND PP CONFORMANCE ... 14
TABLE 4 – THREATS ... 15
TABLE 5 – ASSUMPTIONS ... 16
TABLE 6 – SECURITY OBJECTIVES FOR THE TOE ... 17
TABLE 7 – IT SECURITY OBJECTIVES ... 17
TABLE 8 – NON-IT SECURITY OBJECTIVES ... 18
TABLE 9 – TOE SECURITY FUNCTIONAL REQUIREMENTS ... 20
TABLE 10 – ACCESS TYPES ... 24
TABLE 11 – MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR BY ROLE ... 28
TABLE 12 – MANAGEMENT OF SECURITY ATTRIBUTES BY ROLE ... 28
TABLE 13 - ASSURANCE REQUIREMENTS ... 30
TABLE 14 – MAPPING OF TOE SECURITY FUNCTIONS TO SECURITY FUNCTIONAL REQUIREMENTS ... 31
TABLE 15 – AUDIT RECORD CONTENTS ... 32
TABLE 16 – THREATS : OBJECTIVES MAPPING ... 35
TABLE 17 – ASSUMPTIONS : OBJECTIVES MAPPING ... 37
TABLE 18 - OBJECTIVES:SFRS/SARS MAPPING ... 38
TABLE 19 - FUNCTIONAL REQUIREMENTS DEPENDENCIES ... 40
TABLE 20 – ACRONYMS ... 42

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the Symmetrix VMAX Series with Enginuity Operating Environment 5875, Solutions Enabler 7.2.0, and Symmetrix Management Console 7.2.0, and will hereafter be referred to as the TOE throughout this document. The TOE is software that provides data availability, storage, and management capabilities for mid- to high-end data storage systems. The TOE can operate within a Storage Area Network[1] (SAN) or connected directly to a device[2].

1.1 Purpose

This ST contains the following sections to provide a mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats:

- Introduction
- (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. 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. 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 Security Functional Requirement (SFR) dependencies as pertaining to their consistency, completeness, and suitability.
- Acronyms and Terms (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® Symmetrix ® VMAX™ Series with Enginuity™ Operating Environment 5875, Solutions Enabler 7.2.0, and Symmetrix Management Console 7.2.0 Security Target
ST Version	Version 0.7
ST Author	Corsec Security Inc.

[1] Please refer to “SAN” in Section 9.2 Terminology for a definition of the term “SAN”.

[2] The term “device” refers to any type of computing device that can attach to or access storage on a Symmetrix system. Typical usage refers to application servers (e.g., a web server or file server), and mainframes (i.e., computing devices used to house large databases).

ST Publication Date	2011-01-26
TOE Reference	EMC® Symmetrix ® VMAX™ Series with Enginuity™ Operating Environment 5875.151, Solutions Enabler 7.2.0, and Symmetrix Management Console 7.2.0
Keywords	EMC, Symmetrix, Symmetrix Management Console, SAN, storage array, data storage, Enginuity.

1.3 Product Overview

The Symmetrix VMAX Series storage solution offers a physical storage array combined with operating and management software to fulfill an organization's data storage and availability needs. Application servers can use the storage array to store mission-critical data and facilitate the sharing of important files. Storage arrays can range in size from hundreds of terabytes to petabytes of raw[3] data storage capacity, and can be composed of a combination of high-capacity magnetic platter disk drives, or high-speed Enterprise Flash[4] drives. Disks in the storage array can be further grouped into a collection of Redundant Array of Independent Disks (RAID[5]) groups to ensure reliability and mitigate data loss.

Symmetrix arrays offer storage to direct-attached and SAN-attached devices. The SAN is composed of a series of controller cards and fabric[6] connections that provide redundant access to the storage array. The SAN architecture allows many different types of devices to share the services that a single Symmetrix array can provide, and allows organizations to manage storage across all devices from a single interface. Simplified management of storage for devices allows users greater control over storage allocation, improved fault tolerance, and simplified backups versus directly attaching storage to individual devices.

Several racks filled with Symmetrix components, called bays, organize the Symmetrix hardware into serviceable units. There are two types of bays: system bays, which contain the components necessary for controlling and servicing the Symmetrix array, and storage bays, which hold disks (up to 240 per bay) and Link Control Cards (LCCs). LCCs provide several services for disk drives, including data connectivity, environmental monitoring, failover[7] control, drive detection, and other functions related to drive control and reliability. Depending on solution level, the Symmetrix array can include one system bay and one to ten storage bays. The VMAX SE[8] alternative offers an integrated system bay with up to 120 disks and an optional storage bay.

Each storage bay connects (directly or daisy-chained) to the system bay, which connects to devices that use the Symmetrix array. The system bay mediates access between devices and the data stored on the Symmetrix array.

EMC offers other products that can be used to enhance the functionality of a Symmetrix system. EMC Celerra allows Symmetrix storage to be presented as Network Attached Storage[9] (NAS) to devices. EMC

[3] The term "raw" refers to the total storage capacity offered by the Symmetrix disks. After users apply RAID and the Symmetrix array claims a small portion of the space for its own use, the drives offer less total storage capacity.

[4] Please refer to "Flash" in Section 9.2 Terminology for a definition of the term "flash".

[5] Please refer to "RAID" in Section 9.2 Terminology for a definition of the term "RAID".

[6] Please refer to "Fabric" in Section 9.2 Terminology for a definition of the term "fabric".

[7] Please refer to "Failover" in Section 9.2 Terminology for a definition of the term "failover".

[8] SE – Single Engine

[9] Please refer to "NAS" in Section 9.2 Terminology for a definition of the term "NAS".

ControlCenter allows administrators[10] to manage the TOE via a separate management software suite. Neither Celerra nor ControlCenter are included in the evaluated configuration of the TOE for this ST.

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 TOE is the software portion of the Symmetrix VMAX Series storage solution. EMC develops Symmetrix arrays to provide enterprise-class data availability, storage, and management to a user's Information Technology (IT) infrastructure. The software portion of the Symmetrix solution consists of:

- Enginuity, the Symmetrix operating environment,
- Solutions Enabler 7.2.0, a Command Line Interface (CLI) and Application Programming Interface (API) that allows management and configuration of Symmetrix arrays, and
- Symmetrix Management Console (SMC), a web-based Graphical User Interface (GUI) that allows management and configuration of Symmetrix arrays.

The Enginuity operating environment efficiently services devices' read and write (Input/Output (I/O)) requests. Enginuity is designed to work with the Symmetrix architecture to manage I/O operations while minimizing the delays typically associated with such operations. Techniques that increase efficiency include caching of data in a large area of global memory[11], intelligent prefetching[12], and asynchronous writes to disk[13].

Solutions Enabler includes the Symmetrix Application Programming Interface (SYMAPI) and Symmetrix Command Line Interface (SYMCLI). These two interfaces, along with SMC, provide the management and configuration framework for Symmetrix arrays. Administrators can enter commands through SYMCLI, interact with the SMC GUI, or write scripts that take advantage of SYMAPI to manage and configure the TOE. Each interface requires that administrators identify themselves before the TOE performs any actions on their behalf. SMC also requires administrators to authenticate their identities.

The TOE does not present physical disks to users; instead, administrators define logical disks. Logical disks typically include segments from multiple physical disks, rather than occupying physically adjacent areas on a single disk. When creating a logical disk, administrators can define the capacity of the disk. Administrators configure one or more logical disks into pools— groups of logical disks—and give users access to the pools.

The TOE offers administrators the ability to provide tiered storage for users with differing speed requirements. The storage array must contain multiple types of disks, such as high speed Enterprise Flash drives and high capacity magnetic drives, for this feature to function. Administrators can select the type of physical disks that will contain a logical disk, and thereby provide tiered storage based on the disk type

[10] Unless explicitly noted, the term "administrator" is used in this document to refer to an individual who manages the TOE and not the "administrator" role.

[11] Please refer to "Global Memory" in Section 9.2 Terminology for a definition of the term "Global Memory".

[12] Intelligent prefetching is a technique used to predict what data will be accessed next, based on what data has been recently accessed.

[13] Asynchronous writes occur because devices write data to global memory, rather than directly to the disk. Enginuity performs the disk write as a separate operation.

selected. Users of such logical disks benefit from the shortened access times that faster physical disks provide whenever the TOE must retrieve data into global memory.

The TOE offers a secure erase feature that allows administrators to destroy the data on a physical disk before the physical disk is removed from the storage array. Administrators can select one of several algorithms to use, and can set the number of passes to make. After the secure erase function has completed, no residual information exists on the erased disk.

The TOE offers an Instantaneous Volume Table Of Contents (iVTOC) function. iVTOC is a method of formatting disks or partitions on disks with 0's while still allowing the TOE to access the disk. If the area of the disk accessed is the portion being formatted or scheduled to be formatted, then the TOE returns all 0's in place of actual data, until the formatting operation is complete and data is stored in those portions of the disk.

The TOE is capable of grouping disks into RAID groups. The supported RAID types are:

- RAID 1 and RAID 10,
- RAID 5 (3+1) and RAID 5 (7+1),
- RAID 6 (6+2) and RAID 6 (14+2).

The RAID configurations allow the TOE to preserve data stored within a RAID group when a disk in the RAID group fails. When a disk in a RAID group fails and is replaced, the TOE automatically rebuilds the data from the other drives and populates the new disk.

The TOE provides access control functions that restrict the ability of administrators to manage pools of logical disks. Administrators can use Solutions Enabler and SMC to assign management rights to devices based on each device's unique identifier (typically the device's hostname).

Figure 1 shows the details of the deployment configuration and the physical boundary of the TOE.

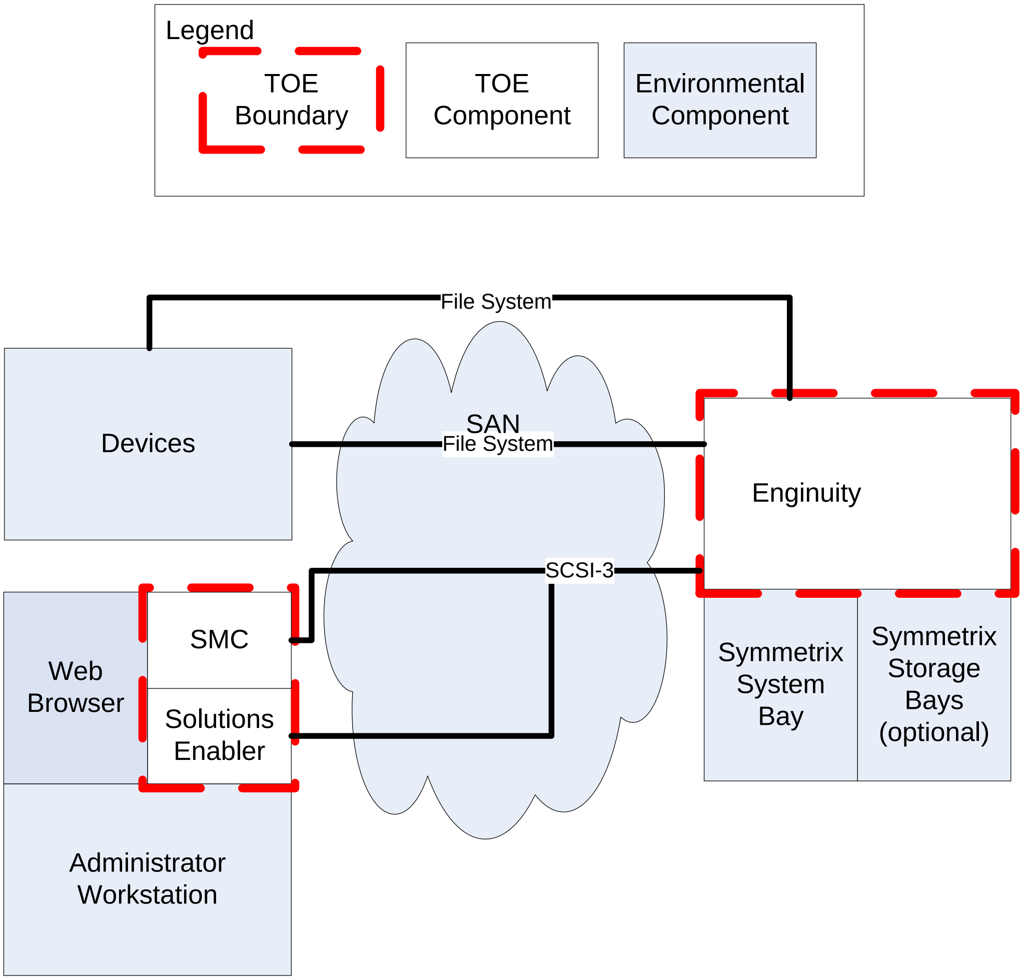

Figure 1 - Deployment Configuration and Physical Boundary of the TOE

The TOE can provide the following services:

- Monitor the integrity of stored user data against unintentional corruption,
- Control access to stored user data and storage space,
- Control access to the ability to manage user data storage.

1.4.1 TOE Environment

The evaluated deployment configuration of the TOE requires the following environmental components in order to function properly:

- the Symmetrix hardware, including both system and storage bays and their contents,
- a SAN to allow devices to connect to the TOE,
- devices on the network that use the storage that the TOE provides,
- cables and connectors that allow the devices to connect to the SAN, and
- an administrator workstation with an operating system that supports Solutions Enabler and a web browser. Supported web browsers include Internet Explorer 6 through 8 and Firefox 3.

The TOE is intended to be deployed in a physically secure cabinet room or data center with the appropriate level of physical access control and physical protection (e.g., fire control, locks, alarms, etc.) The TOE is intended to be managed by administrators operating under a consistent security policy.

The TOE is intended to provide storage to devices on a SAN or directly attached to the Symmetrix array. For the TOE to operate correctly, all devices must be connected to the TOE directly or through the SAN. The TOE environment is required to provide for this configuration.

The TOE is managed through a CLI and web-based GUI. Administrators must access these interfaces from a trusted workstation that supports the Solutions Enabler software and a graphical web browser. The CLI and web GUI are part of the TOE. Administrators access the CLI via the Solutions Enabler product, and the web GUI through a web browser.

Solutions Enabler can run on the platforms listed in Table 2 below:

Table 2 - Solutions Enabler Supported Platforms

Company	Operating System	Operating System Versions
Fujitsu Technology Solutions	Solaris	v10, v9
Hewlett Packard	HP-UX 11i	v1.0, v2, v3
	Open VMS	V7.3-2, V8.2, V8.2-1, V8.3, V8.3-1H1
	Tru64 UNIX	V5.1B-0, V5.1B-1, V5.1B-2, V5.1B-3, V5.1B-4, V5.1B-5
IBM	AIX	v5.2, v5.3, v6.1
	IBMi	v7.1, vi6.1.1
	VIOS	V2.1.2.10, v2.1.2.12, v2.1.2.13, v2.1.3.10
	i5/OS [System i]	V5R4M5, V6R1/i6.1
Microsoft	Windows 2003 [IA64]	Data Center SP2, Enterprise Edition SP2, Standard Edition SP2
	Windows 2003 [x64]	DataCenter R2 SP2, SP2
		Enterprise Edition R2 SP2, SP2
		Standard Edition R2 SP2, SP2
	Windows 2003 [x86]	DataCenter SP2, Enterprise Edition SP2, Standard Edition SP2
	Windows 2008 [IA64] for Itanium-based Systems	R2, SP2
	Windows 2008 [x64] for Itanium-based Systems	DataCenter, DataCenter R2,
		Enterprise Edition, Enterprise Edition R2
		Standard Edition, Standard Edition R2
	Windows 2008 [x86]	DataCenter, DataCenter SP2,
		Enterprise Edition, Enterprise Edition SP2
		Standard Edition, Standard Edition SP2

Oracle	Solaris	10 (SPARC, x86)
		9 (SPARC)
Red Hat	RHEL [32-bit]	3.0: U7 AS/ES, U8 AS/ES
		3.9 AS/ES1
		4.0: AS/ES, U1 AS/ES, U2 AS/ES, U3 AS/ES, U4 AS/ES
		4.5 AS/ES
		4.6 AS/ES
		4.7 AS/ES
		4.8 AS/ES
		5.0
		5.1
		5.2
		5.3
		5.4
		5.5
	RHEL [AMD-64]	3.0: U7 AS/ES, U8 AS/ES
		3.9 AS/ES
	RHEL [EM64T]	3.0: U7 AS/ES, U8 AS/ES
		3.9 AS/ES
	RHEL [IA64]	3.0: U7 AS/ES, U8 AS/ES
		3.9 AS/ES
		4.0: AS/ES, U1 AS/ES, U2 AS/ES, U3 AS/ES, U4 AS/ES
		4.5 AS/ES
		4.6 AS/ES
		4.7 AS/ES
		4.8 AS/ES
		5.0
		5.1
		5.2
		5.3
		5.4
		5.5
	[IBM Power]	4.5 AS
		4.6 AS
		5.0

		5.1
		5.2
		5.3
		5.4
		5.5
	[s390x–64–Bit]	5.4
		5.5
	[x86_64]	4.0 AS/ES, U1 AS/ES, U2 AS/ES, U3 AS/ES, U4 AS/ES
SuSE	SLES [32–Bit]	10, 10 SP1, 10 SP2, 10 SP3
		11, 11 SP1
		9 GM, 9 SP1, 9 SP2, 9 SP3
	SLES [IA64]	10, 10 SP1, 10 SP3
		11, 11 SP1
		9 SP1, 9 SP2, 9 SP3
	SLES [IBM Power]	10, 10 SP1, 10 SP2, 10 SP3
		9 SP3, 9 SP4
	SLES [s390x–64–Bit]	10 SP3
		11 SP1, 11
	SLES [x86_64]	10, 10 SP1, 10 SP2, 10 SP3
		11, 11 SP1
		9 SP1, 9 SP2, 9 SP3
VMware	ESX	3.5
		4.0 (vSphere 4)
		4.1 (vSphere 4)
	ESXi	3.5
		4.0 (vSphere 4)
		4.1 (vSphere 4)

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 1 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.

The TOE is a software-only storage solution which runs on custom Symmetrix hardware. The TOE is installed on the Symmetrix hardware and a separate administrator workstation as depicted in Figure 1 above. The essential physical components for the proper operation of the TOE in the evaluated configuration are the Enginuity, Solutions Enabler, and SMC software. The TOE must run on the included Symmetrix hardware.

1.5.1.1 Guidance Documentation

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

- SymmetrixSolutions Enabler Release Notes,
- Symmetrix Management Console Release Notes,
- Symmetrix VMAX Series Release Notes,
- Symmetrix VMAX Series Product Guide,
- Symmetrix VMAX Series Physical Planning Guide,
- Solutions Enabler Installation Guide,
- Solutions Enabler Symmetrix CLI Quick Reference,
- Solutions Enabler Symmetrix CLI Command Reference,
- Symmetrix Management Console Online Help,
- Symmetrix Management Console Installation Guide.

1.5.2 Logical Scope

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, and
- Security Management.

1.5.2.1 Security Audit

The TOE is capable of generating audit messages that administrators can review. Audit review is provided through Solutions Enabler and SMC. Audits show the history of administrator commands.

1.5.2.2 User Data Protection

The TOE controls access to the storage that it provides to users. Users can use and manage the storage only if an administrator has configured the TOE's Discretionary Access Control Policy to allow access to an area of storage. If administrators have not assigned permissions to a user for a storage area, then the user cannot access or manage that storage.

The TOE protects stored user data from unintentional corruption through the use of RAID groups.

The TOE can erase all data from a physical disk that is to be removed from the storage array. Several algorithms provide the TOE with the ability to ensure that no residual information remains on an erased disk.

The TOE can apply iVTOC functionality to logical disks, which results in the TOE formatting the disks. Any information previously on the disk or partition that was formatted is replaced with 0's upon initiation of the iVTOC process.

1.5.2.3 Identification and Authentication

The TOE ensures that SMC administrators must identify themselves and authenticate their identities before accessing any of the functionality available in SMC. Administrators that use Solutions Enabler must identify their identities before performing any actions through Solutions Enabler.

1.5.2.4 Security Management

The TOE provides administrators with the ability to manage the behavior of security functions and security attributes. Administrators are assigned one of six roles: Administrator, SecurityAdmin, StorageAdmin, Auditor, Monitor, and None. The TOE allows administrators to manage the attributes associated with the— by default restrictive—Discretionary Access Control Policy and Storage Access Control Policy.

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

Features and functionality that are not part of the evaluated configuration of the TOE include:

- the Service Processor,
- any hardware component that is part of the Symmetrix product,
- TimeFinder,
- Symmetrix Remote Data Facility (SRDF),
- priority controls,
- Celerra,
- ControlCenter, and
- use of crypto-generated numbers for identification of devices.

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 3, July 2009; CC Part 2 conformant; CC Part 3 conformant; Parts 2 and 3 Interpretations from the Interpreted Common Evaluation Methodology as of 2009-09-18 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	2+ augmented with ALC_FLR.2 Flaw reporting procedures

3 Security Problem

This section describes the security aspects of the environment in which the TOE is 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 assets against which protection is required by the TOE or by the security environment. The threat agents are divided into three 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/parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)
- Natural threats: These are threats to the TOE Security Function (TSF) that are a natural byproduct of the systems that compose the TOE, such as electromagnetic interference on a line during transmission of user data.

The following threats are applicable:

Table 4 – Threats

Name	Description
T.DATA_CORRUPTION	User data and configuration data could become corrupted due to hardware failure or incorrect system operations.
T.IMPROPER_SERVER	A user or attacker could attempt to bypass the access controls provided by the TOE by using one of the systems connected to the TOE.
T.NO_AUDIT	An attacker may perform security-relevant operations on the TOE without being held accountable for them.

3.2 Organizational Security Policies

There are no Organizational Security Policies (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	It is assumed that there are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	It is assumed that the administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.LOCATE	It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrators only.
A.FIREWALL	It is assumed that the IT Environment must block all traffic originating from outside of the controlled access facility intended for the Solutions Enabler ports of the TOE.
A.TIMESTAMPS	It is assumed that the IT Environment will provide reliable timestamps for the TOE to use.
A.CONNECTIVITY	It is assumed that the IT Environment will be configured in such a way as to allow TOE users to access the information stored on the TOE.

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.ADMIN	The TOE must provide a method for administrators to manage the TOE.
O.PROTECT	The TOE must protect configuration and user data that it has been entrusted to protect.
O.LOG	The TOE must record events of security relevance at the "not specified" level of audit. The TOE must provide authorized administrators with the ability to review the audit trail.

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.PROPER_NAME_ASSIGNMENT	The TOE Environment must provide accurate unique server identifiers for each system that communicates with the TOE.
OE.SECURE_COMMUNICATIONS	The TOE Environment must provide untampered communications between systems connected to the SAN.
OE.SECURE_SERVERS	The TOE Environment must ensure that application servers communicating with the TOE do not allow unauthorized users or attackers access to the TOE.
OE.TIMESTAMPS	The hardware that the TOE is installed on will provide reliable timestamps for the TOE.
OE.FIREWALL	The TOE Environment must ensure that the port designated for use

	by Solutions Enabler is blocked for traffic coming from outside the controlled access facility where the TOE is housed.
OE.CONNECT	The TOE administrators will configure the IT Environment so that users can access data through a direct connection to the TOE, or so that zones are configured on the SAN that allow users to access data stored on 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 do not require the implementation of functions in the TOE software. Thus, they are satisfied largely through application of procedural or administrative measures.

Table 8 – Non-IT Security Objectives

Name	Description
OE.MANAGE	Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.
OE.NOEVIL	Sites using the TOE shall ensure that TOE administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
OE.PHYSICAL	The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

5.1 Extended TOE Security Functional Components

There are no extended SFRs defined for this ST.

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.1.

6.1.1 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 Parts 2 and 3 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 italicized 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		✓		
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_RIP.1a	Subset residual information protection	✓	✓	✓	✓
FDP_RIP.1b	Subset residual information protection	✓	✓	✓	✓
FDP_SDI.2	Stored data integrity monitoring and action		✓	✓	
FIA_UAU.2	User authentication before any action			✓	
FIA_UID.2	User identification before any action			✓	
FMT_MOF.1	Management of security functions behaviour	✓	✓		
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3a	Static attribute initialisation	✓	✓		✓

FMT_MSA.3b	Static attribute initialisation	✓	✓		✓
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		

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:

- Start-up and shutdown of the audit functions;
- All auditable events, for the [*not specified*] level of audit; and
- [*all inline commands issued, all Symmetrix Service Processor log-ins, all config change script activity, all serviceability and replacement script activity*].

FAU_GEN.1.2

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other information*].

Dependencies: FPT_STM.1 Reliable time stamps

Application Note: The TOE's audit function cannot be stopped other than by the shutdown of the TOE. No "shutdown" audit record is generated, but auditing ends upon shutdown. When the TOE starts up again, an audit record is generated. An administrator can tell that the TOE previously shutdown by looking at the start up audit record and the audit record immediately preceding the start up audit record.

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*the Administrator, SecurityAdmin, and Auditor roles*] with the capability to read [*all audit information viewable through the SMC*] 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 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 Policy*] on [

Subjects: access control groups
Objects: groups of logical disks
Operations: configure, manage

].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1b Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1b

The TSF shall enforce the [*Storage Access Control Policy*] on [

Subjects: devices accessing storage controlled by the TOE
Objects: Storage space
Operations: read/write from storage, masking operation
].

Dependencies: FDP_ACF.1 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 Policy*] to objects based on the following: [

Subject (device) attributes:

- *Host ID*
- *Access control entries (permissions)*

Object (logical disk group) attributes:

- *Group name*
- *Logical disks included in the group*
- *Access control entries (permissions)*

].

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 device can manage or configure a logical disk pool if the device has the appropriate Access Type to perform the requested operation on that logical disk pool—see* Table 10].

FDP_ACF.1.3a

The TSF shall explicitly authorize access of subjects to objects based on ~~the following~~ **no** additional rules~~:~~.

FDP_ACF.1.4a

The TSF shall explicitly deny access of subjects to objects based on ~~the~~ [*no additional rules*].

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

Table 10 – Access Types

Access Type	Description
ADMIN	Grants administrator privilege to grant/deny access control entries to hosts and users.
ADMINRD	Grants read access only to all access control information.
ALL	All possible access types granted except ADMIN and ADMINRD. Must be directed to ALL devices.
BASE	Allows the discovery of devices and to obtain states and statistics from the Symmetrix array (directors and devices).
BASECTRL	Allows base control operations on devices and device groups.
BCV	Allows TimeFinder[14] (BCV) and clone control and status operations.
CACHCTRL	Allows cache control operations concerning partition management.
CFGDEV	Allows powerful configuration control operations that manage various types of configuration changes on devices in the Symmetrix.
CFGSYM	Allows access to set Symmetrix attributes, set port flags, and swap SRDF groups. Must be directed to ALL devices.
CHECKSUM	Allows Symmetrix device Double Checksum operations.
CREATEDV	Allows the creation and deletion of Symmetrix devices.
DIRCTRL	Allows you to take directors and their ports offline and online. Must be directed to ALL devices.
ECC	Allows the ECC Symmetrix agent to run on the requested host.
OPTMZR	Allows user-configurable attributes that may affect the Symmetrix Optimizer behavior.
POWRPATH	Access to PowerPath-directed devices in an RDF consistency group. Must be directed to ALL devices.
QOS	Allows the execution of Quality of Service (QOS) performance control operations to manage copy priorities. Excludes cache partition management functionality.
RCOPY	Manages Open Replicator sessions.

[14] Please note that TimeFinder is not included within this evaluation of the TOE.

RDF	Allows SRDF control and set operations.
SDDF	Allows the DeltaMark (Change Tracker) functionality that monitors track changes.
SDR	Allows mapping/unmapping of devices to directors/ports for the Symmetrix Disk Reallocation (SDR) feature.
SNAP	Allows the creation and management of virtual copy sessions between a source device and multiple virtual (VDEV) target devices.
VLOGIX	Enables access to Device Masking or Volume Logix devices.

FDP_ACF.1b Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1b

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

Subject (devices accessing storage controlled by the TOE) attributes:

- *Group name*
- *Devices included in the group*
- *Access control entries (permissions)*

Object (storage space) attributes:

- *Initiator Group*
- *Storage Group*
- *Port Group*
- *Masking View*

].

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 device can access a logical disk if:

- *the device is connected to a port (directly or through a SAN) that is part of a View,*
- *the Masking View includes the logical disk within its Storage Group, and*
- *the device designates an initiator from an Initiator Group that is part of the View*

].

FDP_ACF.1.3b

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

FDP_ACF.1.4b

The TSF shall explicitly deny access of subjects to objects based on ~~the~~ [*no additional rules*].

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

FDP_RIP.1a Subset residual information protection

Hierarchical to: No other components.

FDP_RIP.1.1a

The TSF shall ensure that any previous information content of a ~~resource~~ **physical disk** is made unavailable upon the [*deallocation of the disk from*] the following objects: [*the storage array*].

Dependencies: No dependencies

FDP_RIP.1b Subset residual information protection

Hierarchical to: No other components.

FDP_RIP.1.1b

The TSF shall ensure that any previous information content of a ~~resource~~ **logical disk** is ~~made unavailable~~ **zeroized** upon the [*allocation of the disk to*] the following objects: [*the list of disks to be formatted using iVTOC functionality*].

Dependencies: No dependencies

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 [*unintentional integrity errors*] on all ~~objects~~ **user data**, based on the following attributes: [*mirroring for RAID 1 and RAID 10; parity data for RAID 5 (3+1) and (7+1); and parity data for RAID 6 (6+2) and (14+2)*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [*reconstruct the user data and notify the authorized administrator*].

Dependencies: No dependencies

6.2.3 Class FIA: Identification and Authentication

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~~ **SMC administrator** to be successfully authenticated before allowing any other TSF-mediated actions **through SMC** on behalf of that ~~user~~ **administrator**.

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~~ **administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.

Dependencies: No dependencies

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [*determine the behavior of, disable, enable, modify the behavior of*] the functions [*listed under the 'Security Functions Behavior Permissions' column of Table 11*] to [*the roles listed under the 'Role' column of Table 11*].

Table 11 – Management of Security Functions Behaviour by Role

Role	Security Functions Behavior Permissions
Administrator	Can perform all operations
SecurityAdmin	Change own password, reset other administrator passwords, assign permissions to other administrators, create and delete SMC accounts, discover arrays, set access controls, set Replication and Reservation preferences, view audit log
StorageAdmin	Manage arrays, show and add license keys, set Alerts and Optimizer monitoring options, release array locks, set access controls, set Replication and Reservation preferences, view audit log
Auditor	View settings (no restrictions)
Monitor	View settings (excluding audit log and Access Control definitions)
None	No actions authorized.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Discretionary Access Control Policy, Storage Access Control Policy*] to restrict the ability to [*perform the operations specified in the 'Security Attribute Permissions' column of Table 12 on]* the security attributes [*listed in the 'Security Attribute Permissions' column of Table 12*] to [*the roles listed in the 'Role' column of Table 12*].

Table 12 – Management of Security Attributes by Role

Role	Security Attribute Permissions
Administrator	Can perform all operations on all security attributes
SecurityAdmin	Set access controls
StorageAdmin	Set access controls (autoprovisioning only)
Auditor	None
Monitor	None
None	None

Dependencies: **FDP_ACC.1 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 Policy*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP[15].

FMT_MSA.3.2a

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

Dependencies: **FMT_MSA.1 Management of security attributes**
FMT_SMR.1 Security roles

FMT_MSA.3b Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1b

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

FMT_MSA.3.2b

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

Dependencies: **FMT_MSA.1 Management of security attributes**
FMT_SMR.1 Security roles

FMT_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: [*Management of Security Functions Behavior, 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 [*Administrator, SecurityAdmin, StorageAdmin, Auditor, Monitor, None*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: **FIA_UID.1 Timing of identification**

[15] SFP – Security Functional Policy

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 EAL 2+ augmented with ALC_FLR.2. Table 13 - Assurance Requirements summarizes the requirements.

Table 13 - Assurance Requirements

Assurance Requirements	
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

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 14 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	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_RIP.1a	Subset residual information protection
	FDP_RIP.1b	Subset residual information protection
	FDP_SDI.2	Stored data integrity monitoring and action
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3a	Static attribute initialisation
	FMT_MSA.3b	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles

7.1.1 Security Audit

The TOE generates audit records to keep a record of all inline commands issued, all Symmetrix Service Processor log-ins, all config change script activity, all serviceability and replacement script activity. The TOE audit records contain the following information:

Table 15 – Audit Record Contents

Field	Content
Record Number	An integer that starts at 1 and is incremented by 1 for each new audit log record generated.
Time	Time the audit record was created in MM/DD/YY HH:MM:SS format.
Vendor ID	Almost always "EMC Corp".
Application ID	Which application triggered the log entry.
Host Name	The network name of the host generating the record. This name is unique for each host and thus allows host identification.
Client Host	If the hostname is a server acting on behalf of a client system, then the name of the client system is placed in this field. Values for this field are generated as are the hostname values.
Function Class	Class, or major functional area, of action being performed.
Action Code	Subordinate action in a Function Class being performed. The kinds of actions include: • Successful connection • Failed connection • Loss of connection • Reboot • File transfer • Configuration change • Installation • Uninstallation of tokens
Text	Free-form text description of action being performed.
Username	The name of the logged-in user responsible for issuing the command that triggered the record.

Audit records can be viewed through SMC or through the Solutions Enabler CLI. In SMC administrators can select the audit log page through a tab menu along the top of the screen.

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

7.1.2 User Data Protection

The TOE enforces a Discretionary Access Control Policy on devices attempting to manage or configure logical disk pools, and a Storage Access Control Policy on devices trying to read to or write from the storage that the TOE provides. Access via the Discretionary Access Control Policy is based on the Access Type assigned to the device attempting to manage or configure the logical disk pool. Access via the Storage Access Control Policy is based on the Initiator Group, Storage Group, Port Group, and Masking View associated with the storage space:

- initiators specify an address that devices can use to connect to logical disks on a SAN,
- storage specifies TOE storage device identification numbers,
- ports specify physical ports that connect the TOE with the SAN and other devices, and
- Masking Views are constructs created when an initiator group, storage group, and port group are associated with one another. Masking Views allow a set of initiators access to a group of logical disks.

The TOE allows administrators to erase data on drives within the storage array. Administrators can specify the algorithm to use and the number of times to execute the erasure algorithm. As a result, administrators can destroy all residual information on a physical disk before it is removed from the storage array (e.g., if it is a failed drive).

The TOE allows administrators to perform iVTOC functionality on logical disks and partitions within the storage array. Administrators specify which logical disks and partitions should be formatted. The formatting process replaces all of the data on the disk or partition with 0's, removing any residual data that existed on the disk.

The TOE protects stored user data from unintentional corruption through the use of RAID groups. RAID groups provide mirroring and striping of data. Mirroring creates an exact copy of all of the data on a disk, so that in the event that some of the data becomes corrupted or becomes inaccessible (e.g., because of a disk failure), the RAID can discover the error and replace it with the correct data. Parity calculates a code from the actual data present on the disks, then distributes the parity data so that it exists on a separate drives than the drives containing the information it was calculated from. If an error occurs in a parity-based RAID group, the data can be rebuilt from the parity information stored on the other disks.

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

7.1.3 Identification and Authentication

Both SMC and Solutions Enabler require administrators to identify themselves before the TOE performs any actions on their behalf. Solutions Enabler identifies the administrator by submitting a host identifier and the identifier for the user logged into that host alongside commands. SMC requires administrators to enter a valid username and password pair before performing any actions on behalf of the administrator. SMC Administrators enter the username and password pair at the SMC login screen and invoke the Login button.

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

7.1.4 Security Management

The TOE provides two management interfaces for administrators: Solutions Enabler as a CLI and SMC as a web GUI. SMC is accessed through a web browser on an administrator workstation and presents commands to users in the form of Hypertext Markup Language (HTML) elements (such as text boxes, hyperlinks, and drop-down lists). Solutions Enabler is customer software that must be installed on the administrator's workstation. The Solutions Enabler interface uses well-defined text conventions to pass commands to the TOE. Both interfaces are protected from tampering and disclosure: SMC via Secure

Hypertext Transfer Protocol (HTTPS) and Solutions Enabler via Transport Layer Security (TLS) wrapping of CLI commands.[16]

The TOE presents six limited roles to administrators: Administrator, SecurityAdmin, StorageAdmin, Auditor, Monitor, and None. The None role is used to specifically deny management access to a group of devices. Other roles have a predefined set of permissions to view or configure different parts of the TOE. Only the Administrator role has unlimited access to manage the TOE.

Administrators can also manage security attributes associated with the Discretionary Access Control Policy and the Storage Access Control Policy. Only the Administrator, SecurityAdmin, and StorageAdmin roles have access rights to manage these attributes. The Discretionary Access Control Policy, by default, does not permit any devices access to manage or configure the storage that the TOE provides. The Storage Access Control Policy, by default, does not permit any devices to use the storage provided by the TOE.

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

[16] SSL and TLS are provided by the TOE Environment, not the TOE, and only when the TOE is in Client-Server Mode.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Parts 2 and 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 Revision 3. There are no extended SFRs or SARs contained within this ST.

There are no protection profile claims for this ST.

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 that the mappings between the threats, polices, and assumptions to the security objectives is 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 16 – Threats : Objectives Mapping

Threats	Objectives	Rationale
T.DATA_CORRUPTION User data and configuration data could become corrupted due to hardware failure or incorrect system operations.	O.ADMIN The TOE must provide a method for administrators to manage the TOE.	O.ADMIN counters this threat by allowing administrators to properly configure the mechanisms of the TOE that prevent data corruption and restrict access to authorized individuals.
	O.PROTECT The TOE must protect configuration and user data that it has been entrusted to protect.	O.PROTECT counters this threat by providing mechanisms to protect the configuration and user data that has been entrusted to the TOE.
	OE.FIREWALL The TOE Environment must ensure that the port designated for use by Solutions Enabler is blocked for traffic coming from outside the controlled access facility where the TOE is housed.	OE.FIREWALL counters this threat by preventing unauthenticated use of Solutions Enabler by subjects outside of the controlled access facility where the TOE is housed.
T.IMPROPER_SERVER A user or attacker could attempt to bypass the access controls provided by the TOE by using one of the systems connected to the TOE.	O.ADMIN The TOE must provide a method for administrators to manage the TOE.	O.ADMIN counters this threat by allowing administrators to properly configure the mechanisms of the TOE designed to control the Discretionary Access Control Policy and the Storage Access Control Policy.
	OE.PROPER_NAME_ASSIGNME	OE.PROPER_NAME_ASSIGNME

	NT The TOE Environment must provide accurate unique server identifiers for each system that communicates with the TOE.	NT counters this threat by ensuring that the unique server identifiers provided to the TOE are accurate. This allows the mechanisms provided by O.PROTECT to properly protect data.
	OE.SECURE_COMMUNICATIONS The TOE Environment must provide untampered communications between systems connected to the SAN.	OE.SECURE COMMUNICATIONS counters this threat by ensuring that all communications with the TOE are untampered for administration of the TOE, internal TOE communications, and data sent to or from the TOE.
	O.PROTECT The TOE must protect configuration and user 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 configuration data. O.PROTECT allows administrators to destroy residual user or configuration data that is contained within hard drives before they are removed from the storage array.
	OE.SECURE_SERVERS The TOE Environment must ensure that application servers communicating with the TOE do not allow unauthorized users or attackers access to the TOE.	OE.SECURE_SERVERS mitigates this threat by ensuring that only authorized users can access the TOE through servers connected to the TOE.
T.NO_AUDIT An attacker may perform security-relevant operations on the TOE without being held accountable for them.	O.LOG The TOE must record events of security relevance at the "not specified" level of audit. The TOE must provide authorized administrators with the ability to review the audit trail.	O.LOG counters this threat by ensuring that an audit trail of management events and alerts on the TOE is preserved.
	OE.TIMESTAMPS The hardware that the TOE is installed on will provide reliable timestamps for the TOE.	OE.TIMESTAMPS counters this threat by ensuring that accurate timestamps are provided for all audit records, allowing the order of events to be preserved.

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 ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 17 – Assumptions : Objectives Mapping

Assumptions	Objectives	Rationale
A.MANAGE It is assumed that there are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.	OE.MANAGE upholds this assumption by ensuring that those responsible for the TOE provide competent individuals to perform management of the security of the environment. These individuals restrict these functions and facilities from unauthorized use.
A.NOEVIL It is assumed that the administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.	OE.NOEVIL Sites using the TOE shall ensure that TOE administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.	OE.NOEVIL upholds this assumption by ensuring that administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.LOCATE It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrators only.	OE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	OE.PHYSICAL upholds this assumption by ensuring that physical security is provided for the TOE.
A.FIREWALL It is assumed that the IT Environment must block all traffic originating from outside of the controlled access facility intended for the Solutions Enabler ports of the TOE.	OE.FIREWALL The TOE Environment must ensure that the port designated for use by Solutions Enabler is blocked for traffic coming from outside the controlled access facility where the TOE is housed.	OE.FIREWALL upholds this assumption by ensuring the necessary ports will be blocked from traffic coming from outside the controlled access facility.
A.CONNECTIVITY It is assumed that the IT Environment will be configured in such a way as to allow TOE users to access the information stored on the TOE.	OE.CONNECT The TOE administrators will configure the IT Environment so that users can access data through a direct connection to the TOE, or so that zones are configured on the SAN that allow users to access data stored on the TOE.	OE.CONNECT upholds this assumption by ensuring that the IT Environment is configured appropriately to allow users to access information stored on 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 SFRs defined for this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs defined for this ST.

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 Relating to the TOE Objectives

Table 18 - Objectives:SFRs/SARs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must provide a method for administrators to manage the TOE.	FIA_UAU.2 User authentication before any action	This requirement supports O.ADMIN by requiring SMC administrators to authenticate their claimed identities before the TOE will perform any actions on their behalf via SMC.
	FIA_UID.2 User identification before any action	This requirement supports O.ADMIN by requiring administrators to identify themselves before the TOE will perform any actions on their behalf.
	FMT_MOF.1 Management of security functions behaviour	This requirement supports O.ADMIN by specifying what roles can modify the behavior of, enable, disable, and determine the behavior of the TSF.
	FMT_MSA.1 Management of security attributes	This requirement supports O.ADMIN by specifying the security attributes of the TOE that can be modified and which administrators can modify them.
	FMT_MSA.3a Static attribute initialisation	This requirement supports O.ADMIN by specifying that restrictive default values are used by the Discretionary Access

		Control Policy, and specifying which administrative roles can specify alternative values.
	FMT_MSA.3b Static attribute initialisation	This requirement supports O.ADMIN by specifying that restrictive default values are used by the Storage Access Control Policy, and specifying which administrative roles can specify alternative values.
	FMT_SMF.1 Specification of management functions	This requirement supports O.ADMIN by specifying each of the management functions that are used to securely manage the TOE. These functions are provided by Solutions Enabler and SMC.
	FMT_SMR.1 Security roles	This requirement supports O.ADMIN by specifying the roles defined to govern management of the TOE.
O.PROTECT The TOE must protect configuration and user data that it has been entrusted to protect.	FDP_ACC.1a Subset access control	This requirement supports O.PROTECT by enforcing an access control policy that ensures that only authorized devices gain access to configuration data within the TOE.
	FDP_ACC.1b Subset access control	This requirement supports O.PROTECT by enforcing an access control policy that ensures that only authorized devices gain access to configuration data within the TOE.
	FDP_ACF.1a Security attribute based access control	This requirement supports O.PROTECT by providing access control functionality to manage access to configuration data within the TOE.
	FDP_ACF.1b Security attribute based access control	This requirement supports O.PROTECT by providing access control functionality to manage access to user data within the TOE.
	FDP_RIP.1a Subset residual information protection	This requirement supports O.PROTECT by ensuring that residual data on the disks in the storage array is destroyed before they are removed from the storage array.
	FDP_RIP.1b	This requirement supports

	Subset residual information protection	O.PROTECT by ensuring that residual data on the disks in the storage array is destroyed before they are reallocated for use after formatting.
	FDP_SDI.2 Stored data integrity monitoring and action	This requirement supports O.PROTECT by providing data integrity against unintentional corruption via the RAID options the TOE implements.
O.LOG The TOE must record events of security relevance at the "not specified" level of audit. The TOE must provide authorized administrators with the ability to review the audit trail.	FAU_GEN.1 Audit Data Generation	This requirement supports O.LOG by requiring the TOE to produce audit records for the system security events.
	FAU_SAR.1 Audit review	This requirement supports O.LOG by requiring the TOE to make the recorded audit records available for review.

8.5.2 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to 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. While the System may monitor a hostile environment, it 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 System has 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 Dependency Rationale

This ST satisfies all the requirement dependencies of the Common Criteria. Table 19 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 19 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Timestamps are provided by the IT Environment.
FAU_SAR.1	FAU_GEN.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_RIP.1a	None	Not applicable	
FDP_RIP.1b	None	Not applicable	
FDP_SDI.2	None	Not applicable	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is included and is hierarchical to FIA_UID.1.
FIA_UID.2	None	Not applicable	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FMT_SMF.1	✓	
	FDP_ACC.1b	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1a	✓	
FMT_MSA.3a	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3b	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	Not applicable	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is included and is hierarchical to FIA_UID.1.

9 Acronyms and Terms

9.1 Acronyms

Table 20 – Acronyms

Acronym	Definition
API	Application Programming Interface
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
GB	Gigabyte
GUI	Graphical User Interface
HTTPS	Secure Hypertext Transfer Protocol
HTML	Hypertext Markup Language
I/O	Input/Output
IT	Information Technology
LCC	Link Control Card
NAS	Network Attached Storage
PP	Protection Profile
QOS	Quality Of Service
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SAR	Security Assurance Requirement
SE	Single Engine
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMC	Symmetrix Management Console
SRDF	Symmetrix Remote Data Facility
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function

9.2 Terminology

Administrator – an individual who manages and configures the TOE. Also can be used as the "Administrator role" where indicated.

Device – The term "device" refers to any type of computing device that can attach to or access storage on a Symmetrix. Typical usage refers to application servers (e.g., a web server or file server), and mainframes (i.e., computing devices used to house large databases).

Fabric – The hardware that connects devices to storage arrays in a SAN.

Failover – Failover is an operation that automatically switches data from a failed system to an operational system in the event that a system fails. In this case, "system" refers to the disks in the storage array.

Flash – Flash is a technology that uses a special type of transistor to isolate and hold an electrical charge long-term, thereby allowing non-volatile storage of electronic data without requiring moving parts.

Global Memory – Global memory is volatile memory that is shared by all of the components of the Symmetrix system (analogous to random access memory in a desktop computer).

LCC – LCCs provide several services for disk drives, including data connectivity, environmental monitoring, failover control, drive detection, and other functions related to drive control and reliability.

NAS – A system that provides storage to devices on a network.

Pool – A group of one or more logical disks.

RAID – A technology that copies redundant data across an array of disks. This technique preserves data stored in a RAID in case one or more (depending on RAID type) of the drives in a RAID fails.

Raw – The term "raw" refers to the total storage capacity offered by the disks within Symmetrix. After users apply RAID and the Symmetrix claims a small portion of the space for its own use, the drives will offer less total storage capacity.

SAN – A SAN is a network architecture that allows remote storage to appear local to devices accessing that storage.

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

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