EMC Corporation
EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC® Solutions Enabler 6.3

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 1.0

Prepared for:	Prepared by:
EMC Corporation 176 South Street Hopkinton, MA 01748 Phone: (508) 435-1000 http://www.emc.com	**Corsec Security, Inc.** 10340 Democracy Lane, Suite 201 Fairfax, VA 22030 Phone: (703) 267-6050 http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
1.0	2007-10-30	Nathan Lee	Initial release.

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Target of Evaluation is the EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3, and will hereafter be referred to as the Symmetrix or the TOE throughout this document. The TOE is software which runs on a mid- to high-end data storage array that is designed to operate within a Storage Area Network (SAN) or to be directly connected to a server (direct- or SAN-attached will henceforth be referred to as "Symmetrix storage connectivity").

1.1 Purpose

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

- Security Target Introduction (Section 1) – Provides a brief summary of the content of the ST and describes the organization of other sections of this document.
- TOE Description (Section 2) – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- Security Environment (Section 3) – Describes the threats 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.
- Security Requirements (Section 5) – Presents the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE and by the TOE's environment.
- TOE Summary Specification (Section 6) – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- Protection Profile Claims (Section 7) – Provides the identification of any ST Protection Profile claims as well as a justification to support such claims.
- Rationale (Section 8) – Presents the rationale for the security objectives, security requirements, and the TOE summary specification as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target, TOE and CC Identification and Conformance

Table 1 - ST, TOE, and CC Identification and Conformance

ST Title	EMC Corporation EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC® Solutions Enabler 6.3 Security Target
ST Version	Version 1.0
Author	Corsec Security, Inc. Nathan Lee and Matthew Appler
TOE Identification	EMC® Symmetrix® Access Control, Enginuity™ 5771.100.108 with EMC Solutions Enabler 6.3.0
Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 (aligned with ISO/IEC 15408:2005); CC Part 2 conformant; CC Part 3 conformant; Parts 2 and 3 Interpretations from the Interpreted CEM as of July 5, 2006 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+: EAL2 Augmented with ALC_FLR.1 Basic flaw remediation

Keywords	Storage Area Network (SAN), storage array, data storage

1.3 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 several operations to be performed on security requirements: assignment, refinement, selection and iteration. These operations are presented in the same manner in which they appear in Parts 2 and 3 of the CC with the following exceptions:

- 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.
- Iterations are identified by appending a letter in parenthesis following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

1.4 Terminology

Throughout this document the terms "application server", "server", and "host" are used interchangeably. These terms are used to describe any computer (excluding the Solutions Enabler Management Computer and the EMC ControlCenter Agent) that utilizes the storage environment provided by the TOE.

2 TOE Description

This section provides a general overview of the TOE as an aid to understanding the general capabilities and security functions provided by the TOE. The TOE description provides a context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Product Type

The TOE is the software portion of the Symmetrix DMX-3, a storage device designed to provide managed storage in a Symmetrix storage connectivity environment (which includes a SAN). The purpose of a SAN is to allow many different application servers (also referred to as “hosts”) to share storage provided by centrally managed storage devices. The TOE allows an organization to manage its storage needs separately from its application servers. This allows greater control over storage allocation, fault tolerance, and backups versus storage that is directly attached to individual application servers.

In a typical deployment scenario, individual application servers are attached to the Symmetrix either directly or via a SAN through a Fibre Channel switch. These application servers are then configured to use storage on the Symmetrix, in the form of Logical Units (LUNs), as storage for their applications. Symmetrix storage can also be used through an EMC Celerra to provide Network Attached Storage (NAS) for traditional Internet Protocol (IP)-based clients. The TOE is primarily administered via the Solutions Enabler software running on an attached management computer. Optionally, the TOE can also be administered via the separate EMC ControlCenter management software suite; however, administration via EMC ControlCenter is not included in the evaluated configuration of the TOE.

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

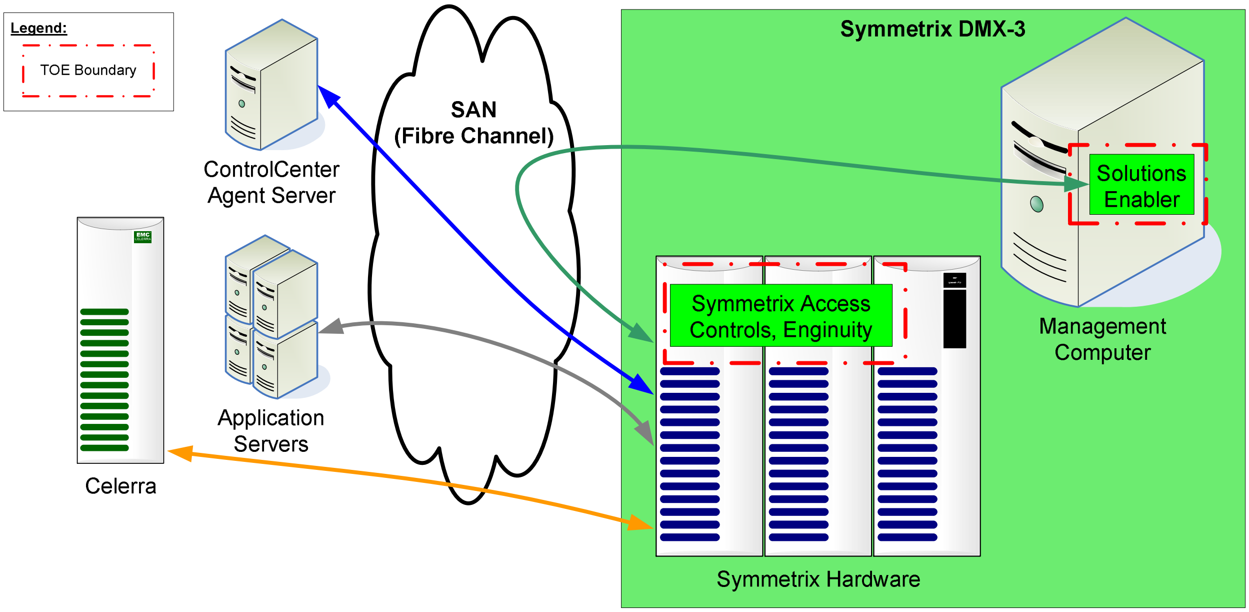

Figure 1 - Deployment Configuration of the TOE

2.2 Product Description

The Symmetrix provides direct-attached and SAN-attached storage to configured servers. The Symmetrix provides the ability to combine several individual drives into useful logical groups, provides fault tolerance for stored data, and manages access to the data that it stores. The Symmetrix accomplishes this through custom-built hardware and software. The Symmetrix is designed to allow customers to scale both system performance and storage capacity. Symmetrix Access Control provides granular control over management of LUNs on the Symmetrix.

2.2.1 Symmetrix Concepts

The Symmetrix comprises blades (also called "Directors") that connect to servers and other blades that connect to disk drives. Both of these blade types provide the processing power for operation as a disk array. There may be additional bays containing additional disk drives. The storage capability provided by these disk drives is divided into numerous LUNs and presented for use by hosts. The control blades provide the authorized administrator with the ability to manage the Symmetrix and to establish LUNs.

Storage is presented to the server in the form of a LUN. Each LUN represents a unit of storage to an application server, analogous to a local disk drive. However, the LUN provided by the Symmetrix is not necessarily a single physical disk; rather, a typical deployment would have a physical disk divided into up to 255 partitions. These partitions, called "hyper volumes," can be configured to form a logical LUN in a RAID[1] configuration, or collections of small 'hypers' in 'striped' configurations can be configured for high performance applications. The system offers tremendous flexibility in presenting storage to a server as a LUN (often referred to as a Symmetrix "Device" in other EMC product literature).

The Symmetrix supports a variety of disk types and capacities. Devices can be configured by an administrator with various attributes, such as which RAID level to provide. In this manner, an administrator can manage the Symmetrix through successive levels of abstraction.

Symmetrix Access Control provides administrators of the Symmetrix with the ability to restrict the management of LUNs on the Symmetrix. Since the Symmetrix is intended to be deployed in a highly secure datacenter staffed by competent and trusted administrators, the standard Symmetrix product will allow any host running the Symmetrix Management Console software to configure and manage any LUN on the Symmetrix. Although this is the preferred mode of operation in many Symmetrix environments, some customers wish to restrict LUN management rights to only certain hosts on the SAN. Symmetrix Access Control utilizes the EMC Solutions Enabler software to enforce these management restrictions by assigning management rights to hosts with specific unique identifiers.

2.3 TOE Boundaries and Scope

This section will primarily address what physical and logical components of the TOE are included in evaluation.

2.3.1 Physical Boundary

Figure 1 above 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 software-only TOE comprises custom-built software that runs on Symmetrix DMX-3 hardware and a custom-built software application which runs on a standard PC running a Windows operating system (Microsoft Windows 2000 SP4, Microsoft Windows Server 2003; SP1, R2, or Microsoft Windows Server 2003 (Itanium); SP1) or Sun Solaris 10 (Sun OS 5.10).

[1] RAID: Redundant Array of Independent/Inexpensive Disks

2.3.1.1 TOE Environment

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

The TOE provides LUN configuration access control. For this to operate correctly, the unique server Access Control identifier that is provided to the TOE must be accurate and must not be spoofed. The TOE Environment is required to provide this.

2.3.2 Logical Boundary

The security functions implemented by the TOE are usefully grouped under the following Security Function Classes:

- User Data Protection
- Security Management
- Protection of the TSF

2.3.2.1 User Data Protection

The User Data Protection function implements functionality necessary to protect User Data which is entrusted to the TOE. The TOE protects user data primarily in three ways. First, it ensures that only the application servers that have been granted access to a LUN have access to that LUN. Second, it ensures that only authorized hosts can configure LUNs. Third, it ensures the integrity of the data entrusted to it through its use of RAID levels.

2.3.2.2 Security Management

The Security Management function provides administrators with the ability to properly manage and configure the TOE to store user data. Administrative hosts are assigned to Access Control Groups which have rights that govern which LUNs they are authorized to configure.

2.3.2.3 Protection of the TSF

The Protection of the TSF function provides the integrity and management of the mechanisms that protects the TSF. The security functions in this evaluation are impractical to bypass because the TOE is designed in such a way that no access is possible without passing through key TOE security features, such as identification and authentication and access control mediation. The TOE maintains its own domain for execution and does not share any hardware with other applications.

2.3.3 Physical/Logical Features and Functionality Not Included in the Evaluated Configuration of the TOE

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

- Management via EMC ControlCenter product
- Symmetrix Service Processor (a component of the Symmetrix which is only used during initial configuration)

3 Security Environment

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:

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

3.1 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 2 – 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 and TOE users are non-hostile, appropriately trained, and follow all administrator guidance.
A.PHYSICAL	Physical security will be provided for the TOE and its environment.

3.2 Threats to Security

This section identifies the threats to the information technology (IT) assets against which the TOE must protect. The threat agents are individuals who are not authorized to use the TOE. 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/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)

The following threats are applicable:

Table 3 – Threats

Name	Description
T.DATA_CORRUPTION	User data and configuration 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 be used by Users of the TOE or attackers to access or modify configuration data that it was not intended to access by bypassing the protection mechanisms of the TOE.

3.3 Organizational Security Policies

There are no Organizational Security Policies.

4 Security Objectives

This section identifies the security objectives for the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the TOE's security needs.

4.1 Security Objectives for the TOE

The specific security objectives are as follows:

Table 4 – TOE Security Objectives

Name	Description
O.ADMIN	The TOE must provide a method for administrative control of the TOE.
O.BYPASS	The TOE must ensure that the TSF cannot be bypassed.
O.PROTECT	The TOE must protect configuration data that it has been entrusted to protect.

4.2 Security Objectives for the Environment

4.2.1 IT Security Objectives

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

Table 5 – Security Objectives for the TOE Environment

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 Storage Area Network
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.

4.2.2 Non-IT Security Objectives

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

Table 6 – 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 non-hostile, appropriately trained and follow all administrator guidance.
OE.PHYSICAL	The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.

5 Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE as well as SFRs met by the TOE IT environment. These requirements are presented following the conventions identified in Section 1.3.

5.1 TOE Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 7 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 7 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓	✓	
FDP_SDI.2	Stored data integrity		✓	✓	
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_RVM.1	Non-bypassability of the TSP				
FPT_SEP.1	TSF domain separation				

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

Section 5.1 contains the functional components from Part 2 of the CC with the operations completed. For the conventions used in performing CC operations please refer to Section 1.3.

5.1.1 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1

The TSF shall enforce the [*Discretionary Access Control SFP*] on [

- *Subjects: external host Access Control Groups*
- *Objects: LUNs*
- *Operations: configure/manage*

].

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1

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

- *Subjects: external host Access Control Groups*
  - *Security Attributes:*
    - *Unique server Access Control identifier*
    - *Access Control Group rights*
- *Objects: LUNs*
  - *Security Attributes:*
    - *LUN ID*
    - *Access Control Group rights*

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*an external host can configure a LUN if the host's Access Control Group has appropriate rights on the LUN's LUN ID*].

FDP_ACF.1.3

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

FDP_ACF.1.4

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_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1

FDP_SDI.2.1

The TSF shall monitor user data stored within the TSC for [*integrity errors*] on all **user data** ~~objects~~, based on the following attributes: [*Mirroring for RAID 1; Parity data for RAID 5 ((3+1) and (7+1)), and RAID 10*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [*reconstruct the user data (except for RAID 0) and notify the authorized administrator*].

Dependencies: No dependencies

5.1.2 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1

The TSF shall enforce the [*Discretionary Access Control SFP*] to restrict the ability to [*modify, delete*] the security attributes [*Access Control Group rights, Unique server Access Control identifier, LUN ID*] to [*the authorized administrator*].

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1

The TSF shall enforce the [*Discretionary Access Control SFP*] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.[2]

FMT_MSA.3.2

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

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

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*modify, delete*] the [*configuration data*] to [*the authorized administrator*].

[2] In order to maintain compatibility with legacy applications and servers, the Symmetrix is delivered to the customer with a default configuration which grants all unregistered hosts full access to all of the Symmetrix storage devices.

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

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

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

- *Management of all TSF data*
- *Management of all 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 [

- *authorized administrator*
- *authorized host*[3]
- *unknown host*[4]

].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

[3] An authorized host is a host which is registered as a member of an Access Control Group.

[4] An unknown host is a host which is not registered as an explicit member of any Access Control Group and thus falls under the control of the UnknwGrp (the “unknown host group”).

5.1.3 Class FPT: Protection of the TSF

FPT_RVM.1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies

FPT_SEP.1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies

5.2 Security Functional Requirements on the IT Environment

This section specifies the SFRs for the TOE's IT environment. This section organizes the SFRs by CC class. Table 8 identifies all SFRs implemented by the TOE's IT environment and indicates the ST operations performed on each requirement.

Table 8 - IT Environment Security Functional Requirements

Name	Description	S	A	R	I
FIA_UAU.2	User authentication before any action			✓	
FIA_UID.2	User identification before any action			✓	
FPT_ITT.1	Basic internal TSF data transfer protection	✓		✓	

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

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1

The ~~TSF~~ **IT Environment** shall require each user to be successfully authenticated before allowing any ~~other~~ TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

FIA_UID.2.1

The ~~TSF~~ **IT Environment** shall require each user to identify itself before allowing any ~~other~~ TSF-mediated actions on behalf of that user.

Dependencies: No dependencies

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

FPT_ITT.1.1

The ~~TSF~~ **IT Environment** shall protect TSF data from [*modification*] when it is transmitted between separate parts of the TOE.

Dependencies: No dependencies

5.3 Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from Part 3 of the CC at EAL2+ augmented with ALC_FLR.1. Table 9 – Assurance Requirements summarizes the requirements.

Table 9 – Assurance Requirements

Assurance Requirements	
Class ACM: Configuration management	ACM_CAP.2 Configuration items
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Flaw Remediation	ALC_FLR.1 Basic flaw remediation
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_VLA.1 Developer vulnerability analysis

6 TOE Summary Specification

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

6.1 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 are suitable to satisfy the necessary requirements.

Table 10 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Protection of TOE Security Functions	FPT_RVM.1	Non-bypassability of the TSP
	FPT_SEP.1	TSF domain separation
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_SDI.2	Stored data integrity

6.1.1 User Data Protection

The TOE provides the User Data Protection security function to manage LUN access by enforcing the Discretionary Access Control SFP and configuration by SAN hosts. The purpose of SAN-attached storage is to allow high speed, scalable, fault-tolerant storage separate from individual application servers. The TOE provides this functionality for connected servers. The Discretionary Access Control SFP is defined below.

> Discretionary Access Control SFP: The Discretionary Access Control SFP is enforced on external hosts Access Control Groups attempting to configure or manage LUNs. External hosts are identified by unique server Access Control identifiers and LUN are identified by LUN IDs. External hosts are members of Access Control Groups which are granted rights to LUNs. If an external host's Access Control Group has the appropriate rights to a LUN ID, that host is able to configure or manage that LUN.

Using the Security Management security function, Administrators of the TOE can configure LUNs to provide storage to hosts (typically application servers). These hosts are then placed into Access Control Groups, which allows an Administrator to provide different levels of LUN configuration rights to one or more SAN hosts. When a host requests configuration access to a LUN, the TOE Environment provides a unique identifier for the host. The TOE then determines whether or not to grant that host configuration access to the LUN. With each successive request to configure a LUN, the TOE ensures that only authorized hosts may configure the LUN.

The TOE also provides for the integrity of user data. When creating RAID Groups from individual disk drives, an Administrator can configure storage as RAID levels 0[5], 1, 5, or 10. 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 (except for RAID 0). Additionally, Administrators can configure "hot spare" or "Global Spare" disk drives. When a drive failure is detected, the drive that has failed will automatically be recreated on a "spare". The two forms of spare work in the following way; a "Global Spare" takes on the role of the failed drive permanently, and when the failed drive is replaced, that replacement drive becomes a member of the Global Spare pool. When a "hot spare" is used, the system automatically copies the data off the hot spare and onto the replacement drive (when one is assigned) and the hot spare returns to the pool of available hot spare drives. All changes in LUN identifiers, RAID relationships, *etc.* are handled automatically by the TOE. These processes all occur while real-time access to user data continues.

6.1.2 Security Management

The purpose of the TOE is to provide a storage system to application servers attached to a Symmetrix. The TOE provides mechanisms to govern which hosts can configure which LUNs. The Security Management function allows Administrators to properly configure this functionality.

The TOE maintains three roles: "authorized administrator", "authorized host", and "unknown host". Hosts that are authorized to administer the Symmetrix are assigned the "authorized administrator" role. Hosts that are part of an Access Control Group are assigned the "authorized host" role. Hosts that are not explicit members of an Access Control Group are assigned the "unknown host" role (via their default membership in the "UnknwGrp" group).

Management of the TOE occurs through the Solutions Enabler Command Line Interface. Numerous granular rights can be assigned to any particular host running the Symmetrix Management Console, and only those rights explicitly granted to a host can be exercised by an authorized administrator using the SMC from that host.

6.1.3 Protection of the TSF

Protection of the TSF provides for the integrity of the mechanisms that protect the TOE. The TOE comprises two main components: one is software and firmware which runs on a custom-built hardware appliance which does not share memory or processors with any other application or system[6]; the other is a software application (Solutions Enabler) which runs on a standard PC running a Windows operating system. The TOE maintains its own domain for its execution. Interfacing with the TOE is only done through well defined interfaces, each utilizing security

[5] When Raid 0 is used, the TOE does not provide integrity of user data. Raid 0 is provided for situations where the benefit provided by integrity checking does not balance the loss of storage space required to store integrity data.

[6] The hardware appliance is not included in the TOE boundary.

functions to maintain the security of that interface. The TOE relies on its environment to provide protection from physical tampering.

Non-bypassability of the TOE is provided through basic configuration and enforcement of the security mechanisms. All administrators of the TOE must be authenticated (via their access to an authorized host) prior to performing any security functionality. Once authenticated, administrators can only perform operations which their host has been explicitly granted permission to perform. The TOE uses unique session identifiers for each operator and maintains separation between concurrent operators.

6.2 TOE Security Assurance Measures

EAL2+ was chosen to provide a basic level of independently assured security. This section of the Security Target maps the assurance requirements of the TOE for a CC EAL2+ level of assurance to the assurance measures used for the development and maintenance of the TOE. The following table provides a mapping of the appropriate documentation to the TOE assurance requirements.

Table 11 - Assurance Measures Mapping to TOE Security Assurance Requirements (SARs)

Assurance Component	Assurance Measure
ACM_CAP.2	EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 - Configuration Management: Capabilities
ADO_DEL.1	EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 - Delivery and Operation: Secure Delivery
ADV_FSP.1	EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_HLD.1	EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
ADV_RCR.1	EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 - TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence
AGD_ADM.1	Numerous administrative guides are available on EMC’s Powerlink website.
AGD_USR.1	Numerous user guides are available on EMC’s Powerlink website.
ALC_FLR.1	EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 – Life Cycle Support: Flaw Remediation
ATE_COV.1	EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 – Tests: Coverage Functional Tests
ATE_FUN.1	EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 – Tests: Coverage Functional Tests
ATE_IND.2	Provided by laboratory evaluation
AVA_VLA.1	EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 - Vulnerability Assessment

7 Protection Profile Claims

This section provides the identification and justification for any Protection Profile conformance claims.

7.1 Protection Profile Reference

There are no protection profile claims for this security target.

8 Rationale

This section provides the rationale for the selection of the security requirements, objectives, assumptions, and threats. In particular, it shows that the security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

8.1 Security Objectives Rationale

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the Security Target. The following tables demonstrate the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption and threat.

8.1.1 Security Objectives Rationale Relating to Threats

Table 12 – Security Objectives Rationale Relating to Threats

Threats	Objectives	Rationale
T.DATA_CORRUPTION User data and configuration 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 supports the mitigation of this threat by allowing an administrator to properly configure the mechanisms of the TOE designed to mitigate this threat.
	O.BYPASS The TOE must ensure that the TSF cannot be bypassed.	The objective O.BYPASS ensures that the protection mechanisms of the TOE designed to mitigate this threat cannot be bypassed.
	O.PROTECT The TOE must protect configuration data that it has been entrusted to protect.	O.PROTECT mitigates this threat by providing mechanisms to protect the configuration data that has been entrusted to the TOE.
T.IMPROPER_SERVER A system connected to the TOE could be used by Users of the TOE or attackers to access or modify configuration data that it was not intended to access.	O.ADMIN The TOE must provide a method for administrative control of the TOE.	O.ADMIN supports the mitigation of this threat by allowing an administrator to properly configure the mechanisms of the TOE designed to mitigate this threat.
	O.BYPASS The TOE must ensure that the TSF cannot be bypassed.	The objective O.BYPASS ensures that the protection mechanisms of the TOE designed to mitigate this threat cannot be bypassed.
	O.PROTECT The TOE must protect configuration	O.PROTECT ensures that the TOE provides adequate mechanisms to give only authorized servers access to

Threats	Objectives	Rationale
	data that it has been entrusted to protect.	the appropriately authorized configuration data.
	OE.PROPER_NAME_ASSIGNMENT The TOE environment must provide accurate unique server identifiers for each system that communicates with the TOE.	OE.PROPER_NAME_ASSIGNMENT ensures 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 Storage Area Network.	OE.SECURE_COMMUNICATIONS ensures that all communications with the TOE are untampered for administration of the TOE, internal TOE communications, and data sent to or from the TOE.
	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.

8.1.2 Security Objectives Rationale Relating to Assumptions

Table 13 – Security Objectives Rationale Relating to Assumptions

Assumptions	Objectives	Rationale
A.PHYSICAL Physical security will be provided for the TOE and its environment.	OE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by untrusted subjects.	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. OE.PHYSICAL satisfies this assumption.
A.MANAGE 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.	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. OE.MANAGE satisfies this assumption.

Assumptions	Objectives	Rationale
A.NOEVIL Administrators and TOE users are non-hostile, appropriately trained, and follow all administrator guidance.	OE.NOEVIL Sites using the TOE shall ensure that TOE administrators are non-hostile, appropriately trained and follow all administrator guidance.	Sites using the TOE ensure that administrators are non-hostile, appropriately trained, and follow all administrator guidance. OE.NOEVIL satisfies this assumption.

8.2 Security Functional Requirements Rationale

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

8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 14 – SFR Rationale Related to TOE Objectives

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must provide a method for administrative control of the TOE.	FMT_MSA.1 Management of security attributes	Security attributes of the TOE can only be changed by authorized administrators. All administrative actions are mediated by the I&A functions implemented by the TOE environment.
	FMT_MSA.3 Static attribute initialisation	Permissive values for data access are provided, and the TOE administrator can change them when a data object is created. All administrative actions are mediated by the I&A functions implemented by the TOE environment.
	FMT_MTD.1 Management of TSF data	The ability to modify and delete configuration data is granted only to the authorized administrator.
	FMT_SMF.1 Specification of management functions	FMT_SMF specifies each of the management functions that are utilized to securely manage the TOE. These functions are provided by the Solutions Enabler.
	FMT_SMR.1 Security roles	Specific roles are defined to govern management of the TOE. All administrative actions are mediated by the I&A functions implemented by the TOE environment.

Objective	Requirements Addressing the Objective	Rationale
O.BYPASS The TOE must ensure that the TSF cannot be bypassed.	FPT_RVM.1 Non-bypassability of the TSP	The TOE ensures that policy enforcement functions are invoked and succeed before each function is allowed to proceed.
	FPT_SEP.1 TSF domain separation	The TOE maintains a security domain for its execution that protects it from interference and tampering.
O.PROTECT The TOE must protect configuration data that it has been entrusted to protect.	FDP_ACC.1 Subset access control	The TOE has an access control policy which ensures that only authorized servers gain access to configuration data within the TOE.
	FDP_ACF.1 Security attribute based access control	The TOE provides access control functionality to manage access to configuration data within the TOE.
	FDP_SDI.2 Stored data integrity	The TOE provides data integrity via the various RAID options it implements.

8.2.2 Rationale for Security Functional Requirements of the IT Environment

Table 15 – SFR Rationale Related to Objectives of the TOE Environment

Objective	Requirements Addressing the Objective	Rationale
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.	FIA_UAU.2 User authentication before any action	Users are not able to access the TOE until the environment has properly authenticated the user.
OE.PROPER_NAME_ASSIGNMENT The TOE environment must provide accurate unique server identifiers for each system that communicates with the TOE.	FIA_UID.2 User identification before any action	Users are not able to access the TOE until the environment has properly identified the user.
	FIA_UAU.2 User authentication before any action	Users are not able to access the TOE until the environment has properly authenticated the user.

Objective	Requirements Addressing the Objective	Rationale
OE.SECURE_COMMUNICATIONS The TOE environment must provide untampered communications between systems connected to the Storage Area Network.	FPT_ITT.1 Basic internal TSF data transfer protection	The TOE environment will provide an untampered network for communications between TOE components.

8.3 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 and hardware engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate for the threats defined for the environment. At EAL2+, the TOE will incur a search for obvious flaws to support its introduction into the non-hostile environment.

8.4 Rationale for Refinements of Security Functional Requirements

The following refinements of Security Functional Requirements from CC version 2.3 have been made to clarify the content of the SFRs, and make them easier to read:

- The words “no additional rules” were added to, and others stricken from, FDP_ACF.1.
- The word “objects” was changed to “user data” to specify more precisely what is protected with FDP_SDI.2.

8.5 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 16 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 16 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_SDI.2	No dependencies	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency.
FIA_UID.2	No dependencies	✓	
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1 and therefore satisfies this dependency.
FPT_RVM.1	No dependencies	✓	
FPT_SEP.1	No dependencies	✓	

8.6 TOE Summary Specification Rationale

8.6.1 TOE Summary Specification Rationale for the Security Functional Requirements

Each subsection in the TOE Summary Specification (Section 6) describes a security function of the TOE. These sets of security functions work together to satisfy all of the security requirements. Furthermore, all of the security functions are necessary in order for the TSF to meet the security functional requirements. This section, in conjunction with the TOE Summary Specification section, provides evidence that the security functions are suitable to fulfill the TOE security requirements.

Table 10 identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement).

8.6.2 TOE Summary Specification Rationale for the Security Assurance Requirements

EAL2+ was chosen to provide a basic level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated threat environment.

8.6.2.1 Configuration Management

The *EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 Configuration Management: Capabilities* documentation provides a description of tools used to control the configuration items and how they are used at the EMC. The documentation provides a complete configuration item list and a unique reference for each item. Additionally, the configuration management system is described including procedures that are used by developers to control and track changes that are made to the TOE. The documentation further details the TOE configuration items that are controlled by the configuration management system.

Corresponding CC Assurance Components:

- Configuration Items

8.6.2.2 Delivery and Operation

The *EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 Delivery and Operation: Secure Delivery* documentation provides a description of the secure delivery procedures implemented by EMC to protect against TOE modification during product delivery. The Installation Documentation provided by EMC details the procedures for installing the TOE and placing the TOE in a secure state offering the same protection properties as the master copy of the TOE. The Installation Documentation provides guidance to the administrator on the TOE configuration parameters and how they affect the TSF.

Corresponding CC Assurance Components:

- Delivery Procedures
- Installation, Generation and Start-Up Procedures

8.6.2.3 Development

The *EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 TOE Architecture: High Level Design, Functional Specification, and Representation Correspondence* design documentation consists of several related design documents that address the components of the TOE at different levels of abstraction. The following design documents address the Development Assurance Requirements:

- The Functional Specification provides a description of the security functions provided by the TOE and a description of the external interfaces to the TSF. The Functional Specification covers the purpose and method of use and a list of effects, exceptions, and errors message for each external TSF interface.
- The High-Level Design provides a top level design specification that refines the TSF functional specification into the major constituent parts (subsystems) of the TSF. The high-level design identifies the basic structure of the TSF, the major elements, a listing of all interfaces, and the purpose and method of use for each interface.

- The Correspondence Analysis demonstrates the correspondence between each of the TSF representations provided. This mapping is performed to show the functions traced from the ST description to the High-Level Design.

Corresponding CC Assurance Components:

- Informal Functional Specification
- Descriptive High-Level Design
- Informal Representation Correspondence

8.6.2.4 Guidance Documentation

The EMC Guidance documentation provides administrator and user guidance on how to securely operate the TOE. The Administrator Guidance provides descriptions of the security functions provided by the TOE. Additionally, it provides detailed accurate information on how to administer the TOE in a secure manner and how to effectively use the TSF privileges and protective functions. The User Guidance provided directs users on how to operate the TOE in a secure manner. Additionally, User Guidance explains the user-visible security functions and how they are to be used and explains the user's role in maintaining the TOE's Security. EMC provides single versions of documents which address the Administrator Guidance and User Guidance; there are not separate guidance documents specifically for non-administrator users of the TOE.

Corresponding CC Assurance Components:

- Administrator Guidance
- User Guidance

8.6.2.5 Life Cycle Support

The *EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 Life Cycle Support: Flaw Remediation* documentation describes the processes that EMC follows to capture, track, and correct flaws (or "bugs") that are found within the TOE. The documentation demonstrates that all discovered flaws are recorded and that the process ensures that flaws are tracked through their entire life cycle.

Corresponding CC Assurance Components:

- Basic Flaw Remediation

8.6.2.6 Tests

There are a number of components that make up the *EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 Tests: Coverage Functional Tests*. The Coverage Analysis demonstrates the testing performed against the functional specification. The Coverage Analysis demonstrates the extent to which the TOE security functions were tested as well as the level of detail to which the TOE was tested. EMC Test Plans and Test Procedures, which detail the overall efforts of the testing effort and break down the specific steps taken by a tester, are also provided.

Corresponding CC Assurance Components:

- Evidence of Coverage
- Functional Testing
- Independent Testing

8.6.2.7 Vulnerability Analyses

An *EMC® Symmetrix® Access Control, Enginuity™ 5771 with EMC Solutions Enabler 6.3 Vulnerability Assessment* document is provided to demonstrate ways in which an entity could violate the TSP and provide a list of identified vulnerabilities. Additionally, the document provides evidence of how the TOE is resistant to obvious attacks.

Corresponding CC Assurance Components:

- Vulnerability Analysis

8.7 Strength of Function

There is no Strength of Function claim because there are no security functions or security functional requirements which have probabilistic or permutational functions.

9 Acronyms

Table 17 - Acronyms

Acronym	Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
ID	Identifier/Identification
IP	Internet Protocol
IT	Information Technology
LUN	Logical Unit
OS	Operating System
RAID	Redundant Array of Independent/Inexpensive Disks
SAN	Storage Area Network
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy