DELL Technologies

PowerMax with PowerMaxOS 10

Security Target

Version 1.9

October 2023

Document prepared by

Lightship Security

www.lightshipsec.com

Document History

Version	Date	Description
0.1	April 14, 2022	Initial Doc Creation.
0.2	April 26 2022	Updates based on review
0.3	May 17 2022	Updated developer comments
1.0	May 26 2022	Addressed evaluator comments
1.1	October 14 2022	Updated Solution Enabler claims and TOE build number info.
1.2	December 20 2022	Updated TOE guidance references.
1.3	January 17 2023	Addressed CBORs.
1.4	February 22 2023	Addressed CBORs.
1.5	17 March 2023	Addressed ORs.
1.6	11 July 2023	Updated TOE version and guidance references.
1.7	18 September 2023	Addressed evaluator ORs.
1.8	17 October 2023	Addressed certifier ORs.
1.9	20 October 2023	Provided clarification on TOE versioning.

Table of Contents

List of Tables

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Dell Technologies PowerMax with PowerMaxOS 10 Solutions Enabler 10, and Unisphere for PowerMax 10 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 The TOE provides a platform for large scale storage operations, enabling organizations to grow, easily share, and cost effectively manage massive amounts of block storage.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Dell PowerMax with PowerMaxOS 10 Solutions Enabler 10.0, and Unisphere for PowerMax 10.0 Note: Only Unisphere for PowerMax contains a build identifier. The specific TOE versions are identified in Table 3.
Security Target	Dell Technologies PowerMax with PowerMaxOS 10 Security Target, v1.9

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 Release 5

b) CC Part 2 conformant

c) CC Part 3 conformant

1.4 Terminology

Table 2: Terminology

Term	Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality

2 TOE Description

2.1 Type

4 The TOE is a data storage device.

2.2 Usage

5 As shown in Figure 1, the TOE is a hardware and software solution that provides a platform for large scale storage operations, managing large amounts of block storage. The TOE is managed using the Solutions Enabler Command Line Interface (CLI), or the Unisphere for PowerMax Graphical User Interface (GUI).

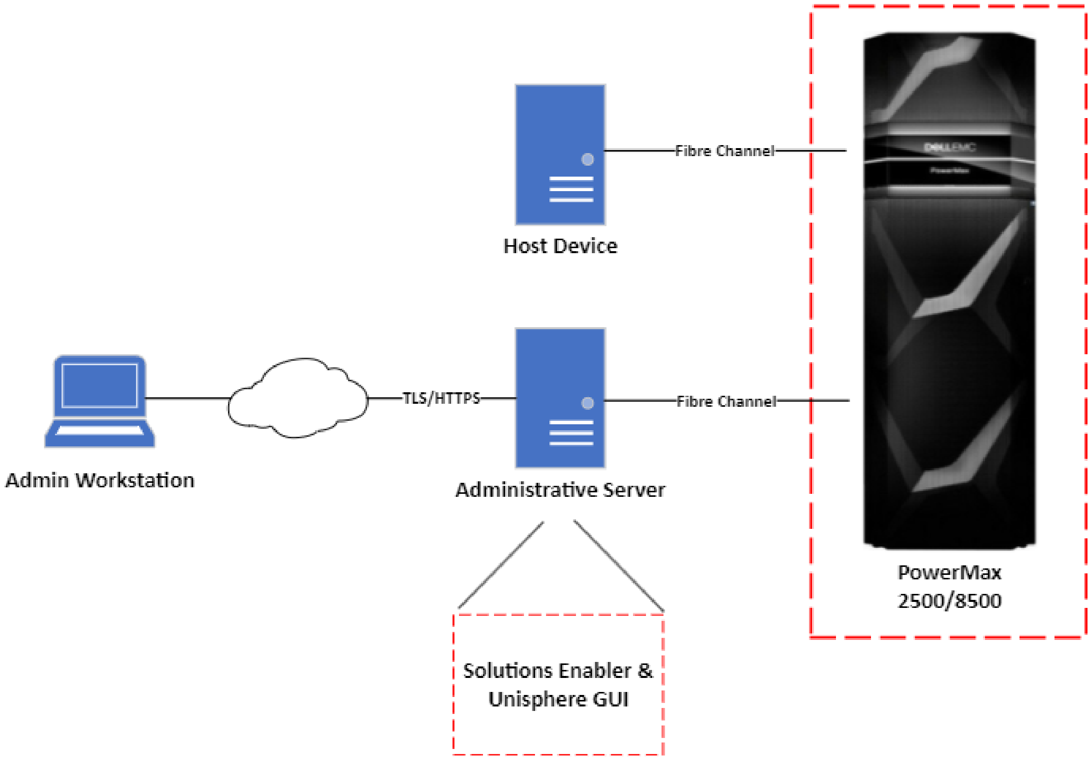

Figure 1: Example TOE deployment

2.3 Security Functions

6 The TOE provides the following security functions:

a) **Security Audit.** Audit entries are generated for security related events. The audit logs may be reviewed and filtered by authorized administrators.

b) **Cryptographic Operation.** The TOE provides for Data at Rest Encryption (D@RE) of information it has been entrusted to store.

c) **User Data Protection.** The TOE ensures that only authorized host devices may access stored data stored. It also ensures that residual information is inaccessible when storage resources are reassigned. RAID functionality protects from potential data loss due to integrity errors in the data.

d) **Identification & Authentication.** Administrative users must be identified and authenticated prior to being granted access to the TOE. Authentication information is obfuscated as it is entered.

e) **Security Management.** Management functions allow administrators to configure the attributes associated with the Block Storage Access Control SFP, perform user management, and to view audit logs. Security roles are provided to limit administrator access to a subset of the security management functions.

f) **Protection of the TSF.** Reliable timestamps are provided in support of audit record generation.

g) **Trusted Path/Channels.** Communications between the TOE and remote administrators are protected using TLSv1.2 (Unisphere GUI).

2.4 Physical Scope

7 The physical boundary of the TOE is the PowerMaxOS operating on the hardware appliances shown in the table below, Solutions Enabler and Unisphere GUI as shown in Table 3.

Table 3: TOE Hardware and Software

TOE Component	Description
Hardware	PowerMax 2500
	PowerMax 8500
Software	PowerMaxOS 10.0.1.2
	Unisphere for PowerMax 10.0.1.0 Build 5
	Solutions Enabler 10.0.1.1

2.4.1 TOE Delivery

8 The TOE software is installed on the TOE hardware and delivered to the customer by a commercial courier service with a package tracking system. The delivery is packaged with a CD ROM that contains the Solutions Enabler and Unisphere for PowerMax software.

2.4.2 Guidance Documents

9 The following guidance documentation is provided to customers online in Portable Document Format (PDF):

- Dell Solutions Enabler 10.0.0, Installation and Configuration Guide, July 2023

  https://dl.dell.com/content/manual47008612-dell-solutions-enabler-installation-and-configuration-guide.pdf?language=en-us&ps=true

- Dell Unisphere for PowerMax 10.0.0, Installation Guide, July 2022

  https://dl.dell.com/content/manual34878027-dell-unisphere-for-powermax-10-0-0-installation-guide.pdf?language=en-us&ps=true

- Dell Solutions Enabler, CLI Reference Guide, 10.0, July 2022

  https://dl.dell.com/content/manual29232065-dell-solutions-enabler-cli-reference-guide-10-0-0.pdf?language=en-us

- Dell PowerMax Family Security Configuration Guide, PowerMax OS, March 2023

  https://dl.dell.com/content/manual37372498-dell-powermax-family-security-configuration-guide-powermaxos-10.pdf?language=en-us

- Dell PowerMax Family Site Planning Guide, PowerMax 2500 and PowerMax 8500, October 2023

  https://dl.dell.com/content/manual49083949-dell-powermax-family-site-planning-guide-powermax-2500-and-powermax-8500.pdf?language=en-us&ps=true

- Dell Unisphere for PowerMax Product Guide, 10.0.0, March 2023

  https://dl.dell.com/content/manual34945916-dell-unisphere-for-powermax-10-0-0-product-guide.pdf?language=en-us&ps=true

10 The following guidance is provided to customers in HMTL format:

- Dell Unisphere for PowerMax, Online Help, 10.0.0

  Note: Online Help is delivered to customers as a .zip file available at: https://supportkb.dell.com/attachment/ka06P000000Y27hQAC/Unisphere%20for%20PowerMax%20Online%20Help10.0.0_pkb_en_US_1.zip. Customers must download and extract the file, and then double-click the index.html file to start and view the Online Help application.

11 The TOE also includes the following Common Criteria Guide, provided as a PDF, and available to customers upon request:

- Dell_PowerMax_EAL2_AGD_1.5.pdf

2.4.3 Non-TOE Components

12 The TOE operates with the following components in the environment:

a) **Administrative Server**. The TOE makes use of an administrative server to host the Solutions Enabler and Unisphere for PowerMax. Windows Server 2019 is the host OS used in the evaluated configuration.

b) **Admin Workstation.** Workstation required to access and manage the TOE. Windows 10 is the host OS in the evaluated configuration.

c) **Host Device.** The TOE makes use of a SAN-connected block storage host device.

2.5 Logical Scope

13 The logical scope of the TOE comprises the security functions defined in section 2.3.

2.6 Excluded Functionality and Interfaces

14 The following functions have not been evaluated:

a) Multi-factor authentication

b) End-to-end Efficient Encryption

15 The TOE supports the use of a REST API for developers. Administrators must create and assign user roles explicitly enabling access to the REST API functionality. The REST API is not used in the evaluated configuration, nor does it support any TOE management functionality.

16 The TOE also supports Dell Secure Remote Service (SRS). SRS is a service that allows Dell to remotely monitor the TOE. This service runs through a distinct physical port and is not connected and not used in the evaluated configuration.

3 Security Problem Definition

3.1 Threats

Table 4: Threats

Identifier	Description
T.ACCESS	Access to storage data could be improperly granted to host devices which should not have access to it.
T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information or perform operations for which no access rights have been granted, via user error, system error, or other actions.
T.DATALOSS	An unauthorized user could gain access to data on a disk if the logical disk has been allocated to another subject.
T.UNDETECT	Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.
T.DISCLOSURE	A malicious user could expose data on the TOE due to weak encryption.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.

3.2 Assumptions

Table 5: Assumptions

Identifier	Description
A.AUTHENTICATE	The TOE will rely on the operating system in the environment for performing administrative user authentication for Solutions Enabler.
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical and logical access.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

3.3 Organizational Security Policies

Table 6: Organizational Security Policies

Identifier	Description
P.RAID	User data must be protected from loss due to disk failure.

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 7: Security Objectives for the Operational Environment

Identifier	Description
OE.ADMIN	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. There are an appropriate number of authorized administrators trained to maintain the TOE, including its security policies and practices. Authorized administrators are non-hostile and follow all administrator guidance.
OE.AUTHENTICATE	The operating system in the TOE environment must ensure that administrative users of Solutions Enabler are authenticated.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical and logical attack.

4.2 Objectives for the TOE

Table 8: Security Objectives

Identifier	Description
O.ACCESS	The TOE must protect the data that it has been entrusted to store from unauthorized access.
O.ADMIN	The TOE must provide functionality that enables an authorized administrator to manage TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.AUDIT	The TOE must provide a means of logging security related events. The audit records must be viewable, and users must be able to filter the records by date and user.
O.IDAUTH	The TOE must be able to ensure that administrative users are identified and authenticated prior to allowing access to administrative functions and TSF data.

Identifier	Description
O.INTEGRITY	The TOE must protect the data that it has been entrusted to store from integrity errors due to disk failure.
O.CRYPTO	The TOE must protect the confidentiality of data it has been entrusted to store using cryptographic functions.
O.PROTCOMMS	The TOE shall provide protected communication channels for remote administrators.
O.PROTECT	The TOE must protect against inadvertent access to data. The TOE must ensure that data is removed prior to reallocation of the resource.
O.TIME	The TOE must provide reliable timestamps.

5 Security Requirements

5.1 Conventions

17 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

5.2 Extended Components Definition

18 The TOE does not claim extended components.

5.3 Functional Requirements

Table 9: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_RIP.1	Subset residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FIA_UAU.2	User authentication before any action
FIA_UAU.7	Protected authentication feedback
FIA_UID.2	User identification before any action
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation

Requirement	Title
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_STM.1	Reliable time stamps
FTP_TRP.1	Trusted Path

5.3.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

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

c) *[modification of user roles, storage access configuration changes].*

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *additional details specified in the above table.*

FAU_SAR.1 Audit Review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*users in the role of Administrator, SecurityAdmin, StorageAdmin or Auditor*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.3 Selectable audit Review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*filtering*] of audit data based on [*date, username*].

5.3.2 Cryptographic support (FCS)

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES-XTS*] and cryptographic key sizes [*256*] that meet the following: [*FIPS 140-2*].

5.3.3 User Data Protection (FDP)

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Block Storage Access Control SFP*] on
[*Subjects: host devices*
Objects: storage objects
Operations: read from and write to storage].

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

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

FDP_ACF.1.1 The TSF shall enforce the [*Block Storage Access Control SFP*] to objects based on the following: [
Subjects: host devices
Subject attributes: initiator
Objects: storage objects
Object attributes: masking view (which includes the host name, port group and storage group)].

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

A host device can access storage objects if:

- *The masking view includes the host name associated with the host device attempting to access storage*
- *The host name is associated with a valid initiator for the host device attempting to access storage*
- *The masking view includes the storage group associated with the storage object being accessed by the host device*
- *The host device is connected (directly or through a SAN) to a port that is part of the port group included in the storage masking view*

].

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

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

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects: [*the storage array*].

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all objects, based on the following attributes: [*parity data for RAID 5 and RAID 6*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*reconstruct the user data and send a notification*].

5.3.4 Identification and Authentication (FIA)

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each **administrative** user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*obscured feedback in the form of asterisks*] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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

5.3.5 Security Management (FMT)

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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.1.1 The TSF shall enforce the [*Block Storage Access Control SFP*] to restrict the ability to [query, modify, delete, [*create*]] the security attributes [*masking view, including host name, port group and storage group*] to [*users in the Administrator and StorageAdmin roles*].

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

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

FMT_MSA.3.1 The TSF shall enforce the [*Block Storage Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*users in the Administrator and StorageAdmin roles*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [*perform the operations listed in Table 10*] the [*TSF data listed in Table 10*] to [*the roles listed in Table 10*].

Table 10: Security Management of TSF Data

TSF Data Type	Operations	Roles
User account information	Create Query Modify Delete	Administrator SecurityAdmin
Roles	Create Query Modify Delete	Administrator SecurityAdmin
Audit data	Query	Administrator SecurityAdmin Auditor
Storage Access	Create Query Modify Delete	Administrator StorageAdmin

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*manage storage access, manage users and roles, view audit records*].

FMT_SMR.1 Security Roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Administrator, SecurityAdmin, StorageAdmin, Auditor*].

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

5.3.6 Protection of the TSF (FPT)

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

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

5.3.7 Trusted path/channels (FTP)

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [remote administration].

5.4 Assurance Requirements

19 The TOE security assurance requirements are summarized in Table 11 commensurate with EAL2+ (ALC_FLR.2).

Table 11: Assurance Requirements

Assurance Class	Components	Description
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
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
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent Testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6 TOE Summary Specification

6.1 Security Function

20 This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements. Table 12 provides information on how the TOE satisfies the SFRs outlined in Section 5.

Table 12: Security Function SFRs

SFR	Fulfilment
FAU_GEN.1.1	The TOE generates audit records for startup and shutdown of the audit function, all administrator login attempts, and all administrator actions that result in a configuration change.
FAU_GEN.1.2	Audit records contain the date and time of the event, the type of event, subject identity (if applicable), and the outcome of the event (success or failure)
FAU_SAR.1.1	The TOE provides authorized users with the capability to read all audit information from the audit records.
FAU_SAR.1.2	The audit records are presented in a manner suitable for a user to interpret the information.
FAU_SAR.3.1	The TOE provides the ability to apply filtering of audit data based on date and username.
FCS_COP.1.1	Each TOE hardware appliance is deployed with a series of Samsung NVMe TCG Opal SSC SEDs providing for encryption and decryption of data at rest. D@RE is implemented using AES-256-XTS (CAVP #s: C1271 & C1292).
FDP_ACC.1.1	The TOE enforces Block Storage Access Control SFP on host devices, storage objects and reading and writing to storage.
FDP_ACF.1.1	The TOE enforces Block Storage Access Control SFP to objects based on host devices, an initiator attribute, storage objects, the masking view which includes host name, port group and storage group.

SFR	Fulfilment
FDP_ACF.1.2	The following rules are enforced to determine if an operation among controlled subjects and controlled objects is allowed: A host device can access storage objects if: • The masking view includes the host name associated with the host device attempting to access storage • The host name is associated with a valid initiator for the host device attempting to access storage • The masking view includes the storage group associated with the storage object being accessed by the host device The host device is connected (directly or through a SAN) to a port that is part of the port group included in the storage masking view
FDP_ACF.1.3	The TOE explicitly authorises access of subjects to objects based on no additional rules.
FDP_ACF.1.4	The TOE explicitly denies access of subjects to objects based on no additional rules.
FDP_RIP.1.1	The TOE ensures previous information content of a resource is made unavailable upon the deallocation of the resource from the storage array.
FDP_SDI.2.1	The TOE monitors users data stored in containers for integrity errors on all objects based on parity data for RAID 5 and RAID 6.
FDP_SDI.2.2	Upon detection of a data integrity error, user data is reconstructed and a notification sent.
FIA_UAU.2.1 FIA_UID.2.1	Users must be identified and authenticated prior to being granted access to security management functionality within the Solutions Enabler CLI or the Unisphere GUI. In the evaluated configuration, administrative users login directly to Unisphere using a username and password. Identification and authentication is performed by Unisphere for PowerMax. Solutions Enabler ensures that users are identified and authenticated prior to being granted access, but does not perform the authentication of users. Administrative users must be authenticated by the Windows operating system. The authenticated identity is then passed to Solutions Enabler and the user is granted access. Although any user with credentials on the Administrative host machine may be able to access Solutions Enabler, unless the user has been assigned one or more roles, the user will not be able to view any system information or perform any administrative functions.
FIA_UAU.7.1	The Unisphere GUI provides obscured feedback in the form of asterisks to the user while authentication is in progress.

SFR	Fulfilment
FMT_MSA.1.1	The TOE enforces Block Storage Access Control SFP to restrict the ability to query, modify, delete and create the security attributes masking view, including host name, port group and storage group, to users in Administrator and StorageAdmin roles. Note: The Auditor and SecurityAdmin roles have the ability to query masking views.
FMT_MSA.3.1	The TOE enforces Block Storage Access Control SFP to provide restrictive default values for security attributes.
FMT_MSA.3.2	The TOE allows users in Administrator and StorageAdmin roles to specify alternative values to override the default values when an object or information is created.
FMT_MTD.1.1	The TOE restricts the ability to perform operations to TSF data to specific roles as follows: Create, query, modify and delete operations can only be executed on “User account information” data by Administrator and SecurityAdmin roles. Create, query, modify and delete operations can only be executed on “Roles” data by Administrator and SecurityAdmin roles. Query operations can only be executed on “Audit data” by Administrator, SecurityAdmin, and Auditor roles. Create, query, modify and delete operations can only be executed on “Storage Access” data by Administrator and StorageAdmin roles.
FMT_SMF.1.1	The TOE is capable of performing the following management functions: manage storage access, manage users and roles, view audit records.
FMT_SMR.1.1	The TOE maintains Administrator, SecurityAdmin, StorageAdmin, Auditor roles.
FMT_SMR.1.2	The TOE associates users with roles.
FPT_STM.1.1	The TOE provides reliable time stamps. Time information is obtained from the TOE hardware.

SFR	Fulfilment
FTP_TRP.1	All communications with remote administrators via Unisphere are protected using TLSv1.2. The following cipher suites are supported in the evaluated configuration: • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256

7 Rationale

7.1 Security Objectives Rationale

21 Table 13 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 13: Security Objectives Mapping

	T.ACCESS	T.ACCOUNT	T.DATALOSS	T.UNDETECT	T.DISCLOSURE	T.EAVES	P.RAID	A.AUTHENTICATE	A.LOCATE	A.NOEVIL
O.ACCESS	X									
O.ADMIN	X	X		X						
O.AUDIT				X						
O.IDAUTH		X		X						
O.INTEGRITY							X			
O.CRYPTO					X					
O.PROTCOMMS						X				
O.PROTECT	X		X							
O.TIME				X						
OE.ADMIN										X
OE.AUTHENTICATE								X		
OE.PHYSICAL									X	

22 Table 14 provides the justification to show that the security objectives are suitable to address the security problem.

Table 14: Suitability of Security Objectives

Element	Justification
T.ACCESS	**O.ACCESS** mitigates this threat by allowing only authorized host devices access to protected data. **O.ADMIN** mitigates this threat by only allowing authorized administrators the ability to manage TOE access functions. **O.PROTECT** mitigates this threat by ensuring that data is removed prior to reallocation of a disk.
T.ACCOUNT	**O.ADMIN** mitigates this threat by ensuring that access to the security management functions of the TOE are restricted to authorized administrators. **O.IDAUTH** mitigates this threat by ensuring that all authorized administrators are identified and authenticated prior to gaining access to the TOE security management functions..
T.DATALOSS	**O.PROTECT** mitigates this threat by providing removal of data on reallocation of the resource.
T.UNDETECT	**O.ADMIN** mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized administrators. **O.AUDIT** counters this threat by ensuring that the TOE maintains a record of all management functions performed on the TOE. **O.IDAUTH** mitigates this threat by ensuring that all administrative users are identified and authenticated prior to gaining access to the TOE security management functions. **O.TIME** mitigates this threat by providing reliable timestamps for use with the audit records, thereby ensuring an accurate accounting of security related events.
T.DISCLOSURE	**O.CRYPTO** mitigates this threat by protecting the confidentiality of data using cryptographic functions.
T.EAVES	**O.PROTCOMMS** mitigates this threat as it requires the TOE to encrypt communications with remote administrators.
A.AUTHENTICATE	**OE.AUTHENTICATE** supports this assumption by ensuring that administrative users of Solutions Enabler are authenticated.
A.LOCATE	**OE.PHYSICAL** supports this assumption by protecting the TOE from physical attack.
A.NOEVIL	**OE.ADMIN** supports this assumption by ensuring that the administrators managing the TOE have been specifically chosen to be careful, attentive and non-hostile.

Element	Justification
P.RAID	**O.INTEGRITY** supports this policy by ensuring that the TOE provides the ability to protect data in the case of disk failure.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

23 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices with the addition of ALC_FLR.2 to provide assurance that any identified security flaws will be addressed.

7.2.2 SFR Rationale

Table 15: Security Requirements Mapping

	O.ACCESS	O.ADMIN	O.AUDIT	O.IDAUTH	O.INTEGRITY	O.CRYPTO	O.PROTCOMMS	O.PROTECT	O.TIME
FAU_GEN.1			X						
FAU_SAR.1			X						
FAU_SAR.3			X						
FCS_COP.1						X			
FDP_ACC.1	X								
FDP_ACF.1	X								
FDP_RIP.1								X	
FDP_SDI.2					X				
FIA_UAU.2				X					
FIA_UAU.7		X		X					
FIA_UID.2				X					
FMT_MSA.1		X							

	O.ACCESS	O.ADMIN	O.AUDIT	O.IDAUTH	O.INTEGRITY	O.CRYPTO	O.PROTCOMMS	O.PROTECT	O.TIME
FMT_MSA.3		X							
FMT_MTD.1		X							
FMT_SMF.1		X							
FMT_SMR.1		X							
FPT_STM.1			X						X
FTP_TRP.1							X		

Table 16: Suitability of SFRs

Objectives	**SFRs**
O.ACCESS	**FDP_ACC.1 and FDP_ACF.1** support this objective by identifying the rules and attributes of the Block Storage Access Control SFP, which are used to control host device access to data stored on the TOE.
O.ADMIN	**FIA_UAU.7** supports this objective by preventing the inadvertent viewing of passwords, thereby reducing the risk of unauthorized users accessing TOE security functions. **FMT_MSA.1 and FMT_MSA.3** support this objective by providing restrictions on access to the attributes that configure the Block Storage Access Control SFP. **FMT_MTD.1** supports this objective by providing controls on the access to TSF data that is used to enforce security functions. **FMT_SMF.1** meets this objective by providing the management functions to securely manage the TOE. **FMT_SMR.1** supports this objective by ensuring that specific roles are defined to govern management of the TOE.

Objectives	SFRs
O.AUDIT	**FAU_GEN.1** outlines what data must be included in audit records and what events must be audited. **FAU_SAR.1** provides the means to review audit records. **FAU_SAR.3** provides the ability to filter the records by date or user. **FPT_STM.1** provides reliable time stamps in support of audit records.
O.IDAUTH	**FIA_UAU.2** meets this objective by ensuring that TOE Administrators are successfully authenticated before gaining access to TOE functions and data. **FIA_UAU.7** supports this objective by protecting the passwords used to gain administrative access from accidental disclosure, thereby reducing the risk of an unauthorized user gaining access to administrative functions and TSF data. **FIA_UID.2** supports this objective by ensuring that the identity of each TOE Administrator is known before allowing access to TOE functions and data.
O.INTEGRITY	**FDP_SDI.2** meets this objective by providing the RAID functionality that protects against integrity errors due to a hardware fault.
O.CRYPTO	**FCS_COP.1** supports this objective by providing cryptographic operations that secure data stored on the TOE.
O.PROTCOMMS	**FTP_TRP.1** requires encrypted communications for remote administration.
O.PROTECT	**FDP_RIP.1** supports this objective by ensuring that the content of the storage array is cleared on deallocation of the resource.
O.TIME	**FPT_STM.1** satisfies this objective by providing reliable time stamps.

Table 17: Dependency Rationale

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met
FAU_SAR.1	FAU_GEN.1	Met
FAU_SAR.3	FAU_SAR.1	Met
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Not met, as it is not required to be met by CCCS policy.
	FCS_CKM.4	
FDP_ACC.1	FDP_ACF.1	Met

SFR	Dependency	Rationale
FDP_ACF.1	FDP_ACC.1	Met
	FMT_MSA.3	Met
FDP_RIP.1	None	-
FDP_SDI.2	None	-
FIA_UAU.2	FIA_UID.1	Met, FIA_UID.2 is hierarchical to FIA_UID.1
FIA_UAU.7	FIA_UAU.1	Met, FIA_UAU.2 is hierarchical to FIA_UAU.1
FIA_UID.2	None	-
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Met by FDP_ACC.1
	FMT_SMR.1	Met
	FMT_SMF.1	Met
FMT_MSA.3	FMT_MSA.1	Met
	FMT_SMR.1	Met
FMT_MTD.1	FMT_SMR.1	Met
	FMT_SMF.1	Met
FMT_SMF.1	None	-
FMT_SMR.1	FIA_UID.1	Met, FIA_UID.2 is hierarchical to FIA_UID.1
FPT_STM.1	None	-
FTP_TRP.1	None	-