Dell EMC™ Data Domain® 7.2

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2160-000-D102
Version: 1.17
26 September 2022

Dell EMC
176 South Street
Hopkinton, MA, USA
01748

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J 7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8 Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	Dell EMC™ Data Domain® 7.2 Security Target
ST Version:	1.16
ST Date:	25 August 2022

1.3 TOE REFERENCE

TOE Identification:	Dell EMC™ Data Domain® 7.2 version 7.2.0.95-692608
TOE Developer:	Dell EMC
TOE Type:	Disaster Recovery

1.4 TOE OVERVIEW

The TOE is a series of disk-based inline deduplication appliances and gateways that optimize disaster recovery (DR) in the enterprise environment. These devices, known as Dell EMC Data Domain appliances, vary in storage capacity and data throughput.

Data Domain deduplication technology seamlessly integrates into existing Information Technology (IT) storage infrastructures. It eliminates redundant data from each backup image and stores only unique data, thus reducing the amount of physical storage required for backup.

To a backup server, the Data Domain system appears as a file server. Multiple backup servers can share one Data Domain system which is capable of handling multiple simultaneous backup and restore operations.

All systems run the Data Domain Operating System (DDOS). DDOS provides secure administration for TOE configuration, management, and monitoring via command-line interface (CLI) or the Data Domain System Manager (DD System Manager) graphical user interface (GUI). Use of both the CLI and GUI, as well as system events, is audited.

To protect against data loss from software and hardware failures, the Data Domain systems are setup in a double parity RAID 6 (Redundant Array of Independent Disks) configuration and use NVRAM (Non-Volatile Random Access Memory) to keep data synchronized during a hardware or power failure. All data stored on the TOE is compressed, deduplicated and encrypted during transfer. Encrypted data requested from the Data Domain system is decrypted as it is being read from disk.

The DD6900, DD9400, and DD9900 appliances are being evaluated but Dell also supports the DD3300 appliance.

The TOE is a software and hardware TOE.

1.4.1 TOE Environment

The following hardware and networking components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Local Management Workstation	General purpose computing platform running CentOS 7.6 and supports	Local Management Workstation

Component	Operating System	Hardware
	VT100 emulation.	
Remote Management Workstation	General purpose computing platform running 64-bit Windows 10.	Remote Management Workstation
Windows Authentication Server	General purpose computing platform running Windows Server 2016 with Active Directory.	Windows Authentication Server
DD Boost Backup Server	SUSE 12 hosting NetBackup 8.1 with DD BOOST 3.5.0.2 plugin is used for this evaluation.	DD Boost Backup Server

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE consists of the hardware and software described in Table 2. Figure 1 illustrates the TOE in its evaluated configuration:

TOE Component	Description
Hardware Appliance	DD6900, DD9400, and DD9900
Software	DDOS (Data Domain Operating System) version 7.2.0.95-692608

Table 2 - TOE Components

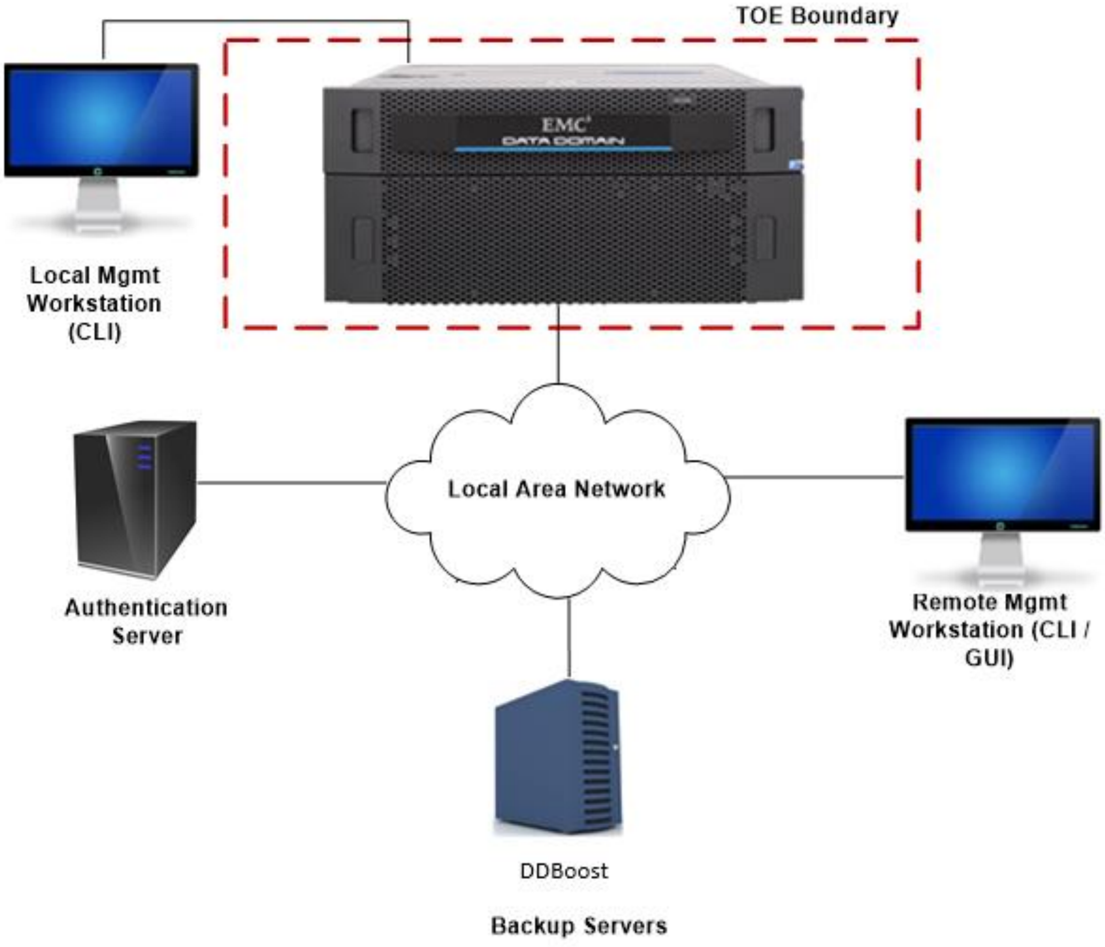

Figure 1 – TOE Diagram

1.5.1.1 TOE Delivery

The TOE is delivered to customers via trusted couriers, with the operating system pre-installed on the appliance.

The TOE software is also available to registered users via the Dell Digital Locker website (https://www.dell.com/support/software/us/en/4#/registration [dell.com]), and is presented to customers as a Red Hat Package Manager (.rpm) file:

- *7.2.0.95-692608.rpm*

1.5.1.2 TOE Guidance

All guidance documentation is provided in Portable Document Format (PDF) and is available for download to registered users at: https://support.emc.com/products.

The TOE includes the following guidance documentation:

- Dell EMC DD OS, Version 7.2, Administration Guide, June 2021
  - *dd_os_7.2_admin_guide_01.pdf*
- Dell EMC DD OS, Version 7.x, DD OS USB Installation Guide, May 2020
  - *DD_OS_7_X_USB_Installation_Guide_01.pdf*
- Dell EMC DD OS, version 7.2, Command Reference Guide, December 2020
  - *dd_os_7.2_command_reference_guide_04.pdf*
- Dell EMC PowerProtect DD6900 System, Installation Guide, December 2020
  - *DD6900_install_guide_01.pdf*
- Dell EMC PowerProtect DD9400 System, Installation Guide, December 2020
  - *DD9400_install_guide_01.pdf*
- Dell EMC PowerProtect DD9900 System, Installation Guide, December 2020
  - *DD9900_install_guide_01.pdf*
- Dell EMC Data Domain Boost for OpenStorage, Version 3.5, Administration Guide, December 2018
  - *docu91984_Data-Domain-Boost-for-OpenStorage-3.5-Administration-Guide.pdf*
- Dell EMC DDBoost for Partner Integration, Administration Guide, Version 7.2.0.50, June 2021
  - *DD_Boost_7.2.0.50_Partner_Integration_Guide_02.pdf*

The following Common Criteria Guidance Supplement is also available to customers, in PDF format, upon request:

- Dell EMC™ Data Domain® 7.2 Common Criteria Guidance Supplement, Version 1.9
  - *DD_EAL2_AGD_1.9.pdf*

1.5.2 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events.
Cryptographic Support	Data stored on the TOE is encrypted and decrypted using FIPS validated cryptographic algorithms, as detailed in Section 6.2.2. The TOE implements the Dell EMC Data Domain Crypto-C Micro Edition cryptographic module (CMVP Cert# 2757) for performing all cryptographic operations. The vendor affirms that no source code changes were made to the cryptographic module prior to recompilation into the TOE software.
User Data Protection	The TOE provides role-based access control capabilities to ensure that only authorized users are able to administer the TOE. The TOE controls access from servers to backup and recovery resources, and provides deduplication functionality to limit the disk size required to support these functions. RAID 6 ensures the integrity of stored data.
Identification and Authentication	Users must identify and authenticate prior to accessing the TOE. Obscured feedback is provided during authentication.
Security Management	The TOE provides management capabilities locally via Command Line Interface and remotely via Web-Based GUI and CLI. Management functions allow authorized administrators to configure users, roles, and client access attributes.
Protection of the TSF	The TOE preserves the secure state in the event of up to two disk failures. The TOE provides reliable time stamps for auditable events.
Trusted Path	The TOE provides a trusted path of communication.

Table 3 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

1.5.3.1 Excluded TOE Interfaces

Use of the following interfaces is not included in this evaluation and are disabled on the TOE by default:

USB Port – All instances of the TOE are equipped with a Universal Serial Bus (USB) port that may be used by an authorized administrator for DDOS system maintenance and updates. This port may also be used for connecting a USB keyboard during configuration.

FTP/FTPS – Authorized users can view system logs and alerts by accessing the TOE via File Transfer Protocol/File Transfer Protocol Secure (FTP/FTPS).

Telnet – Use of Telnet protocol is not permitted in the evaluated configuration of the TOE.

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

2.3 PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2 augmented with ALC_FLR.2 Flaw Reporting Procedures.

2.4 CONFORMANCE RATIONALE

This ST does not claim conformance of the TOE with any PP, therefore a conformance rationale is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 4 lists the threats addressed by the TOE. Potential threat agents are authorized TOE users, and unauthorized persons. The level of expertise of both types of attacker is assumed to be unsophisticated. TOE users are assumed to have access to the TOE, extensive knowledge of TOE operations, and to possess a high level of skill. They have moderate resources to alter TOE parameters, but are assumed not to be wilfully hostile. Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters and no physical access to the TOE.

Mitigation of the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.ACCESS	An unauthorized person may attempt to bypass the TOE security policy to access protected resources.
T.ACCOUNT	An unauthorized user could gain access to TOE configuration information or security management functions and use this to allow unauthorized access to information protected by the TOE.
T.AUDACC	Persons may not be held accountable for their changes to the TSF data because their actions are not recorded.

Table 4 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 5 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.DETECT	All events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity must be collected to ensure that all users are held accountable for their actions.
P.DUPDATA	The TOE must optimize performance and storage capacity by reducing the storage of duplicate data segments.
P.MANAGE	The TOE shall be managed only by authorized administrators.

OSP	Description
P.PROTECT	The TOE shall incorporate mechanisms to protect against potential loss or disclosure of the data it has been entrusted to store.
P.TRUSTEDPATH	The TOE shall provide cryptography to establish a trusted path with the management interface.

Table 5 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 6.

Assumptions	Description
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE.
A.NETWORK	The network on which the TOE components are operating on are sufficiently protected from attackers.
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.

Table 6 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.AUDIT	The TOE must record audit records for security related events.
O.COMMS	The TOE must provide cryptography required to adequately establish a trusted path.
O.CRYPTO	The TOE must protect the confidentiality of data it has been entrusted to store using cryptographic functions.
O.DATAOPT	The TOE must prevent the duplication of stored data by identifying and removing previously stored segments.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
O.OBSFEED	The TOE must provide obscured feedback to users while authentication is in progress.
O.PROTECT	The TOE must protect the integrity of data that it has been entrusted to store.

Table 7 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	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.NETWORKPROTECT	Those responsible for the TOE must establish and implement procedures to ensure that logical networks are protected in an appropriate manner.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.ACCESS	T.ACCOUNT	T.AUDACC	P.DETECT	P.DUPDATA	P.MANAGE	P.PROTECT	P.TRUSTEDPATH	A.LOCATE	A.MANAGE	A.NETWORK	A.NOEVIL
O.ACCESS	X	X				X						
O.ADMIN	X	X	X			X						
O.AUDIT			X	X								
O.DATAOPT					X							
O.COMMS								X				

	T.ACCESS	T.ACCOUNT	T.AUDACC	P.DETECT	P.DUPDATA	P.MANAGE	P.PROTECT	P.TRUSTEDPATH	A.LOCATE	A.MANAGE	A.NETWORK	A.NOEVIL
O.CRYPTO							X					
O.IDENTAUTH	X	X		X		X						
O.OBSFEED	X	X										
O.PROTECT							X					
OE.ADMIN										X		X
OE.NETWORKPROTECT											X	
OE.PHYSICAL									X		X	

Table 9 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE and the Operational Environment back to the threats addressed by the TOE.

Threat: **T.ACCESS**	An unauthorized person may attempt to bypass the TOE security policy to access protected resources.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.OBSFEED	The TOE must provide obscured feedback to users while authentication is in progress.

Rationale:	O.ACCESS helps to mitigate the threat by ensuring that only authorized users have access to the TOE functions and data. O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE is restricted to authorized administrators. O.IDENTAUTH mitigates this threat by ensuring all authorized users are identified and authenticated prior to gaining access to the TOE. O.OBSFEED mitigates this threat by providing obscured feedback while authentication is in progress.

Threat: **T.ACCOUNT**	An unauthorized user could gain access to TOE configuration information or security management functions and use this to allow unauthorized access to information protected by the TOE.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
	O.OBSFEED	The TOE must provide obscured feedback to users while authentication is in progress.
Rationale:	O.ACCESS helps to mitigate the threat by ensuring that only authorized users have access to the TOE functions and data. O.ADMIN mitigates this threat by ensuring that access to the security functions of the TOE are restricted to authorized administrators. O.IDENTAUTH mitigates this threat by ensuring all authorized users are identified and authenticated prior to gaining access to the TOE. O.OBSFEED mitigates this threat by providing obscured feedback while authentication is in progress, protecting authentication information from being used by an unauthorized person.	

Threat: **T.AUDACC**	Persons may not be held accountable for their changes to the TSF data because their actions are not recorded.

Objectives:	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.AUDIT	The TOE must record audit records for security related events.
Rationale:	O.ADMIN helps mitigate this threat by only allowing authorized administrators access to TOE audit functions. O.AUDIT mitigates this threat by ensuring changes to the TSF data are logged.	

4.3.2 Security Objectives Rationale Related to OSPs

The security objectives rationale related to OSPs traces the security objectives for the TOE and the Operational Environment back to the OSPs applicable to the TOE.

Policy: **P.DETECT**	All events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity must be collected to ensure that all users are held accountable for their actions.	
Objectives:	O.AUDIT	The TOE must record audit records for security related events.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
Rationale:	O.AUDIT ensures that the use of the TOE is recorded. This may be used to provide evidence of inappropriate activity. O.IDENTAUTH supports this policy by ensuring that the TOE has a clear identity for any user who may be misusing the TOE.	

Policy: **P.DUPDATA**	The TOE must optimize performance and storage capacity by reducing the storage of duplicate data segments.	
Objectives:	O.DATAOPT	The TOE must prevent the duplication of stored data by identifying and removing previously stored segments.
Rationale:	O.DATAOPT supports this policy by ensuring that storage capacity is maximized by eliminating multiple copies of the same data segments.	

Policy: **P.MANAGE**	The TOE shall be managed only by authorized administrators.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
Rationale:	O.ACCESS supports this policy by ensuring that only authorized users have access to the TOE functions and data. O.ADMIN ensures that access to the security functions of the TOE are restricted to authorized administrators. O.IDENTAUTH supports this policy by ensuring all authorized users are identified and authenticated prior to gaining access to the TOE.	

Policy: **P.PROTECT**	The TOE shall incorporate mechanisms to protect against potential loss or disclosure of the data it has been entrusted to store.	
Objectives:	O.CRYPTO	The TOE must protect the confidentiality of data it has been entrusted to store using cryptographic functions.
	O.PROTECT	The TOE must protect the integrity of data that it has been entrusted to store.
Rationale:	O.CRYPTO ensures that stored data is protected from disclosure through the use of cryptographic mechanisms. O.PROTECT ensures that the integrity of data it has been entrusted to store is protected from physical component failure or unauthorized access.	

Policy: **P.TRUSTEDPATH**	The TOE provides cryptography to produce a trusted path for the management interfaces (remote console and the web GUI).	
Objectives:	O.COMMS	The trusted path is adequately protected by the TOE-supplied cryptography.
Rationale:	The data sent using the trusted path is protected from modification and disclosure. The confidentiality of the data is maintained.	

4.3.3 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE’s operational environment.

Assumption: **A.LOCATE**	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE from physical attack.	

Assumption: **A.MANAGE**	There are one or more competent individuals assigned to manage the TOE.	
Objectives:	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.
Rationale:	OE.ADMIN supports this assumption by ensuring that multiple competent administrators are given TOE management authority.	

Assumption: **A.NETWORK**	The network on which the TOE components are operating on are sufficiently protected from attackers.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
	OE.NETWORKPROTECT	Those responsible for the TOE must establish and implement procedures to ensure that logical networks are protected in an appropriate manner.
Rationale:	OE.PHYSICAL supports this assumption by protecting TOE components from physical attack. OE.NETWORKPROTECT supports this assumption by ensuring the protection of any logical networks used by the TOE.	

Assumption: **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.	
Objectives:	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.
Rationale:	OE.ADMIN supports this assumption by ensuring that the administrators managing the TOE have been specifically chosen to be careful, attentive, non-hostile, and follow all administrator guidance.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section specifies the extended Security Functional Requirements (SFRs) used in this ST. The following extended SFR has been created to address additional security features of the TOE:

- Duplicate data removal (FDP_DDR _EXT.1)

5.1.1 Family FDP_DDR_EXT: Duplicate Data Removal

Duplicate data removal functions involve optimizing data storage by identifying segments of data that have already been stored and ensuring that redundancy is not caused by storing those segments multiple times for different data sets. The duplicate data removal family was modeled after FDP_SDI: Stored data integrity.

Family Behaviour

This family defines the requirements for duplicate data removal functionality.

Component Levelling

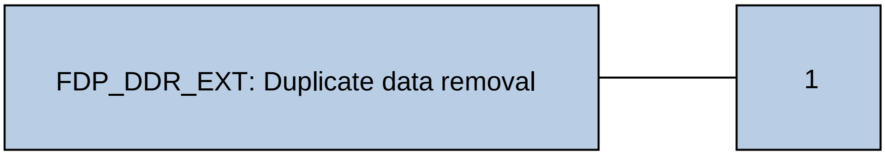

Figure 2 – FDP_DDR_EXT: Duplicate Data Removal Component Levelling

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.1.1.1 FDP_DDR_EXT.1 Duplicate data removal

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_DDR_EXT.1.1 The TSF shall check incoming data to ensure that only unique data segments are stored in containers controlled by the TSF.

FDP_DDR_EXT.1.2 Upon detection of duplicate data, the TSF shall [assignment: *action to be taken*] before writing new data to a storage container.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 10.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key Destruction
	FCS_COP.1	Cryptographic operation
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_DDR_EXT.1	Duplicate data removal

Class	Identifier	Name
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_SDI.2	Stored data integrity monitoring and action
Identification and Authentication (FIA)	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1(1)	Management of security attributes (Management Access Control SFP)
	FMT_MSA.1(2)	Management of security attributes (User Data Information Flow Control SFP)
	FMT_MSA.3(1)	Static attribute initialisation (Management Access Control SFP)
	FMT_MSA.3(2)	Static attribute initialisation (User Data Information Flow Control SFP)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_STM.1	Reliable time stamps
Trusted Path (FTP)	FTP_TRP.1	Trusted Path

Table 10 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 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) [*none*].

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, [*none*].

6.2.1.2 FAU_GEN.2 User identity association

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Deterministic Random Bit Generation*] and specified cryptographic key sizes [*128 bit, 256 bit*] that meet the following: [*SP800-90A*].

6.2.2.2 FCS_CKM.4 Cryptographic key destruction

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.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2*].

6.2.2.3 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*] and cryptographic key sizes [*128 bit, 256 bit*] that meet the following: [*FIPS 197*].

6.2.3 User Data Protection (FDP)

6.2.3.1 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 [*Management Access Control SFP*] on

[*Subjects: Authorized Administrators;*

Objects: TOE configuration data;

Operations: create, modify, delete].

6.2.3.2 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 [*Management Access Control SFP*] to objects based on the following: [

- *Subjects: Authorized Administrators*
  Security Attributes:
  a) *User ID*
  b) *Role*

- *Objects: TOE configuration data*
  Security Attributes: None
  ].

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 authorized administrator with the appropriate role can manipulate the TOE configuration*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

6.2.3.3 FDP_DDR_EXT.1 Duplicate data removal

Hierarchical to:	No other components.
Dependencies:	No dependencies

FDP_DDR_EXT.1.1 The TSF shall check incoming data to ensure that only unique data segments are stored in containers controlled by the TSF.

FDP_DDR_EXT.1.2 Upon detection of duplicate data, the TSF shall [*perform a global compression process and eliminate redundant data*] before writing new data to a storage container.

6.2.3.4 FDP_IFC.1 Subset information flow control

Hierarchical to:	No other components.
Dependencies:	FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [*User Data Information Flow Control SFP*] on

[*Subjects: external servers;*

Information: stored user data;

Operations: read and write].

6.2.3.5 FDP_IFF.1 Simple security attributes

Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the [*User Data Information Flow Control SFP*] based on the following types of subject and information security attributes: [

- *Subjects: External servers*[1]
  Security Attributes: Identity of the server

- *Information: Stored user data*
  Security Attributes: Directory Permissions
  ].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*an external server can read and write stored user data if the identity of the external server is associated with the data's directory permissions*].

FDP_IFF.1.3 The TSF shall enforce the [*no additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*none*].

6.2.3.6 FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.

[1] External servers are called 'clients' in the Data Domain user documentation, and are identified by hostname or IP address.

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 6*].

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

Application Note: Stored user data represents the objects for this family.

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification

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

6.2.4.2 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 [*the number of characters typed*] to the user while the authentication is in progress.

6.2.4.3 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
Dependencies:	No dependencies.

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

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MSA.1(1) Management of security attributes (Management Access Control SFP)

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(1) The TSF shall enforce the [*Management Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*User ID and role*] to [*authorized administrators*].

6.2.5.2 FMT_MSA.1(2) Management of security attributes (User Data Information Flow Control SFP)

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(2) The TSF shall enforce the [*User Data Information flow control SFP*] to restrict the ability to [modify, delete, [*create*]] the security attributes [*server identity*] to [*authorized administrators*].

6.2.5.3 FMT_MSA.3(1) Static attribute initialisation (Management Access Control SFP)

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

FMT_MSA.3.1(1) The TSF shall enforce the [*Management* A*ccess Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [*authorised administrators*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.4 FMT_MSA.3(2) Static attribute initialisation (User Data Information Flow Control SFP)

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

FMT_MSA.3.1(2) The TSF shall enforce the [*User Data Information Flow Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [*authorized administrators*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.5 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

a) administer user account information;
b) administer TOE configuration functions; and
c) administer user data information flow control rules

].

6.2.5.6 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 [

- *Admin*
- *Limited-admin*
- *User*
- *Security*
- *Backup Operator*
- *None*
- *Tenant-Admin*
- *Tenant-User*

].

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

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*up to two concurrent disk failures*].

6.2.6.2 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.

6.2.7 Trusted path (FTP)

6.2.7.1 FTP_TRP.1 Trusted Path

Hierarchical to: No other components.
Dependencies: No dependencies.

FTP_TRP.1.1 The TSF operational environment 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 [*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 [*DDBoost server communication, remote administration*].

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 11.

Assurance Class	Assurance Components	
	Identifier	Name
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	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)	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)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample

Assurance Class	Assurance Components	
	Identifier	Name
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 11 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

The following Table provides a mapping between the SFRs and Security Objectives.

	O.ACCESS	O.ADMIN	O.AUDIT	O.COMMS	O.CRYPTO	O.DATAOPT	O.IDENTAUTH	O.OBSFEED	O.PROTECT
FAU_GEN.1			X						
FAU_GEN.2			X						
FCS_CKM.1					X				
FCS_CKM.4					X				
FCS_COP.1					X				
FDP_ACC.1	X	X							
FDP_ACF.1	X	X							
FDP_DDR_EXT.1						X			
FDP_IFC.1									X
FDP_IFF.1									X
FDP_SDI.2									X
FIA_UAU.2	X	X					X		
FIA_UAU.7								X	

	O.ACCESS	O.ADMIN	O.AUDIT	O.COMMS	O.CRYPTO	O.DATAOPT	O.IDENTAUTH	O.OBSFEED	O.PROTECT
FIA_UID.2	X	X					X		
FMT_MSA.1(1)		X							
FMT_MSA.1(2)		X							
FMT_MSA.3(1)		X							
FMT_MSA.3(2)		X							
FMT_SMF.1		X							
FMT_SMR.1		X					X		
FPT_FLS.1									X
FPT_STM.1			X						
FTP_TRP.1				X					

Table 12 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: **O.ACCESS**	The TOE must allow authorized users to access only appropriate TOE functions and data.	
Security Functional Requirements:	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Rationale:	FDP_ACC.1 meets this objective by enforcing an access control policy to ensure only authorized users can gain access to appropriate TOE functions and data. FDP_ACF.1 meets this objective by enforcing the rules and attributes that govern the access control policy. FIA_UAU.2 meets this objective by ensuring that each user is	

	successfully authenticated before gaining access to TOE functions and data. FIA_UID.2 supports this objective by ensuring that the identity of each user is known before allowing access to TOE functions and data.

Objective: **O.ADMIN**	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	
Security Functional Requirements:	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FIA_UAU.2	User authentication before any action
	FIA-UID.2	User identification before any action
	FMT_MSA.1(1)	Management of security attributes (Management Access Control SFP)
	FMT-MSA.1(2)	Management of security attributes (User Data Information Flow Control SFP)
	FMT_MSA.3(1)	Static attribute initialisation (Management Access Control SFP)
	FMT_MSA.3(2)	Static attribute initialisation (User Data Information Flow Control SFP)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Rationale:	FDP_ACC.1 supports this objective by only allowing authorized administrators access to management functions of the TOE access control policies. FDP_ACF.1 supports this objective by enforcing rules that only allow users with the appropriate role to manipulate the TOE configuration. FIA_UAU.2 meets this objective by ensuring that each user is successfully authenticated before gaining access to TOE functions and data. FIA_UID.2 supports this objective by ensuring that the identity of each user is known before allowing access to TOE functions and data. FMT_MSA.1(1) and FMT_MSA.3(1) support this objective by restricting the ability to manipulate the Management Access Control SFP security attributes to users with the admin and security roles.	

	FMT_MSA.1(2) and FMT_MSA.3(2) support this objective by restricting the ability to manipulate the User Data Information Flow Control SFP security attributes to users with the admin and security roles. FMT_SMF.1 supports this objective by identifying the management functions authorized administrators are able to perform. FMT_SMR.1 meets this objective by supporting a list of authorized roles for the TOE.

Objective: **O.AUDIT**	The TOE must record audit records for security related events.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FPT_STM.1	Reliable time stamps
Rationale:	FAU_GEN.1 supports this objective by generating audit records for auditable events. FAU_GEN.2 supports this objective by associating a user identity with each auditable event generated. FPT_STM.1 provides a time stamp for each auditable event.	

Objective: **O.COMMS**	The TOE must protect the confidentiality of data it has been entrusted to store using cryptographic functions.	
Security Functional Requirements:	FTP_TRP.1	Trusted path
Rationale:	FTP_TRP.1 supports this objective by providing the cryptographic functionality required to establish a trusted path with the management interface and the remote console and between the web GUI and the management interface.	

Objective: **O.CRYPTO**	The TOE must protect the confidentiality of data it has been entrusted to store using cryptographic functions.	
Security Functional Requirements:	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation

Rationale:	FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 support this objective by providing the cryptographic functionality required to protect the confidentiality of data stored on the TOE.	

Objective: **O.DATAOPT**	The TOE must prevent the duplication of stored data by identifying and removing previously stored segments.	
Security Functional Requirements:	FDP_DDR_EXT.1	Duplicate data removal
Rationale:	FDP_DDR_EXT.1 supports this objective by ensuring that storage capacity is maximized by eliminating multiple copies of the same data segments.	

Objective: **O.IDENTAUTH**	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FMT_SMR.1	Security roles
Rationale:	FIA_UAU.2 supports this objective by ensuring that each user is successfully authenticated before gaining access to TOE functions and data. FIA_UID.2 supports this objective by ensuring that the identity of each user is known before allowing access to TOE functions and data. FMT_SMR.1 meets this objective by supporting authorized roles for the TOE.	

Objective: **O.OBSFEED**	The TOE must provide obscured feedback to users while authentication is in progress.	
Security Functional Requirements:	FIA_UAU.7	Protected authentication feedback
Rationale:	FIA_UAU.7 supports this objective by providing only the number of characters typed to users while authentication is in progress.	

Objective: O.PROTECT	The TOE must protect the integrity of data that it has been entrusted to store.	
Security Functional Requirements:	FDP_ITC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_SDI.2	Store data integrity monitoring and action
	FPT_FLS.1	Failure with preservation of state
Rationale:	FDP_IFC.1 supports this objective by enforcing the User Data Information Flow Control SFP on external servers. FDP_IFF.1 supports this objective by identifying the rules and security attributes associated with the User Data Information Flow Control SFP. FDP_SDI.2 protects stored user data from integrity errors. FPT_FLS.1 protects stored user data from disk failure.	

6.4.3 Dependency Rationale

Table 13 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1.
	FCS_CKM.4	✓	
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1.
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1.
	FCS_CKM.4	✓	
FDP_ACC.1	FDP_ACF.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(1).
FDP_DDR_EXT.1	None	N/A	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(2).
FDP_SDI.2	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UAU.7	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1.
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_IFC.1.
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3(1)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(1).
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(2).
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_FLS.1	None	N/A	

SFR	Dependency	Dependency Satisfied	Rationale
FPT_STM.1	None	N/A	
FTP_TRP.1	None	N/A	

Table 13 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw reporting procedures (ALC_FLR.2). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.2 augmentation since there are a number of areas where current practices and procedures exceed the minimum requirements for EAL 2.

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 SECURITY AUDIT

The TOE generates a set of log files determined by the system events that occur. Log files cannot be modified or deleted by any user within the DD System Manager but can be copied from the log directory and accessed through another application, such as Notepad. Log files can also be viewed in the CLI by using the *log view* command.

The following logs are generated by the TOE:

Log File Name / Location	Auditable events	Event Log Information
audit.log */ddvar/log/audit.log*	User login events	• Subject identity • Date and time
Messages */ddvar/log/messages*	General system events	• Commands executed • Startup and shut down of the audit functions • Date and time
secure.log */ddvar/log/debug/secure.log*	User events	• Successful and failed logins • User additions and deletions • Password changes • Date and time
access.log */ddvar/log/debug/sm/access_log*	GUI transactions	• Subject identity • Date and time

Table 14 - TOE Log Files

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_GEN.2.

7.2 CRYPTOGRAPHIC SUPPORT

Using cryptographic algorithms, the TOE protects the confidentiality of data at rest. When data is ingested into the TOE, unique segments are identified and collected together into compression units. Each compression unit is encrypted, using a single cryptographic key, before being written to the storage containers. The key for this block of data will remain stored on the TOE until all of the data associated with it is deleted or removed, or until the TOE is decommissioned. As read operations are being performed on the TOE, the data is decrypted using the same key.

Cryptographic keys can only be managed by authorized administrators. Administrators have the option to configure the TOE to use static keys, or rotate the keys by setting a periodic schedule. When key rotation is configured, the currently active key is replaced by the new key, and the key state changed to read-only. The data associated with that key also becomes read only. Once the TOE has been restarted, all new data ingested is encrypted using the new key.

When a key is destroyed, any data associated with it is re-encrypted during the next file system cleaning cycle. Once all the affected data is re-encrypted, the key can be deleted/removed from the system. Deletion/removal of a key will result in a 3-pass overwrite on the key value; one pass with zeroes, one pass with ones and another pass with alternating zeroes and ones.

All cryptographic functions used in data encryption and decryption are performed by a FIPS 140-2 validated cryptographic module, Cryptographic Module Validation Program (CMVP) Cert # 2757. The associated Cryptographic Algorithm Validation Program certificate information is provided in Table 15. Either Cipher Block Chaining (CBC) or Galois/Counter Mode (GCM) may be used. The administrator may choose to encrypt data using AES-128 CBC, AES-256 CBC, AES-128 GCM, or AES-256 GCM.

Algorithm	CAVP Certificate Number
DRBG	191
AES	2017

Table 15 - Cryptographic Algorithms

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

7.3 USER DATA PROTECTION

The TOE enforces the Management Access Control SFP to control access to the administrative functions and configuration of the TOE. Only authorized Administrators have the ability to manipulate the TOE functions.

The User Data Information Flow Control SFP is implemented in a hierarchical manner. When an external server attempts to access a data directory, the identity of the server is checked against the directory permissions associated with the data being requested. For example, if an external server attempts to write files to a directory, but only read permissions are associated with that server, then the TOE prevents the data from being written to the directory.

The TOE uses RAID 6 to preserve the integrity of user data. RAID 6 provides redundancy and data loss recovery capability in the event of up to two concurrent disk failures. If a disk error resulting in the loss of or inability to read user data is encountered, the TOE is able to reconstruct the user data.

Data deduplication optimizes the storage of user data by scanning all user data that is to be stored for segments of data that have already been stored (as part of a different set of user data). If a duplicate segment is found, the TOE will replace the duplicate segment with a pointer to the already-stored segment and store the rest of the unique user data.

Data Domain performs deduplication using the proprietary Stream-Informed Segment Layout (SISL) scaling architecture. The deduplication algorithm breaks the incoming data stream into segments and computes a unique fingerprint for the segment. This fingerprint is then compared to all others in the system to determine whether it is unique or redundant. Only unique data, and additional references to the previously stored unique segment, are stored to disk.

TOE Security Functional Requirements addressed: FDP_ACC.1, FDP_ACF.1, FDP_DDR_EXT.1, FDP_IFC.1, FDP_IFF.1, FDP_SDI.2.

7.4 IDENTIFICATION AND AUTHENTICATION

The Identification and Authentication function ensures that a user requesting a TOE administrative function has provided a valid User ID and password and is authorized to access that service, based on the user’s role.

When a user enters valid credentials at a TOE management interface, the user is granted access based on the user ID and role.

During the authentication process, only the number of characters typed is displayed while the user enters a password.

TOE Security Functional Requirements addressed: FIA_UAU.2, FIA_UAU.7, FIA_UID.2.

7.5 SECURITY MANAGEMENT

The following table identifies the user roles and describes the TOE functions available to each:

User Role	Description
Admin	An admin role user can configure and monitor the entire Data Domain system. Most configuration features and commands are available only to admin role users. However, some features and commands require the approval of a security role user before a task is completed.
Limited-admin	The limited-admin role can configure and monitor the Data Domain system with some limitations. Users who are assigned this role cannot perform data deletion operations, edit the registry, or enter bash or SE mode.
User	The user role enables users to monitor systems and change their own password. Users who are assigned the user management role can view system status, but they cannot change the system configuration.
Security	A security role user, who may be referred to as a security officer, can manage other security officers,

User Role	Description
	authorize procedures that require security officer approval, and perform all tasks supported for user-role users. The security role is provided to comply with the Write Once Read-Many (WORM) regulation. This regulation requires electronically stored corporate data be kept in an unaltered, original state for purposes such as eDiscovery. Dell EMC Data Domain added auditing and logging capabilities to enhance this feature. As a result of compliance regulations, most command options for administering sensitive operations, such as DD Encryption, DD Retention Lock Compliance, and archiving now require security officer approval.
Backup Operator	A backup-operator role user can perform all tasks permitted for user role users, create snapshots for MTrees, import, export, and move tapes between elements in a virtual tape library, and copy tapes across pools.
None	The none role is for DD Boost authentication and tenant-unit users only. A none role user can log in to a Data Domain system and can change his or her password, but cannot monitor, manage, or configure the primary system.
Tenant-Admin	A tenant-admin role user can configure and monitor a specific tenant unit.
Tenant-User	The tenant-user role enables a user to monitor a specific tenant unit and change the user password. Users who are assigned the tenant-user management role can view tenant unit status, but they cannot change the tenant unit configuration.

Table 16 - TOE User Role Descriptions

The Data Domain appliance is installed with a default user account named *sysadmin*. The factory default password is the device's serial number, and the user is prompted to change the password on the first login. This account has admin permissions, and may not be deleted or modified. All administrative functions may be performed by a user in the admin role. Only the sysadmin user (the default user created during the DDOS installation) can create the first security officer, after which the privilege to create security officers is removed from the sysadmin user. After the first security officer is created, only security officers can create other security officers. There are some tasks that must be performed by a user in the admin role, and then approved by a user in the security officer role. However, many these functions are outside of the scope of the evaluation.

User ID and role information may be administered by users in the admin role. Users in the tenant-admin role may perform these functions for their specific tenant unit. Only the sysadmin user is available by default. All other users must be added by a user in the admin, tenant-admin or security officer role. This is considered to be restrictive default values for the User ID and role attributes.

Users in the admin role may determine which external servers or clients are permitted access to the Data Domain resources. Clients are identified by hostname or IP address. By default, no clients are granted access. This is considered to be restrictive default values for the server identity attributes.

Both the CLI and GUI provide functionality to administer the user account information for authorized administrators, configure the TOE for basic setup and to allow access to external servers, and to review audit logs.

TOE Security Functional Requirements addressed: FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_SMF.1, FMT_SMR.1.

7.6 PROTECTION OF THE TSF

The TOE uses a RAID 6 configuration to ensure that data remains consistent between physically separate disks within the same RAID group. The TOE ensures consistency between physically separate disks by specifying that RAID is to be used to protect the integrity of data stored on those disks.

The TOE also provides reliable time stamps for auditable events. Time stamp information is provided by the TOE hardware.

TOE Security Functional Requirements addressed: FPT_FLS.1, FPT_STM.1.

7.7 TRUSTED PATH

The TOE provides cryptography to create a trusted path to the management interface. TLS v1.2 is used to create trusted communications between the web GUI and the management interface, and between the filesystem handler interface and the DDBoost server. DDBoost uses version 1.0.2zd-fips of OpenSSL. SSH v2 is used to create a path between the remote console and the management interface.

TOE Security Functional Requirements addressed: FTP_TRP.1

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Data Deduplication	Data deduplication is a specialized data compression technique for eliminating duplicate copies of repeating data.

Table 17 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CC	Common Criteria
CLI	Command Line Interface
DD	Data Domain
DDOS	Data Domain Operating System
DR	Disaster Recovery
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
GCM	Galois Counter Mode
GUI	Graphical User Interface
IT	Information Technology
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random Access Memory
OSP	Organizational Security Policies
PP	Protection Profile
RAID	Redundant Array Independent Disk

Acronym	Definition
SFP	Security Function Policy
SFR	Security Functional Requirement
SISL	Stream-Informed Segment Layout
SSH	Secure Socket Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Universal Serial Bus
VT	Virtual Terminal
WORM	Write Once Read-Many

Table 18 – Acronyms