EMC Corporation
EMC RecoverPoint version 3.4

Security Target

Evaluation Assurance Level: EAL2+
Document Version: 0.6

Prepared for:

EMC Corporation
171 South Street
Hopkinton, MA 01748

Phone: (508) 435-1000

http://www.emc.com

Prepared by:

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

Phone: (703) 267-6050

http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2010-06-11	Nick Goble	Initial draft.
0.2	2010-06-18	Nick Goble	Updated based on lab comments.
0.3	2010-08-18	Nick Goble	Updated based on CRs.
0.4	2010-12-21	Shaunak Shah	Updated SFRs: FDP_ACF, FDP_IFF and FTA_TAB.
0.5	2011-02-14	Shaunak Shah	Updated diagrams.
0.6	2011-03-23	Amy Nicewick	Updated TOE Reference.

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is the EMC RecoverPoint version 3.4, and will hereafter be referred to as the TOE throughout this document. The TOE is a secure platform for continuous data protection (CDP), continuous remote replication (CRR), and concurrent local and remote (CLR) replication. The TOE is a software-only TOE.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 - ST and TOE References

ST Title	EMC Corporation RecoverPoint version 3.4 Security Target
ST Version	Version 0.6
ST Author	Corsec Security, Inc. Nick Goble
ST Publication Date	3/23/2011
TOE Reference	EMC RecoverPoint version 3.4 (h.102)
Keywords	EMC, RecoverPoint version 3.4, RecoverPoint, continuous data protection, continuous remote replication, concurrent local and remote replication, CDP, CRR, CLR

1.3 Product Overview

The Product Overview provides a high level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

EMC RecoverPoint is an appliance-based product that provides real-time, block-level data replication for systems and devices in an enterprise storage area network (SAN) environment. RecoverPoint runs on an out-of-band RecoverPoint appliance (RPA), not a storage system or application host (where it would use memory and CPU[1] cycles on the storage device or host), and combines cutting edge continuous data protection technology with reductions in required storage and bandwidth requirements. RecoverPoint provides near-zero-data-loss protection both locally and remotely over a wide area network (WAN), as well as zero data loss synchronous replication over extended Fiber Channel links

Replication can be formed in three configurations: CDP, CRR, and CLR. In a CDP configuration, a local SAN connects systems and devices to a local RPA for local replication designed to allow operational recovery from logical corruptions such as human errors or viruses. In a CRR configuration, two geographically dispersed SANs are connected by two RPA clusters for remote replication, designed to allow recovery primarily from geographical or site disasters. In a CLR configuration, both of these are simply done at the same time by the RecoverPoint software and appliances. RecoverPoint also digitally signs replicated data for integrity and records data change journals, allowing roll-back, recovery, and forensic analysis of data writes, all in a distributed system that provides high-availability and low-latency.

Replication is done on the RPAs but it is enabled by components called Splitters, which are proprietary software that is installed on either host operating systems, storage systems, or intelligent fibre switches. The primary function of a splitter is to “split” application writes so they are sent to their normally designated storage volumes and the RPA simultaneously.

Splitting can be performed:

- by splitters that are installed on each protected host,
- by the Fibre Channel (FC) switches to which the systems and devices are connected. Provided that intelligent fabric capabilities are supported by the switch or director, or
- by Storage Arrays (such as EMC CLARiiON, VNX, Symmetrix storage arrays, etc) from and to which the systems and devices are replicated.

RecoverPoint can be integrated into an existing network infrastructure and make use of an NTP[2] server to ensure accurate time between separate RPA instances. RecoverPoint also provides two independent mechanisms for authenticating users: local authentication via appliance operating system, and authentication via an organization’s existing Lightweight Directory Access Protocol (LDAP) server. The two authentication mechanisms can be used simultaneously or exclusively.

Management and monitoring of a complete RecoverPoint distributed system can be performed using either the RecoverPoint CLI[3] or the RecoverPoint Management Application GUI[4]. The RecoverPoint CLI is accessed by using a secure shell (SSH) login. The RecoverPoint CLI supports two operational modes: interactive mode where the system will prompt for mandatory and optional parameters after a command is entered, and command line mode which allows for automation of management tasks through the use of designated scripts. The RecoverPoint Management Application GUI is invoked through a standard web browser (Internet Explorer or Firefox) with a Java plug-in installed over HTTP[5] or HTTPS[6] (using

[1] CPU – Central Processing Unit
[2] NTP – Network Time Protocol
[3] CLI – Command Line Interface
[4] GUI – Graphical User Interface
[5] HTTP – Hypertext Transfer Protocol

SSL[7]v3.0 or TLS[8]v1.0). The RecoverPoint Management Application GUI is automatically downloaded upon first invocation.

RecoverPoint is available in two versions, RecoverPoint/SE[9] and RecoverPoint. RecoverPoint/SE is the entry level offering that simplifies replication and continuous data protection for a single Storage Array or between two Storage Arrays. RecoverPoint is the full featured version that adds support for a full range of splitters, systems, and storage devices. RecoverPoint/SE can be upgraded to the full version of RecoverPoint through the use of a license key.

The following third-party software provides product functionality:

- Apache (Version 2.2.9) – provides a web server for the product;
- Iptables (Version 1.4.2.6) – provides Firewall services for the product;
- OpenSSH (Version 1.5.1) – provides secure remote management for the RecoverPoint CLI;
- OpenSSL (Version 0.9.8g) – provides secure remote management for the RecoverPoint Management Application GUI;

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

RecoverPoint version 3.4 is a software-only TOE, which supports CDP, CRR, and CLR. The TOE includes only the RecoverPoint version of the product not the RecoverPoint/SE version.

Figure 1 shows the CC-evaluated deployment configuration of the TOE, in a CLR configuration:

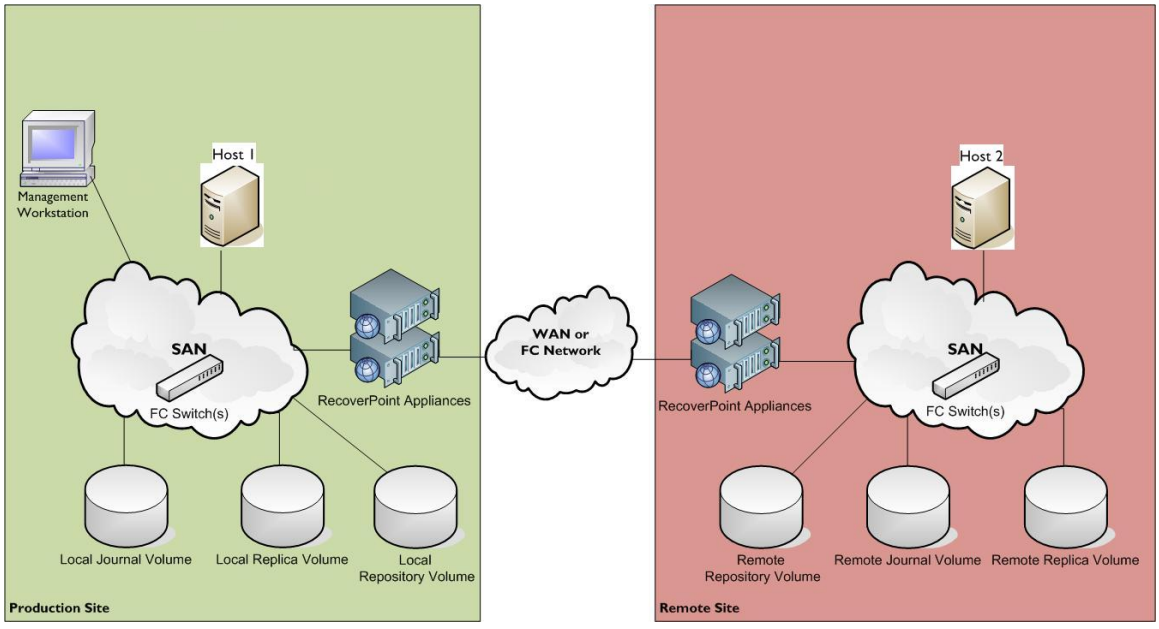

Figure 1 – Deployment Configuration of the TOE

[6] HTTPS – Secure Hypertext Transfer Protocol
[7] SSL – Secure Sockets Layer
[8] TLS – Transport Layer Security
[9] SE – SE is not defined by EMC

The TOE can provide the following services:

- Replication of SAN-resident application data configured with a RecoverPoint splitter;
- Control access between RPAs, systems and devices, and replica volumes;
- Recovery of SAN-resident application data;

1.4.1 Brief Description of the Components of the TOE

The following components are part of the evaluated configuration of the TOE, and work together to provide the TOE functionality. The TOE excludes the physical and logical features and functionality listed in 1.5.3.

1.4.1.1 CLI Component

The CLI component of the TOE is responsible for providing a CLI over which users of the TOE can execute RecoverPoint commands and scripts. The RecoverPoint CLI component supports two operational modes: interactive mode where the system will prompt for mandatory and optional parameters after a command is entered, and command line mode which allows for automation of management tasks through the use of designated scripts.

1.4.1.2 Web Server Component

The Web Server component of the TOE is responsible for providing a RecoverPoint Management Application GUI over which users of the TOE can connect using a standard web browser (Internet Explorer or Firefox) with a Java plug-in installed over HTTP or HTTPS. In addition to serving the Java GUI, the Web Server component also allows authenticated administrators to download appliance logs in .zip format.

1.4.1.3 Installation Server Component

The Installation Server component is a process that runs on all RPAs at all times. The Installation Server component is used to perform initial installation and configuration of an RPA and to perform log monitoring after the RPA is configured and in an operational state.

1.4.1.4 Management Server Component

The Management Server component handles management commands and requests and forwards them to the Control subsystem. The Management Server component also performs monitoring and analysis functions for administrators.

1.4.1.5 Control Component

The Control component implements a state machine that acts as the central hub and decision maker for an RPA. The Control component acts an intermediary between the Replication and Management Server components, by collecting configuration data from the Management Server component and communicating with the Replication component to calculate the state of the system before making changes to the system settings.

1.4.1.6 Replication Component

The Replication component implements the replication logic, used for CDP, CRR, and CLR performed by RPAs.

1.4.1.7 External Management Component

The External Management component is used to communicate with the EMC common management platform for Storage Arrays. The External Management component communicates directly with the Web Server component, Installation Server component, and Management Server component.

1.4.1.8 Firewall Component

The Firewall component provides enhanced security by running IPtables firewall that blocks all unused ports on an RPA.

1.4.2 TOE Environment

The evaluated deployment configuration of the TOE requires the following environmental components:

- RecoverPoint appliance hardware;
- SAN with FC switches to allow systems and devices to connect to the TOE;
- RecoverPoint splitter;
- Storage devices[10] to provide storage for Journal, Replica, and Repository volumes;
- Management Workstation to manage the TOE;

The TOE is intended to be deployed in physically secure environments and managed by administrators who are appropriately trained and follow all guidance listed in 1.5.1.2.

The TOE is intended to provide replication services to systems and devices on a SAN. For the TOE to operate correctly, all systems and devices must maintain connection to the TOE through the SAN. The TOE environment is required to provide for this configuration.

The TOE is managed through the RecoverPoint CLI and the RecoverPoint Management Application GUI. Administrators must access these interfaces from a trusted workstation on a network connected to the SAN.

1.4.2.1 Logical Environmental Components of the TOE

1.4.2.1.1 Journal

The journal consists of one or more volumes that are dedicated on the SAN-attached storage system or device for the purpose of holding images that are waiting to be distributed or have already been distributed to the replica volume. The journal provides the necessary delta differentials for rolling the replica back or forwards to any Point in Time.

1.4.2.1.2 Repository Volume

The repository volume is a special volume that must be dedicated on the SAN-attached storage at each site, for each RPA cluster. The repository volume serves all RPAs of the particular cluster and splitters associated with that cluster. It stores configuration information about the RPAs and consistency groups, which enables a properly functioning RPA to seamlessly assume the replication activities of a failing RPA from the same cluster.

1.4.2.1.3 Replica Volume

The replica volume is the target of replication for a production volume that contains the application data of a SAN-attached host application protected by RecoverPoint.

1.4.2.1.4 Replication Set

Every protected production volume must have a corresponding replica volume at each copy. Together these 2 or 3 volumes (depending on whether the configuration is CDP, CRR, or CLR) are called a replication set.

1.5 TOE Description

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

[10] Note in the evaluated configuration the journal, replica, and repository volumes exist on the same Storage Array for simplicity, but generally these can be stored on different storage devices.

1.5.1 Physical Scope

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

The TOE is a software-only continuous data protection solution operating on a Linux Kernel (Version 2.6.32.9 from Kernel.org) on Gen4 RecoverPoint appliance hardware as depicted in Figure 2 below.

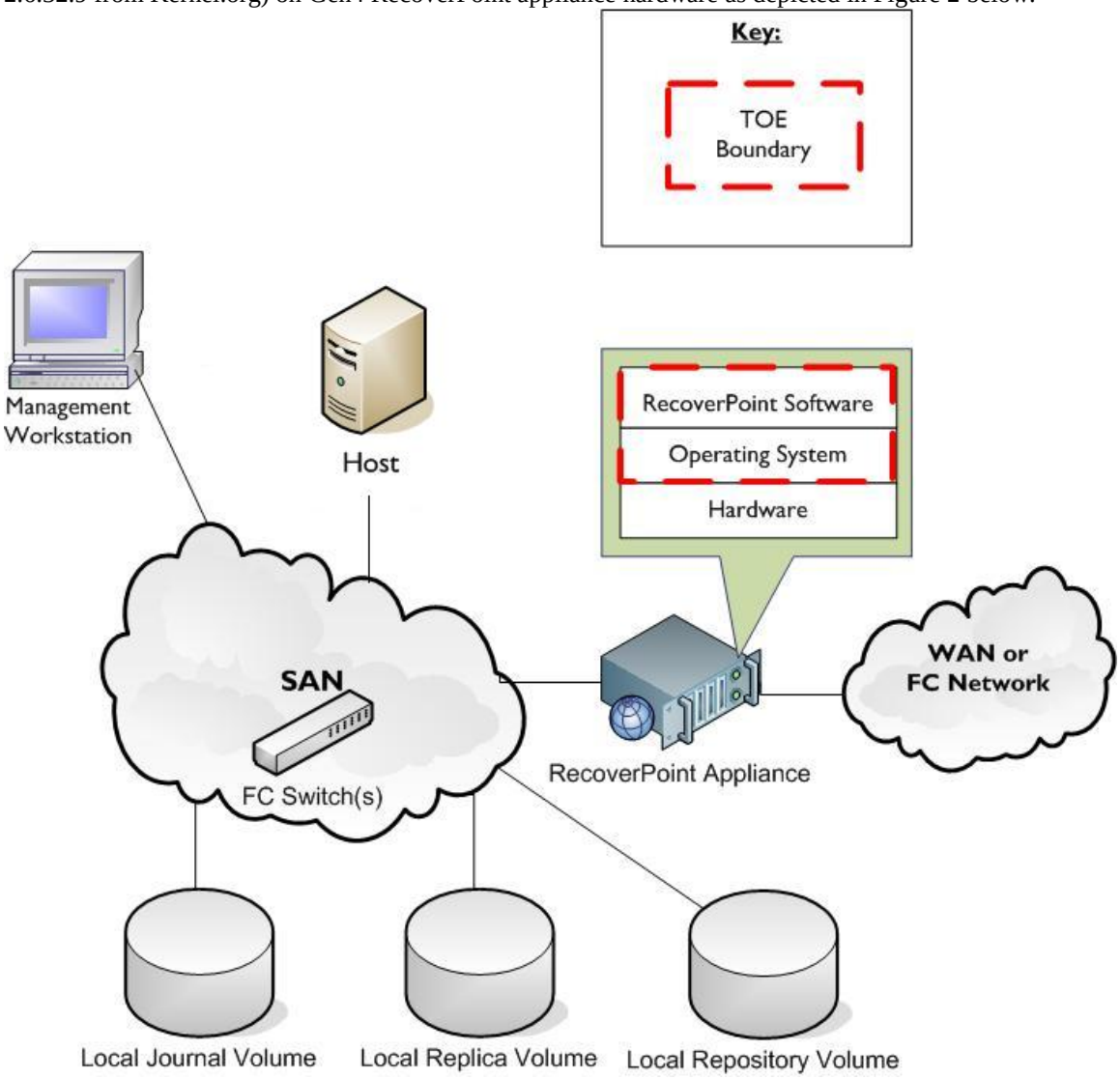

Figure 2 - Physical TOE Boundary

1.5.1.1 TOE Software

The TOE is a software-only continuous data protection and remote replication solution operating on a Linux Kernel (Version 2.6.32.9 from Kernel.org) on RecoverPoint appliance hardware.

The following third-party software is included in the TOE installation:

- Apache (Version 2.2.9) – provides a web server for the TOE;
- Iptables (Version 1.4.2.6) – provides Firewall services for the TOE;

1.5.1.2 Guidance Documentation

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

- RecoverPoint version 3.4 Administrator's Guide
- RecoverPoint version 3.4 Deployment Manager Product Guide
- RecoverPoint version 3.4 Installation Guide
- RecoverPoint version 3.4 Security Configuration Guide
- RecoverPoint version 3.4 CLI Reference Guide

1.5.2 Logical Scope

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

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF[11]
- TOE Access

1.5.2.1 Security Audit

The TOE performs auditing of authentication attempts and administrative actions. The admin and monitor roles can review all audit records through the RecoverPoint CLI and RecoverPoint Management Application GUI. Audit data can be selected for review and ordered based on the following parameters: *start time, end time, topic, level, search_text, and time zone*.

1.5.2.2 User Data Protection

The TOE enforces a Replication Access Control Policy on systems and devices with a RecoverPoint splitter installed, and a Group Access Control Policy on RPAs trying to read or write from the volumes that are configured in the environment for use by the TOE. Access via the Replication Access Policy is based on the Replication Set. Access via the Group Access Control Policy is based on RPAs in the same consistency group.

The TOE enforces an Information Flow Control Policy on RPAs trying to access replicated data, user data, and configuration data. RPAs can only access replicated data, user data, and configuration data over an allowed network port defined in the Port usage section of the RecoverPoint version 3.4 Security Configuration Guide.

The TOE prevents the loss of user data by transmitting it to physically-separated instances of the TOE in a consistency group for storage on a Storage Array. User data can be accessed by physically-separated instances of the TOE in the event of the failure of a single instance of the TOE.

The TOE is able to roll back replicated data stored on the volumes to the systems and devices with splitters installed.

1.5.2.3 Identification and Authentication

The TOE requires that all TOE users are authenticated by the TOE. The TOE is responsible for identification of all authenticated users.

[11] TSF – TOE Security Functionality

In the evaluated configuration, the TOE only supports local authentication, which requires the use of a username and password.

Administrators can configure a password security level (High or Low) over the CLI using the *set_security_level* command. In the evaluated configuration, the security level shall be set to high. The password security level specifies the password complexity (FIA_SOS.1). All users who fail to authenticate in three successive attempts will be locked out until an administrator unlocks the user's account (FIA_AFL.1).

1.5.2.4 Security Management

The TOE provides administrators with the ability to manage the behavior of security functions and security attributes through the RecoverPoint CLI and the RecoverPoint Management Application GUI. The TOE maintains five roles: Security-admin, Admin, Boxmgmt, Monitor, and Webdownload. The TOE allows users to be assigned to one of the predefined roles or be assigned to permissions that are associated with one or more of the predefined roles. If a user is assigned no permissions or all permissions are removed from a user's role then "monitoring" (read-only) privilege will be assigned. The TOE allows users with permissions associated with the Admin role to manage the attributes associated with the Information Flow Control Policy, Replication Access Control Policy, and the Group Access Control Policy.

1.5.2.5 Protection of the TSF

The TOE is intended to be deployed on a RecoverPoint appliance with other RecoverPoint appliances in a consistency group. If any of the RecoverPoint appliances fail, each of the other RecoverPoint appliances continue to provide continuous data protection for any consistency groups configured to use the failed RecoverPoint appliance.

The TOE provides a reliable time stamp using the hardware clock that is located in the IT[12] environment. The reliable time stamps are used in audit record generation.

1.5.2.6 TOE Access

An administrator can configure the TOE to display a warning banner at the beginning of each login prompt of each session.

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

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

- RecoverPoint appliance hardware;
- Cryptographic operations in OpenSSL and OpenSSH;
- ESRS[13] gateway;
- iDRAC[14] support;
- LDAP support;
- NTP support;
- OMSA[15] support;
- SNMP [16]Protocol v1, and v2;
- Splitters (Intelligent-fabric and Host-splitter driver);

[12] IT – Information Technology
[13] ESRS – EMC Secure Remote Support
[14] iDRAC – Integrated Dell™ Remote Access Controller
[15] OMSA – OpenManage Server Administrator
[16] SNMP – Simple Network Management Protocol

- Syslog support;
- User SE[17]

[17] SE – System Engineer.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 2 - CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009; CC Part 2 extended CC Part 3 conformant; Parts 2 and 3 Interpretations of the CEM[18]as of 2010/05/19 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2 augmented with Flaw Remediation (ALC_FLR.2)

[18] CEM – CC Evaluation Methodology

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

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

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into three categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)
- Natural threats: These are threats to the TSF that are a natural byproduct of the systems that compose the TOE, such as electromagnetic interference on a line during transmission of data.

Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. The following threats are applicable:

Table 3 - Threats

Name	Description
T.DATA_CORRUPTION	Replicated data, user data, and configuration data could become corrupted due to hardware failure or incorrect system operations.
T.IMPROPER_SERVER	A user or attacker may attempt to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.
T.NO_AUDIT	A user or attacker may not be accountable for his actions due to his actions not being recorded or due to an administrator not reviewing the audit records.

3.2 Organizational Security Policies

There are no Organizational Security Policies defined for this ST.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for

delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 4 - Assumptions

Name	Description
A.FIREWALL	All ports required for communication between local and remote TOE installations are open, and the TOE is protected from all other traffic outside the controlled access facility where the TOE is housed.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.PHYSICAL	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.PROTECT	The TOE will be placed in a network infrastructure such that host information to be replicated and restored will always maintain connection to the TOE.
A.ZONING	The TOE will be placed in a SAN which contains sufficient LUN masking and port zoning to not allow unrelated hosts access to RecoverPoint owned LUNs.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 5 - Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must provide a method for administrators to manage the TOE.
O.DEPLOY	When multiple instances of the TOE are deployed in a consistency group, each instance of the TOE must maintain the ability to provide all of its functionality in the event that other instances are added or removed.
O.IDAUTH	The TOE must require that all users be identified and authenticated prior to obtaining access to the TOE.
O.LOG	The TOE must provide a means to record an audit trail of security-related events, with accurate dates and times. The TOE must provide authorized users with the ability to review the audit trail.
O.PROTECT	The TOE must protect replicated data, user data, and configuration data that it has been entrusted to protect.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

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

Table 6 - IT Security Objectives

Name	Description
OE.FIREWALL	The TOE environment must ensure that ports required for communication between local and remote TOE installations are open, and that the TOE is protected from all other traffic outside the controlled access facility where the TOE is housed.
OE.PROPER_NAME_ASSIGNMENT	The TOE environment must provide unique identifiers for each system and device that communicates with the TOE.

Name	Description
OE.SECURE_COMMUNICATION	The TOE environment must provide untampered communications between systems and devices connected to the TOE.
OE.SECURE_SPLITTERS	The TOE environment must provide properly configured systems and devices, which contain splitters, to communicate with the TOE.
OE.TIME	The TOE will have access to a hardware clock from the TOE environment.
OE.ZONING	The TOE environment must ensure that sufficient and restrictive LUN masking and port zoning exists in the SAN to not allow unrelated hosts access to RecoverPoint owned LUNs.

4.2.2 Non-IT Security Objectives

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

Table 7 - Non-IT Security Objectives

Name	Description
NOE.MANAGE	Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.
NOE.NOEVIL	Sites using the TOE shall ensure that TOE administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
NOE.PHYSICAL	The TOE will be used in a controlled access facility that protects it from interference and tampering by untrusted subjects.
NOE.PROTECT	The network infrastructure in which the TOE is placed must be installed, administered and operated in a manner that ensures all hosts to be replicated and restored maintain connection with the TOE.

5 Extended Components

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

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 8 identifies all extended SFRs implemented by the TOE.

Table 8 – Extended TOE Security Functional Requirements

Name	Description
EXT_FDP_ITT.1	Basic recovery transfer protection

5.1.1 Class FDP: User Data Protection

Families in this class address the requirements for TSF and TOE security policies (TSP) related to protecting user data. The extended family "EXT_FDP_ITT: Basic recovery transfer protection" was modeled after FDP_ITT.

5.1.1.1 Basic recovery transfer protection (EXT_FDP_ITT)

Family Behavior

This family defines the set of rules which RecoverPoint uses when accessing user data between separate instances of the TOE.

Component Leveling

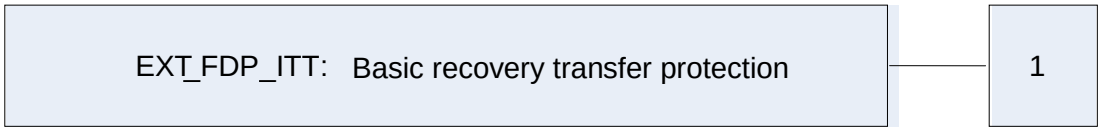

Figure 3 – EXT_FDP_ITT Basic recovery transfer protection family decomposition

EXT_FDP_ITT.1 Basic recovery transfer protection, defines the set of rules which RecoverPoint uses when accessing user data on separate instances of the TOE. It was modeled after FDP_ITT.1.

EXT_FDP_ITT.1 Basic recovery transfer protection

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset Access Control

This component will provide basic recovery transfer protection by preventing loss of use of user data between physically-separated instances of the TOE.

EXT_FDP_ITT.1.1 The TSF shall enforce the [assignment: *access control SFP[19](s) and/or information control SFP(s)*] to prevent the [selection: loss of use] of user data between physically-separated instances of the TOE.

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

[19] SFP – Security Functional Policy

6 Security Requirements

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

6.1.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 - TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FAU_SAR.3	Selectable audit review		✓		
FDP_ACC.1(a)	Subset access control - Splitter		✓		✓
FDP_ACC.1(b)	Subset access control - Group		✓		✓
FDP_ACF.1(a)	Security attribute based access control - Splitter		✓		✓
FDP_ACF.1(b)	Security attribute based access control - Group		✓		✓
EXT_FDP_ITT.1	Basic recovery transfer protection	✓	✓		
FDP_IFC.2	Complete Information Flow Control		✓		
FDP_IFF.1	Simple security attributes		✓		
FDP_ROL.1	Basic rollback		✓		
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.2	User authentication before any action				

Name	Description	S	A	R	I
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓	✓	
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialization	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_FLS.1	Failure with preservation of secure state		✓		
FPT_STM.1	Reliable time stamps				
FTA_TAB.1	Default TOE Access Banners				

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation
Hierarchical to: No other components.
FAU_GEN.1.1
The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events, for the [not specified] level of audit; and
c) [*Authentication attempts (FIA_UAU.2 & FIA_UID.2) and administrative actions (FMT_MSA.1, FMT_MSA.3, FMT_MTD.1)*].
FAU_GEN.1.2
The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no additional information*].
Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review
Hierarchical to: No other components.
FAU_SAR.1.1
The TSF shall provide [*the admin and monitor roles*] with the capability to read [*all audit events*] from the audit records.
FAU_SAR.1.2
The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review
Hierarchical to: No other components.
FAU_SAR.3.1
The TSF shall provide the ability to apply [*methods of selection and ordering*] of audit data based on [*start time, end time, topic, level, search_text, and time zone*].
Dependencies: FAU_SAR.1 Audit review

6.2.2 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control - Splitter
Hierarchical to: No other components.
FDP_ACC.1.1
The TSF shall enforce the [*Replication Access Control SFP*] on [
a) Subjects: *Splitters;*
b) Objects: *Volumes;*
c) Operations: *Read from volumes, Write to volumes;*
].

Dependencies: FDP_ACF.1(a) Security attribute based access control

FDP_ACC.1(b) Subset access control - Group
Hierarchical to: No other components.
FDP_ACC.1.1
The TSF shall enforce the [*Group Access Control SFP*] on [
a) Subjects: *RPAs;*
b) Objects: *Splitters and Volumes;*
c) Operations: *Read from volumes and splitters, Write to volumes and splitters;*
].

Dependencies: FDP_ACF.1(b) Security attribute based access control

FDP_ACF.1(a) Security attribute based access control - Splitter
Hierarchical to: No other components.
FDP_ACF.1.1
The TSF shall enforce the [*Replication Access Control SFP*] to objects based on the following:
[
Subject attributes:
1. *Name of the splitter*
2. *Replication Set*

Object attributes:
1. *WWN*[20] *or LUN*[21]
2. *Replication Set*

].
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 valid Subject of the TOE is allowed to write to an Object if the Subject and Object are members of the same Replication Set.

A valid Subject of the TOE is unable to read from an Object when it is performing writes to the Object.

[20] WWN – World Wide Name
[21] LUN – Logical Unit Number

A valid Subject of the TOE is only able to read from an Object, when the distribution of data from a Subject to an Object has been suspended, and the Subject and Object are members of the same Replication Set.

].

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 [*Splitters in a different replication set and improperly configured splitters*].

Dependencies: **FDP_ACC.1(a) Subset access control**
FMT_MSA.3 Static attribute initialization

FDP_ACF.1(b) Security attribute based access control - Group

Hierarchical to: No other components.

FDP_ACF.1.1

The TSF shall enforce the [*Group Access Control SFP*] to objects based on the following:
[
Subject attributes:
1. *RPA name*

Object attributes:
1. *Name of Splitter and WWN or LUN*

].

FDP_ACF.1.2

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

none.

].

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 rules: [*none*].

Dependencies: **FDP_ACC.1(b) Subset access control**
FMT_MSA.3 Static attribute initialization

FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

FDP_IFC.2.1

The TSF shall enforce the [*Information Flow Control SFP*] on [
subjects:
RPAs;
information:
Replicated data,
user data, and
configuration data
] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2

The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

Dependencies: **FDP_IFF.1 Simple security attributes**

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

FDP_IFF.1.1

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

- *Subjects: RPAs*
  - *Security Attributes:*
    - *Name*
- *Information: Replicated data, user data, configuration data*
  - *Security Attributes:*
    - *Network Ports*
    - *LUN masking*
    - *Zoning*

].

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 RPA can access replicated data, user data, and configuration data, if LUN masking and Zoning techniques are applied properly in case of FC communications, and if the RPA communicates using an allowed network port defined in the Port usage section of the RecoverPoint version 3.4 Security Configuration Guide in case of IP based communications*].

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: [*an RPA may not access replicated data, user data, and configuration data over non-allowed network ports*].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

EXT_FDP_ITT.1 Basic recovery transfer protection

Hierarchical to: No other components.

EXT_FDP_ITT.1.1

The TSF shall enforce the [*Group Access Control SFP*] to prevent the [loss of use] of user data between physically-separated instances of the TOE.

Dependencies: FDP_ACC.1(b) Subset access control

FDP_ROL.1 Basic rollback

Hierarchical to: No other components.

FDP_ROL.1.1

The TSF shall enforce [*Replication Access Control SFP*] to permit the rollback of the [*replicated data*] on the [*volumes*].

FDP_ROL.1.2

The TSF shall permit operations to be rolled back within the [*limitations of storage space on the volumes available for replicated data*].

Dependencies: FDP_ACC.1(a) Subset access control

6.2.3 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components.
FIA_AFL.1.1
The TSF shall detect when [*three*] unsuccessful authentication attempts occur related to [*a user's attempts to establish a new session*].
FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*lockout the user, until a security-admin unlocks the user*].
Dependencies: FIA_UAU.1 Timing of authentication

FIA_SOS.1 Verification of secrets
Hierarchical to: No other components.
FIA_SOS.1.1
The TSF shall provide a mechanism to verify that secrets meet [*the following criteria:*
a) Minimum password length 14 characters;
b) Passwords may only be reset once every 24 hours;
c) Passwords expire every 60 days;
d) Passwords may not be reused until a minimum of ten other passwords have been used;
e) Minimum of four characters must be changed when a new password is created;
f) Password includes at least 2 character from each of the following sets:
1. *Uppercase characters (A-Z);*
2. *Lowercase characters (a-z);*
3. *Numeric characters (0-9);*
4. *Special characters ('(', '!', '@', '#', '$', '%', '^', '*', ')');*

].
Dependencies: No dependencies

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
FIA_UAU.2.1
The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: FIA_UID.1 Timing of identification

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

6.2.4 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
FMT_MOF.1.1
The TSF shall restrict the ability to ~~[selection: determine the behaviour of, disable, enable, modify the behaviour of] the functions~~ **perform the operations** [*listed under the 'Security Functions Behaviour Permissions" column of* Table 10] to [*the authorised identified roles listed under the 'Role" column of* Table 10].
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

Table 10 – Management of Security Functions Behaviour by Role

Role	Security Functions Behavior Permissions
Security-admin	Security: changing users and roles, security levels, and LDAP configuration
Admin	All (Splitter Configuration, Group Configuration, Data Transfer, Target Image, Failover, System Configuration, SNMP Configuration, Upgrade, and Boxmgmt role permissions), except those permissions assigned to the Security-admin and Webdownload roles
Boxmgmt	Install RPAs and appliance maintenance (upgrades)
Monitor	Read only
Webdownload	Download RecoverPoint installation packages from the EMC web site http://www.emc.com

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1
The TSF shall enforce the [*Replication Access Control SFP, Group Access Control SFP*] to restrict the ability to [query, modify, delete, [*create*]] the security attributes [*Splitter Configuration, Group Configuration, Data Transfer, Target Image, and Failover*] to [*users with permissions associated with the Admin role*].
Dependencies: FDP_ACC.1(a) Subset access control
FDP_ACC.1(b) Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation
Hierarchical to: No other components.
FMT_MSA.3.1
The TSF shall enforce the [*Replication Access Control SFP, Group Access Control SFP, Information Flow 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 with permissions associated with the Admin role*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1
The TSF shall restrict the ability to [query, modify, delete, [*create*]] the [*user accounts*] to [*users with permissions associated with the Security-admin role*].

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

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
FMT_SMF.1.1
The TSF shall be capable of performing the following management functions: [
- *Management of Security Functions Behaviour;*
- *Management of Security Attributes;*
- *Management of TSF data*

].
Dependencies: **No Dependencies**

FMT_SMR.1 Security roles
Hierarchical to: No other components.
FMT_SMR.1.1
The TSF shall maintain the roles [*security-admin, admin, boxmgmt, monitor, and webdownload*].
FMT_SMR.1.2
The TSF shall be able to associate users with roles.
Dependencies: **FIA_UID.1 Timing of identification**

6.2.5 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [*failure of one instance of the TOE where multiple instances are present in a consistency group*].
Dependencies: No dependencies.

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
FPT_STM.1.1
The TSF shall be able to provide reliable time stamps.
Dependencies: No dependencies

6.2.6 Class FTA: TOE Access

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

FTA_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE when accessed via RecoverPoint CLI (Command Line Interface).

Dependencies: No dependencies

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 11 - Assurance Requirements summarizes the requirements.

Table 11 - Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM[22] system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

[22] CM – Configuration Management

7 TOE Summary Specification

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

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 12 - Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
User Data Protection	FDP_ACC.1(a)	Subset access control - Splitter
	FDP_ACC.1(b)	Subset access control - Group
	FDP_ACF.1(a)	Security attribute based access control - Splitter
	FDP_ACF.1(b)	Security attribute based access control - Group
	EXT_FDP_ITT.1	Basic recovery transfer protection
	FDP_IFC.2	Complete Information Flow Control
	FDP_IFF.1	Simple security attributes
	FDP_ROL.1	Basic rollback
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions

TOE Security Function	SFR ID	Description
	FMT_SMR.1	Security roles
Protection of TOE Security Functions	FPT_FLS.1	Failure with preservation of secure state
	FPT_STM.1	Reliable time stamps
TOE Access	FTA_TAB.1	Default TOE Access Banners

7.1.1 Security Audit

FAU_GEN.1

The TOE generates audit records for all categories of events listed in Table 13. Audit records without an "Error" level of event are successful. Audit records with an "Error" or "Brief Error" level of event are failures. The TOE audit records contain the following information:

Table 13 - Audit Record Contents

Field	Content
Time	Date and time the audit record was created in MM/DD/YYYY HH:MM:SS format
Event ID	Unique identifier for type of event
Topic	Category of event (Management, Site, RPA, Group, Site, Splitter, or System)
Level	Level of event (Brief Error, Error, Error Off, Info, Warning, or Warning Off)
Description	Provides a description of the event, and includes a subject identity associated with the event (if applicable)

Audit records are retained locally on the RPA on a cyclical basis, with new records replacing older ones after the capacity of 8M is exceeded. Syslog server support has been excluded from the evaluated configuration.

FAU_SAR.1, FAU_SAR.3

The admin and monitor roles can review all audit records through the RecoverPoint CLI and RecoverPoint Management Application GUI. Audit data can be selected for review and ordered based on the following parameters: *start time, end time, topic, level, search_text, and time zone*.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_SAR.3

7.1.2 User Data Protection

FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACF.1(a), FDP_ACF.1(b)

The TOE enforces a Replication Access Control Policy on systems and devices with a RecoverPoint splitter installed, and a Group Access Control Policy on RPAs trying to read or write from the volumes that are configured in the environment for use by the TOE. Access via the Replication Access Policy is based on the Replication Set. RPAs configure a replication set and the splitter performs writes (replicates) to the

configured volume. The Storage Array-based splitter supports volumes up to 32 TB[23]s in size; other splitters are limited to 2 TB-512 MB[24] in size. When the splitter is writing to the configured volume, the volume is inaccessible. Volume access can be enabled only by suspending the distribution of data at the replication volume. To read an image from the volume for which access is to be enabled, the user either selects an image from a list of images, or specifies a specific point-in-time.

Access via the Group Access Control Policy is based on RPAs in the same consistency group. All RPAs in a cluster can access all volumes in all consistency groups, provided the RPA is running the consistency group, which can be assigned by the system at any time. RPAs in the same consistency group are able to read from and write to replication, user, and configuration data.

FDP_IFC.1, FDP_IFF.1

The TOE enforces an Information Flow Control Policy on RPAs trying to access replicated data, user data, and configuration data. RPAs can only access replicated data, user data, and configuration data over an allowed network port defined in the Port usage section of the RecoverPoint version 3.4 Security Configuration Guide.

EXT_FDP_ITT.1

The TOE prevents the loss of user data by transmitting it to physically-separated instances of the TOE for storage on a Storage Array. User data can be accessed by physically-separated instances of the TOE in the event of the failure of a single instance of the TOE as described in 7.1.5.

FDP_ROL.1

The TOE is able to recover replicated data stored on the volumes to the systems and devices with splitters installed. Recovery is permitted within the limitations of storage space on the volumes available for replicated data.

TOE Security Functional Requirements Satisfied: FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACF.1(a), FDP_ACF.1(b), EXT_FDP_ITT.1, FDP_ROL.1

7.1.3 Identification and Authentication

FIA_AFL.1

The TOE is configured by default to lockout a user attempting to establish a new session after three successive unsuccessful attempts. The *security-admin* can unlock the user through the RecoverPoint CLI by running the following command *unlock_user*.

FIA_SOS.1

The TOE provides the capability to enforce strong password restrictions for all users or for specific users as configured by an administrator. An administrator must set the following password restriction parameters, by setting the security level to high, and the TOE will enforce these restrictions.

- *Minimum password length 14 characters;*
- *Passwords may only be reset once every 24 hours;*
- *Passwords expire every 60 days;*
- *Passwords may not be reused until a minimum of ten other passwords have been used;*
- *Minimum of four characters must be changed when a new password is created;*

[23] TB – Terabyte
[24] MB – Megabyte

- *Password includes at least 2 character from each of the following sets:*
  - *Uppercase characters (A-Z);*
  - *Lowercase characters (a-z);*
  - *Numeric characters (0-9);*
  - *Special characters ('(', '!', '@', '#', '$', '%', '^', '*', ')');*

FIA_UAU.2, FIA_UID.2

The TOE requires all users to be successfully identified and authenticated using a username and password. The username and password credentials are checked against a local authentication database. Administrators and users connecting over the RecoverPoint CLI and RecoverPoint Management Application GUI may not perform any TSF-mediated actions until they have been successfully identified and authenticated with valid credentials.

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

7.1.4 Security Management

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1

Administrators can manage the TOE over the RecoverPoint CLI and the RecoverPoint Management Application GUI. Administrators may also configure alerts for specified events over email when SMTP[25] settings are enabled and over SNMP when SNMP traps have been configured. Syslog server notification has been excluded from this evaluation. Table 10 provides a list of all roles with their associated security function behavior permissions.

Administrators can manage security attributes associated with the Replication Access Control Policy and Group Access Control Policy. Only the Admin role has all permissions required to manage these security attributes. The Replication Access Control Policy, by default, does not permit any device splitters to replicate to or restore from the volumes configured by the TOE unless they are assigned to the same replication set. The Group Access Control Policy, by default, does not allow any RPAs to communicate with Splitters and Volumes configured by the TOE unless they are members of the same consistency group. The Information Flow Control Policy, by default, does not not allow any RPAs to access replicated data, user data, or configuration data unless they use an allowed network port defined in the Port usage section of the RecoverPoint version 3.4 Security Configuration Guide.

The ability to create, delete, modify, and query user accounts is restricted to the Security-admin role or users assigned with the Security permission.

FMT_SMR.1

The TOE provides five roles by default: security-admin, admin, boxgmt, monitor, and webdownload. Each role has a predefined set of permissions listed in Table 10 that cannot be changed. Security-admins have the option of assigning users to a predefined role or assigning users permissions directly. By assigning a role to users, the users will receive all the access permissions defined by the role. If users are assigned permissions directly then they may be granted or denied the following permissions listed below in Table 14.

Table 14 – Permissions that may be granted or denied to users

Permission	Description

[25] SMTP – Simple Mail Transfer Protocol

Permission	Description
Splitter Configuration	Add or remove splitters, and attach or detach splitters to volumes.
Group Configuration	Create and remove consistency groups; modify all group settings except those that are included in the data transfer, target image, and failover permissions; bookmark images; resolve settings conflicts.
Data Transfer	Enable and disable access to image, and undo writes to the image access log.
Target Image	Enable and disable access to an image, resume distribution, and undo writes to the image access log.
Failover	Modify replication direction (use temporary and permanent failover), initiate failover, and verify failover.
System Configuration	Configure and manage e-mail alerts, SNMP, System Reports, rules, licenses, serial ID, account ID, syslog, and other system configuration parameters.
Security	Initiate all commands dealing with roles, users, LDAP configuration, and security level.
Upgrade	Install RPA software; RPA maintenance, including upgrading to a minor RecoverPoint release, upgrading to a major release, replacing an RPA, and adding new RPAs.
Web download	Download RecoverPoint installation packages from the EMC web site.

Note: If none of the above permissions are granted or all of the above permissions are removed "monitoring" (read-only) privilege will be assigned.

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

7.1.5 Protection of the TSF

FPT_FLS.1

The TOE protects itself from reaching a non-secure state when a RecoverPoint appliance in a consistency group fails. Due to the high demand of the TOE to provide continuous data replication, this may occur from time to time. When the failure occurs, other RecoverPoint appliances in the consistency group retain all functionality and all TSFs remain in a secure state.

FPT_STM.1

The TOE provides a reliable time stamp using the hardware clock that is located in the IT environment. The reliable time stamps are used in audit record generation.

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

7.1.6 TOE Access

FTA_TAB.1

The TOE provides the ability to display a logon banner (showing an administrator-configured message) when any user attempts to access the management interfaces (RecoverPoint CLI and RecoverPoint Management Application GUI) of the system.

TOE Security Functional Requirements Satisfied: FTA_TAB.1

8 Rationale

8.1 Conformance Claims Rationale

There are no protection profile claims for this ST.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 15 - Threats:Objectives Mapping

Threats	Objectives	Rationale
T.DATA_CORRUPTION Replicated data, user data, and configuration data could become corrupted due to hardware failure or incorrect system operations.	O.ADMIN The TOE must provide a method for administrators to manage the TOE.	O.ADMIN counters this threat by allowing administrators to properly configure the TOE replication settings to prevent data corruption and restrict access to authorized individuals.
	OE.FIREWALL The TOE environment must ensure that ports required for communication between local and remote TOE installations are open, and that the TOE is protected from all other traffic outside the controlled access facility where the TOE is housed.	OE.FIREWALL mitigates this threat by preventing unauthorized connections to the TOE from outside of the controlled access facilities where the TOE installations reside
	O.DEPLOY When multiple instances of the TOE are deployed in a consistency group, each instance of the TOE must maintain the ability to provide all of its functionality in the event that other instances are added or removed.	O.DEPLOY mitigates this threat by maintaining the ability for the TOE to provide all of its functionality in the event other instances in a consistency group are removed due to hardware failure.
	O.PROTECT The TOE must protect replicated data, user data, and configuration data that it has been entrusted to protect.	O.PROTECT counters this threat by providing mechanisms to protect the replicated data, user data, and configuration data
	OE.ZONING The TOE environment must ensure that sufficient and	OE.ZONING mitigates this threat by preventing unrelated hosts access to RecoverPoint owned

Threats	Objectives	Rationale
	restrictive LUN masking and port zoning exists in the SAN to not allow unrelated hosts access to RecoverPoint owned LUNs.	LUNs to avoid possible corruption of data.
T.IMPROPER_SERVER A user or attacker may attempt to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	O.ADMIN The TOE must provide a method for administrators to manage the TOE.	O.ADMIN counters this threat by allowing administrators to properly configure the mechanisms of the TOE designed to control the Group Access Control SFP and Replication Access Control SFP.
	OE.PROPER_NAME_ASSIGNMENT The TOE environment must provide unique identifiers for each system and device that communicates with the TOE.	OE.PROPER_NAME_ASSIGNMENT counters this threat by ensuring that unique identifiers provided to the TOE are accurate. This allows the mechanisms provided by O.PROTECT to properly protect data.
	O.IDAUTH The TOE must require that all users be identified and authenticated prior to obtaining access to the TOE.	O.IDAUTH counters this threat by ensuring that all users and administrators must be authenticated and identified before allowing use of the TOE or resources in the TOE environment.
	OE.SECURE_COMMUNICATION The TOE environment must provide untampered communications between systems and devices connected to the TOE.	OE.SECURE_COMMUNICATION counters this threat by ensuring that all communications with the TOE are untampered for administration of the TOE and data sent to or from the TOE.
	OE.SECURE_SPLITTERS The TOE environment must provide properly configured systems and devices, which contain splitters, to communicate with the TOE.	OE.SECURE_SPLITTERS counters this threat by ensuring all systems and devices connected to the TOE remain properly configured when communicating with the TOE.
	O.PROTECT The TOE must protect replicated data, user data, and configuration data that it has been entrusted to protect.	O.PROTECT counters this threat by requiring the TOE to protect itself from unauthorized access to replicated data, user data, and configuration data that it has been entrusted to protect.
T.NO_AUDIT A user or attacker may not be accountable for his actions due to his actions not being recorded or	O.LOG The TOE must provide a means to record an audit trail of security-related events, with	O.LOG counters this threat by ensuring that an audit trail of security-related events on the TOE is preserved, and authorized

Threats	Objectives	Rationale
due to an administrator not reviewing the audit records.	accurate dates and times. The TOE must provide authorized users with the ability to review the audit trail.	users are provided the ability to review the audit trail.
	OE.TIME The TOE will have access to a hardware clock from the TOE environment.	OE.TIME counters this threat by ensuring that the operating environment will provide a hardware clock used by the TOE to provide a reliable time stamp when generating the audit records.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no Organizational Security Policies defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 16 - Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.FIREWALL All ports required for communication between local and remote TOE installations are open, and the TOE is protected from all other traffic outside the controlled access facility where the TOE is housed.	OE.FIREWALL The TOE environment must ensure that ports required for communication between local and remote TOE installations are open, and that the TOE is protected from all other traffic outside the controlled access facility where the TOE is housed.	OE.FIREWALL satisfies this assumption by ensuring that the necessary ports for replication are open and the TOE is protected from all other traffic outside the controlled access facility.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	NOE.MANAGE Sites deploying the TOE will provide competent TOE administrators who will ensure the system is used securely.	NOE.MANAGE satisfies this assumption by ensuring competent TOE administrators will be assigned to manage the TOE and the security of the information.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	NOE.NOEVIL Sites using the TOE shall ensure that TOE administrators are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.	NOE.NOEVIL satisfies this assumption by ensuring that TOE administrators who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.PHYSICAL	NOE.PHYSICAL	OE.PHYSICAL satisfies this

Assumptions	Objectives	Rationale
The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	The TOE will be used in a controlled access facility that protects it from interference and tampering by untrusted subjects.	assumption by ensuring the TOE will be located in a controlled access facility that protects it from interference and tampering.
A.PROTECT The TOE will be placed in a network infrastructure such that host information to be replicated and restored will always maintain connection to the TOE.	NOE.PROTECT The network infrastructure in which the TOE is placed must be installed, administered and operated in a manner that ensures all hosts to be replicated and restored maintain connection with the TOE.	NOE.PROTECT satisfies this assumption by ensuring that hosts to be replicated and restored will always be connected to the TOE.
A.ZONING The TOE will be placed in a SAN which contains sufficient LUN masking and port zoning to not allow unrelated hosts access to RecoverPoint owned LUNs.	OE.ZONING The TOE environment must ensure that sufficient and restrictive LUN masking and port zoning exists in the SAN to not allow unrelated hosts access to RecoverPoint owned LUNs.	OE.ZONING satisfies this assumption by ensuring the TOE is placed in a SAN which contains sufficient LUN masking and port zoning to not allow unrelated hosts access to RecoverPoint owned LUNs.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

EXT_FDP_ITT.1: Basic recovery transfer protection was created to address the user data storage capability between separate instances of the TOE. The repository volume which is an environmental component in the evaluated configuration assists with the replication of user data between separate instances of the TOE. The FDP_ITT.1 SFR: Basic internal data protection was used as a model for creating this SFR. This requirement has dependencies on FDP_ACC.1 to ensure only TOE instances controlled by an SFP have access to this functionality. This requirement exhibits functionality that can be easily documented in the ADV assurance evidence and thus does not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs defined for this ST.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 17 - Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must provide a method for administrators to manage the TOE.	FMT_MOF.1 Management of security functions behaviour	FMT_MOF.1 supports this objective by specifying what roles can modify the behavior of, enable, disable, and determine the behavior of the TSF.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 supports this objective by specifying the security attributes of the TOE that can be modified and which administrative permissions can modify them.
	FMT_MSA.3 Static attribute initialization	FMT_MSA.3 supports this objective by specifying the restrictive default values that are used by the Replication Access Control Policy and Group Access Control Policy, and specifying which administrative permissions can configure alternate values.
	FMT_MTD.1 Management of TSF data	FMT_MTD.1 supports this objective by restricting the ability to manage TSF data to specific permissions associated with the Security-admin role.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 supports this objective by specifying the management functions used to securely manage the TOE.
	FMT_SMR.1 Security roles	FMT_SMR.1 supports this objective by maintaining the roles of security-admin, admin, boxmgmt, monitor, and webdownload.
O.DEPLOY When multiple instances of the TOE are deployed in a consistency group, each instance of the TOE must maintain the ability to provide all of its functionality in the event that other instances are added or removed.	EXT_FDP_ITT.1 Basic recovery transfer protection	EXT_FDP_ITT.1 supports this objective by preventing the loss of use of user data between physically separated instances of the TOE.
	FPT_FLS.1 Failure with preservation of secure state	FPT_FLS.1 supports this objective by ensuring the preservation of a secure state when a failure of one instance of the TOE occurs, when multiple instances are present.

Objective	Requirements Addressing the Objective	Rationale
O.IDAUTH The TOE must require that all users be identified and authenticated prior to obtaining access to the TOE.	FIA_AFL.1 Authentication failure handling	FIA_AFL.1 supports this objective by requiring users to identify and authenticate themselves within three attempts or they will be locked out.
	FIA_SOS.1 Verification of secrets	FIA_SOS.1 supports this objective by requiring users to identify and authenticate themselves with a strong password.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 supports this objective by requiring that each ser be successfully authenticated before allowing any actions on behalf of that user.
	FIA_UID.2 User identification before any action	FIA_UID.2 supports this objective by requiring that each ser be successfully identified before allowing any actions on behalf of that user.
	FTA_TAB.1 Default TOE Access Banners	FTA_TAB.1 supports this objective by allowing the administrator to configure the TOE to display a warning message prior to the login prompt for each session.
O.LOG The TOE must provide a means to record an audit trail of security-related events, with accurate dates and times. The TOE must provide authorized users with the ability to review the audit trail.	FAU_GEN.1 Audit Data Generation	FAU_GEN.1 supports this objective by providing an audit trail listing all security-related events.
	FAU_SAR.1 Audit review	FAU_SAR.1 supports this objective by presenting audit records in a readable format so that authorized users can review the audit trail.
	FAU_SAR.3 Selectable audit review	FAU_SAR.3 supports this objective by allowing authorized users to apply methods of selection (start time, end time, topic, level, search_text, and time zone) while reviewing the audit trail.
	FPT_STM.1 Reliable time stamps	FPT_STM.1: The TOE provides a reliable time stamp for use in generating audit records so that a timeline of events can be created to provide user accountability. The TOE relies upon the IT

Objective	Requirements Addressing the Objective	Rationale
		environment to provide the hardware clock.
O.PROTECT The TOE must protect replicated data, user data, and configuration data that it has been entrusted to protect.	FDP_ACC.1(b) Subset access control - Group	FDP_ACC.1(b) supports this objective by ensuring that only authorized subjects gain access to the replicated data, user data, and configuration data the TOE has been entrusted to protect.
	FDP_ACC.1(a) Subset access control - Splitter	FDP_ACC.1(a) supports this objective by ensuring that only authorized subjects gain access to the replicated data, user data, and configuration data the TOE has been entrusted to protect.
	FDP_ACF.1(b) Security attribute based access control - Group	FDP_ACF.1(b) supports this objective by enforcing a Group Access Control Policy so that only authorized subjects gain access to the replicated data, user data, and configuration data the TOE has been entrusted to protect.
	FDP_ACF.1(a) Security attribute based access control - Splitter	FDP_ACF.1(a) supports this objective by enforcing a Replication Access Control Policy so that only authorized subjects gain access to the replicated data, user data, and configuration data the TOE has been entrusted to protect.
	FDP_IFF.1 Simple security attributes	FDP_IFF.1 supports this objective by enforcing an Information Flow Control Policy so that only authorized subjects using specified network ports gain access to the replicated data, user data, and configuration data the TOE has been entrusted to protect.
	FDP_IFC.2 Complete Information Flow Control	FDP_IFC.2 supports this objective by enforcing an Information Flow Control Policy so that only authorized subjects using specified network ports gain access to the replicated data, user data, and configuration data the TOE has been entrusted to protect.
	FDP_ROL.1 Basic rollback	FDP_ROL.1 supports this objective by allowing rollback of the replicated data the TOE has

Objective	Requirements Addressing the Objective	Rationale
		been trusted to protect.

8.5.2 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2+, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 18 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 18 - Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FDP_ACC.1(a)	FDP_ACF.1(a)	✓	
FDP_ACC.1(b)	FDP_ACF.1(b)	✓	
FDP_ACF.1(a)	FDP_ACC.1(a)	✓	
FDP_ACF.1(b)	FMT_MSA.3	✓	
	FDP_ACC.1(b)	✓	
FDP_ACF.1(a)	FMT_MSA.3	✓	
EXT_FDP_ITT.1	FDP_ACC.1(b)	✓	
FDP_IFC.2	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	FDP_IFC.2 is hierarchical to FDP_IFC.1.
	FMT_MSA.3	✓	
FDP_ROL.1	FDP_ACC.1(a)	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FIA_AFL.1	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1 is included. This satisfies this dependency.
FIA_SOS.1	None	Not applicable	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UID.2	None	Not applicable	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1(a)	✓	
	FDP_ACC.1(b)	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_SMF.1	None	Not applicable	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_FLS.1	None	Not applicable	
FPT_STM.1	None	Not applicable	
FTA_TAB.1	None	Not applicable	

9 Acronyms

This section describes the acronyms.

9.1 Acronyms

Table 19 - Acronyms

Acronym	Definition
CC	Common Criteria
CDP	Continuous Data Protection
CEM	CC Evaluation Methodology
CLI	Command Line Interface
CLR	Concurrent Local and Remote Replication
CM	Configuration Management
CPU	Central Processing Unit
CRR	Continuous Remote Replication
EAL	Evaluation Assurance Level
ESRS	EMC Secure Remote Support
FC	Fibre Channel
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
iDRAC	Integrated Dell™ Remote Access Controller
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
NTP	Network Time Protocol
OMSA	OpenManage Server Administrator
PP	Protection Profile
RPA	RecoverPoint Appliance
SAN	Storage Area Network
SAR	Security Assurance Requirement
SE	System Engineer
SFP	Security Function Policy

Acronym	Definition
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TB	Terabyte
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
WAN	Wide Area Network

Prepared by:
Corsec Security, Inc.

10340 Democracy Lane, Suite 201
Fairfax, VA 22030

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