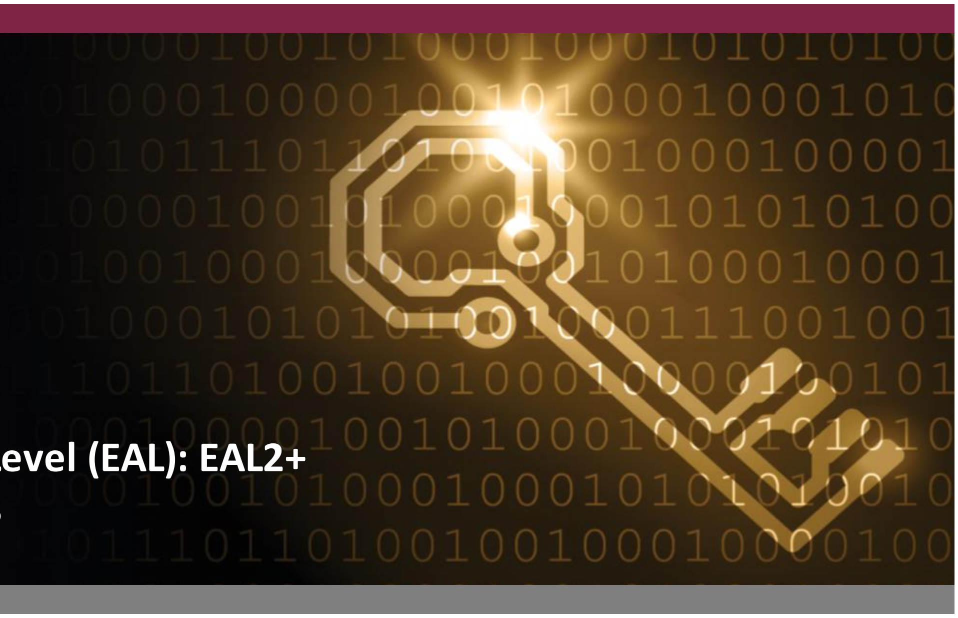
Veritas Technologies

Veritas NetBackup

v9.1.0.1



Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.3

Prepared for:

Veritas Technologies
2625 Augustine Drive
Santa Clara, California 95054
United States of America

Phone: +1 866 837 4827
www.veritas.com

Prepared by:

Corsec Security, Inc.
12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Figures

List of Tables

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the Veritas Technologies (Veritas) NetBackup v9.1.0.1 and will hereafter be referred to as the TOE throughout this document. The TOE is an enterprise data backup and recovery solution that provides cross-platform backup functionality for a variety of Windows and Linux operating systems.

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 functionality 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), Protection Profile (PP), 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 to which the TOE adheres.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the SFRs 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 shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	*Veritas Technologies Veritas NetBackup v9.1.0.1 Security Target*
ST Version	Version 1.3
ST Author	Corsec Security, Inc.
ST Publication Date	2024-05-08
TOE Reference	Veritas NetBackup v9.1.0.1

1.3 TOE Overview

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

Veritas NetBackup is an enterprise data backup and recovery type of TOE. It provides cross-platform backup functionality for a variety of Windows and Linux operating systems. TOE users can set up periodic or calendar-based schedules to perform automatic, unattended backups for clients across a network. A TOE user can carefully schedule backups to achieve systematic and complete backups over a period of time and optimize network traffic caused by the backups during off-peak hours. The TOE includes both server and client software including the following:

- NetBackup Primary Server – This software component resides on a computer that is used to manage the backups, archives, and restores, and is responsible for selecting the NetBackup Media Server to which data is backed-up. The Primary Server contains all binaries and services to allow it to serve in the roles of the Media Server and Client, in addition to its primary function. The NetBackup Primary Server contains the NetBackup catalog, which contains the internal databases with information about NetBackup's backed-up data and configuration.
- NetBackup Media Server – This software component resides on the servers or appliances that are used to store the backed-up data. With two or more NetBackup Media Servers, the network load can be distributed, and performance increased.
- NetBackup Windows Client and NetBackup Linux Client – These software components reside on computers that contain data that needs to be backed up.
- NetBackup Remote Administration Console – This software component resides on a Windows computer that is used to manage the TOE's functionality.
- NetBackup Local Administration Console - This software component resides on the same computer as the Primary Server and is used to manage the TOE's functionality.

TOE users are able to authenticate to the NetBackup Remote Administration Console, NetBackup Local Administration Console, Web User Interface (UI), and Command Line Interface (CLI) to manage the TOE. Using these interfaces, TOE users connect to the NetBackup Primary Server to have access to review audit records, manage encryption policies, manage backup policies, restore data from backups, and manage local accounts.

When creating backup policies to control how data on managed systems is backed up, a TOE user must specify the required security attributes to successfully create a backup policy. The TOE will enforce the backup policy on any system the policy is applied to.

During a backup, the target NetBackup Client sends information to the NetBackup Primary Server. The NetBackup Primary Server manages the location of storage that is specified in the backup policy and ensures that the backup data is encrypted for storage. Backups that are created by the TOE are encrypted using the TOE's Federal Information Processing Standards (FIPS)-validated cryptography (https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2340.pdf) certificate 2340. During a restore, TOE users can browse, and then select, the files and directories to recover. The TOE finds the selected files and directories, decrypts them, and restores them to the disk on the target NetBackup Client's system.

The TOE will generate audit events for various security-related operations that take place within the TOE. The TOE will provide its own timestamp to any audit events that it generates to ensure the timing of the event is reliable. Audit events can be reviewed by TOE users and filtered to allow comprehensive review of the audit data.

1.4 TOE Environment

Table 2 specifies the system requirements for the TOE environment that hosts the various parts of the TOE. The TOE environment will also require any networking equipment needed to allow the TOE components to communicate with each other.

Table 2 – TOE Environment Minimum Requirements

Category	Requirements
NetBackup Primary Server/NetBackup Local Administration Console	General purpose computer hardware • 4 CPU cores • 16 GB RAM Red Hat Enterprise Linux (RHEL) 7.9
NetBackup Media Servers	General purpose computer hardware • 4 CPU cores • 32 GB RAM Windows Server 2019
	NetBackup 5250 Appliance • NetBackup Appliance OS v4.1
	Flex 5350 Appliance • Flex Appliance OS v2.1
NetBackup Linux Client	General purpose computer hardware • RHEL minimum requirements (https://access.redhat.com/articles/rhel-limits) RHEL 7.9
NetBackup Windows Client	General purpose computer hardware • Window Server 2019 minimum requirements (https://learn.microsoft.com/en-us/windows-server/get-started/hardware-requirements) Windows Server 2019
NetBackup Remote Administration Console	General purpose computer hardware • Windows 10 minimum requirements (https://support.microsoft.com/en-us/windows/windows-10-system-requirements-6d4e9a79-66bf-7950-467c-795cf0386715) Windows 10
Cryptographic Support	The host system for the TOE contains a cryptographic module that provides cryptographic services to the TOE.

For this evaluation, the TOE was tested with the NetBackup 5250 Appliance and Flex 5350 Appliance simultaneously in the environment. However, the TOE also runs on the following appliances with the same functionality as the evaluated configurations, but they have not been evaluated: NetBackup 5240, 5330, 5340, 5330HA, and 53440HA Appliances and Flex 5150, 5250, and 5340 Appliances. The TOE can run with any combination of media servers configured in the environment.

In the evaluated configuration, the NetBackup Primary Server, with the NetBackup Local Administration Console included, runs on RHEL. Although it can also run on Windows Server 2019 or one of the appliances with the same functionality, running it on a non-RHEL host has not been evaluated. Similarly, the NetBackup Media Server can run on Windows or RHEL but has not been evaluated on RHEL.

1.5 TOE Description

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

1.5.1 Physical Scope

Figure 1 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

The TOE is a data backup solution running on multiple hardware platforms in the environment that are compliant to the requirements listed in Table 2. The TOE is installed on an internal network as depicted in Figure 1.

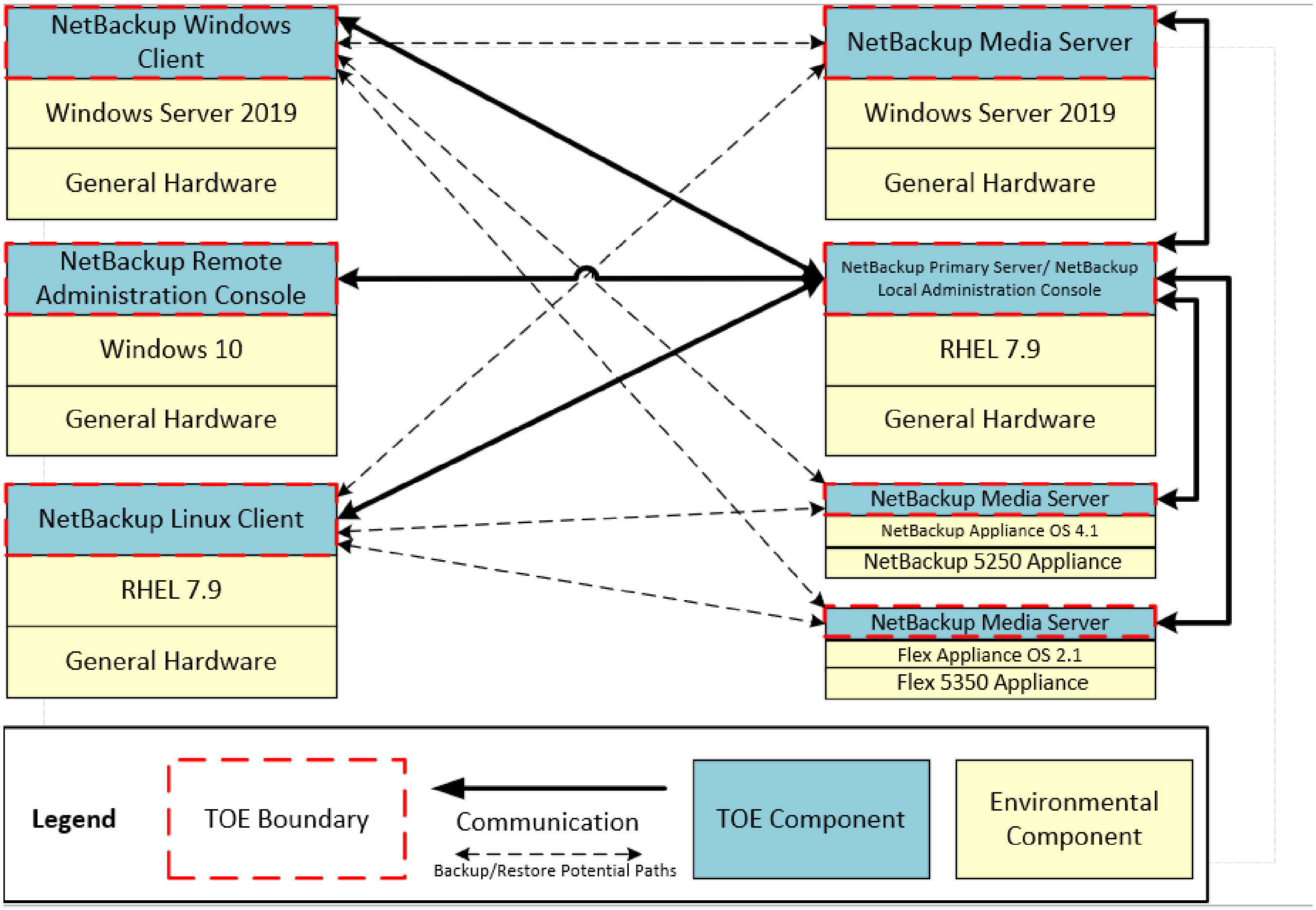


Figure 1 – Physical TOE Boundary

1.5.1.1 TOE Software

The TOE is a software-only TOE and is comprised of the following components:

- Veritas NetBackup v9.1.0.1 Primary Server software in *.tar.gz format.
- Veritas NetBackup v9.1.0.1 Media Server software in *.zip format.
- Veritas NetBackup v9.1.0.1 Media Server software pre-installed on an appliance.
- Veritas NetBackup v9.1.0.1 Windows Client software in *.zip format.
- Veritas NetBackup v9.1.0.1 Linux client software in *.tar.gz format.

- Veritas NetBackup v9.1.0.1 Remote Administration Console software in *.zip format.

Media Server software pre-installed on an appliance is delivered to customers via a trusted courier, such as FedEx. Software delivered for the TOE can be downloaded from the Veritas Support website as the following files: `NetBackup_9.1.0.1_LinuxR_x86_64.tar.gz` and `NetBackup_9.1.0.1_Win.zip`.

All relevant security hotfixes must be installed in order to maintain TOE security. Administrators should monitor TOE hotfixes releases and install the updates as soon as possible. TOE hotfixes do not alter the version of the TOE, therefore all relevant hotfixes can be applied without removing the TOE from the evaluated configuration.

Hotfixes for the TOE software and environmental components can be found on their respective downloads pages:

NetBackup 9.1.0.1	https://www.veritas.com/content/support/en_US/downloads/detail.REL249692#item3
Flex 5350 Appliance OS v2.1	https://www.veritas.com/content/support/en_US/downloads/detail.REL172090#item3
NetBackup 5250 Appliance OS v4.1	https://www.veritas.com/content/support/en_US/downloads/detail.REL617964#item3

The TOE includes the following patches:

- VTS22-004 HotFix for Security Advisory Impacting NetBackup – Primary/Media Server
- VTS22-008 HotFix for Security Advisory Impacting NetBackup Client

1.5.1.2 Guidance Documentation

The following PDF[1] formatted guides, that are available for download through the Veritas website, are required reading and part of the TOE:

- NetBackup Web UI Administrator’s Guide Release 9.1
- Veritas NetBackup Administrator’s Guide, Volume I, UNIX, Windows, and Linux, Release 9.1
- Veritas NetBackup Administrator’s Guide, Volume II, UNIX, Windows, and Linux, Release 9.1
- Veritas NetBackup Commands Reference Guide, UNIX, Windows, and Linux, Release 9.1
- Veritas NetBackup Troubleshooting Guide, UNIX, Windows, and Linux, Release 9.1
- Veritas NetBackup Installation Guide, UNIX and Windows, Release 9.1
- Veritas NetBackup Status Codes Reference Guide, UNIX, Windows, and Linux, Release 9.1
- Veritas NetBackup Security and Encryption Guide, UNIX, Windows, and Linux, Release 9.1
- Veritas Technologies Veritas NetBackup Guidance Supplement v1.1

Additionally, the following PDF formatted guides, that are available for download through the Veritas website, are required reading and are part of the TOE environment:

- Veritas NetBackup™ 52xx Appliance Initial Configuration Guide, Release 4.1
- Flex Appliance Getting Started and Administration Guide, Release 2.1

[1] PDF – Portable Document Format

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The SFRs 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 TOE Security Functionality (TSF)

1.5.2.1 Security Audit

Audit entries are generated by the TOE for events related to TSF mediating actions, starting up the TOE, and shutting down the TOE. The recorded events include relevant information to the event include the identity of the TOE user that initiated the action. Audit entries may be reviewed by authorized TOE users. While reviewing the audit data, filters may be applied to control what is being displayed.

1.5.2.2 User Data Protection

The TOE provides backup and restore functionality to TOE users that are controlled using backup policies. Backup policies are access controlled by the TOE to ensure that only authorized TOE users may query, create, modify, or delete them. The TOE will determine access to the backup policies based on the security attributes of the TOE user's account and the backup policy.

1.5.2.3 Identification and Authentication

The TOE ensures that access to TSF-mediated actions is only provided to TOE users that are authenticated and identified before any actions take place within the TOE. While entering a password into the password fields of the TOE, the TOE will obfuscate the input.

1.5.2.4 Security Management

The TOE provides the following management functionality: audit reviewing, managing encryption policies, managing backup policies, restoring backup data, and managing local accounts. When accessing the TOE to manage these areas, the TOE will associate TOE users to the roles that it maintains. This ensures that TOE users will be restricted to the areas of the TOE for which their roles have access. When managing the backup policies or local accounts, the TOE enforces access control on which roles are able to manage the security attributes for the backup policies and local accounts.

1.5.2.5 Protection of the TSF

To ensure audit records have the correct time, the TOE will provide a reliable timestamp.

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

Any functionality of the TOE not discussed herein is considered to be outside the scope of the evaluation and has not been tested against Common Criteria standards.

The following features and/or functionality that are not part of the evaluated configuration of the TOE are:

- Disabling Enhanced Auditing

The following user roles are excluded from this evaluation:

- Default AHV Administrator
- Default Cloud Administrator
- Default Kubernetes Administrator
- Default NetBackup Kubernetes Operator Service
- Default Resiliency Administrator
- Default Microsoft SQL Server Administrator
- Custom RBAC roles

2. Conformance Claims

This section and Table 3 provide the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017; CC Part 2 extended; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL 2 augmented with Flaw Remediation (ALC_FLR.2)

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 to 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[2] assets against which protection is required by the TOE or by the security environment. The threat agent is an Attacker who is not an administrator of the TOE, does not have account credentials, nor direct physical access to the TOE. Attackers possess a level of knowledge of the TOE, skill level and commensurate to the claimed EAL. The IT assets requiring protection are the TSF[3] and data saved on or transitioning through the TOE. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 4 lists the applicable threats.

Table 4 – Threats

Name	Description
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential unauthorized data accesses to go undetected.
T.PRIVILEGE	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.UNAUTH	An unauthorized user may attempt to access backup data which could result in the loss of sensitive information.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. Table 5 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

Table 5 – Organizational Security Policies

Name	Description
P.ACCOUNT	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.BACKUP	The TOE shall backup specified client data and make it available for restore operations.
P.MANAGE	The TOE shall be managed only by authorized users.

[2] IT – Information Technology

[3] TSF – TOE Security Functionality

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. Table 6 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 – Assumptions

Name	Description
A.CRYPTO	It is assumed that the TOE's operational environment is providing cryptographic support.
A.MANAGE	It is assumed that there are one or more competent individuals assigned to manage the TOE. These users are not careless, willfully negligent, or hostile. They are appropriately trained and will follow the instructions provided by the TOE documentation.
A.NETWORK	It is assumed that the TOE components and their hosts are installed on an internal network which protects the data from disclosure and modification by untrusted systems or users.
A.PROTECT	It is assumed that the hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical access.
A.TIMESTAMPS	It is assumed that the TOE's operational environment is providing a reliable timestamp.

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 listed in Table 7.

Table 7 – Security Objectives for the TOE

Name	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 necessary to support the administrators in their management of the security of the TOE and restrict these functions from unauthorized use.
O.AUDIT	The TOE must generate audit records for security related events.
O.BACKUP	The TOE shall backup specified client data and make it available for restore operations.
O.CRYPTO	Backup data must be protected using approved cryptographic functions.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.PROTECT	The TOE must ensure the integrity of all TSF data, including audit records, by protecting itself from unauthorized access.
O.TIME	The TOE must provide reliable timestamps.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 8 lists the IT security objectives that are to be satisfied by the environment.

Table 8 – IT Security Objectives

Name	Description
OE.CRYPTO	The operational environment will provide cryptographic support to the TOE with a FIPS-validated cryptographic module (Certificate #2340).
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
OE.NETWORK	The operational environment will provide a segregated, internal network that protects the traffic that passes between the TOE components from disclosure and modification by untrusted systems or users.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
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.TIMESTAMPS	The operational environment receives the reliable timestamp from an NTP server through an encrypted channel.

4.2.2 Non-IT Security Objectives

There are no Non-IT Security Objectives defined for this ST.

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.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 9 identifies all extended SFRs implemented by the TOE.

Table 9 – Extended TOE Security Functional Requirements

Name	Description
FDP_BCK_EXT.1	User data backup/restore

5.1.1 Family FDP_BCK_EXT: User Data Backup/Restore

User data backup/restore provides for the functionality to perform backup and restore operations as directed by administrators and users. The User data backup/restore family was modeled after FDP_ACC: Access Control Policy. The User data backup/restore SFR was loosely modeled after FDP_ACC.1: Subset access control.

5.1.1.1 User Data Backup/Restore (FDP_BCK_EXT.1)

Family Behavior

This family defines the requirements for the TOE to provide backup and restore services for IT systems in the operational environment.

Component Leveling

FDP_BCK_EXT: User Data Backup/Restore
1

Figure 2 – FDP_BCK_EXT: User Data Backup/Restore Component Levelling

FDP_BCK_EXT.1 User data backup/restore, provides the functionality to perform backup and restore operations on user data.

Management: FDP_BCK_EXT.1
The following actions could be considered for the management functions in FMT:

- Configuration of the backup and restore operations to be performed.

Audit: FDP_BCK_EXT.1
There are no auditable events foreseen.

FDP_BCK_EXT.1 User data backup/restore

FDP_BCK_EXT.1.1

The TSF shall provide a capability to backup data and systems in accordance with the backup policy configured by authorized administrators.

FDP_BCK_EXT.1.2

The TSF shall provide a capability for authorized administrators to restore files to systems from previously created backups.

5.2 Extended TOE Security Assurance Components

This ST does not include extended Security Assurance Requirements.

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.

6.1 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 [<u>underlined text within brackets</u>].
- Completed assignment statements within a selection statement are identified using [<u>*underlined and italicized text within brackets*</u>].
- 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 end 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 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_GEN.2	User Identity Association				
FAU_SAR.1	Audit review		✓		
FAU_SAR.3	Selectable audit review		✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FDP_BCK_EXT.1	User data backup/restore				
FIA_UAU.2	User authentication before any action				
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.2	User identification before any action				
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_SMF.1	Specification of management functions		✓		

Name	Description	S	A	R	I
FMT_SMR.1	Security roles		✓		
FPT_STM.1	Reliable time stamps				

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

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. [*TSF-related auditable events listed in Table 11*].

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, [*the audit events will include the relevant information listed in Table 12*].

Table 11 – TSF-Related Audit Events

Event Type	Audited Actions
Policy	Adding, deleting, or updating policy attributes, clients, schedules, and backup selections lists
Activity monitor	Canceling, suspending, resuming, restarting, or deleting any type of job
Storage units	Adding, deleting, or updating storage units
Storage servers	Adding, deleting, or updating storage servers
Disk pools and volume pools	Adding, deleting, or updating disk or volume pools
Catalog information	Includes verifying and expiring images
User management	Adding and deleting users in the Enhanced Auditing mode
Host database	NetBackup host database related operations
Login attempts	Any successful or failed login attempts for NetBackup Remote Administration Console and NetBackup Local Administration Console
Security configuration	Information related to changes made to the security configuration settings
Starting a restore job	Starting a restore job
Starting and stopping the NetBackup Audit Manager (nbaudit)	Starting and stopping of the nbaudit manager is always audited, even if auditing is disabled. An audit event indicating nbaudit has stopped indicates that the TOE is not in the evaluated configuration.

Table 12 – Audit Record Contents

Field	Content	Notes
DESCRIPTION	The details of the action that was performed. The details include the new values that are given to a modified object and the new values of all attributes for a newly created object. The details also include the identification of any deleted objects.	N/A
USER	The identity of the user who performed the action. The identity includes the username, the domain, and the domain type of the authenticated user. This is only available in enhanced auditing mode.	N/A
TIMESTAMP	The time that the action was performed. The time is given in Coordinated Universal Time (UTC) and indicated in seconds.	N/A
CATEGORY	The category of user action that was performed.	Displays only with the `-fmt DETAIL` or `-fmt PARSABLE` options.
ACTION	The action that was performed.	
REASON	The reason that the action was performed. A reason displays if a reason was specified in the command that created the change.	
DETAILS	An account of all of the changes, listing the old values and the new values.	

FAU_GEN.2 User identity association

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.

FAU_SAR.1 Audit review

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [*Administrator*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2

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

FAU_SAR.3 Selectable audit review

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1

The TSF shall provide the ability to apply [*filtering*] of audit data based on [*the criteria described in Table 13*].

Table 13 – Audit Record Filters

Option	Description
`-sdate <"MM/DD/YY [HH:[MM[:SS]]]">`	Used to indicate the start date and time of the report data to be viewed.
`-edate <"MM/DD/YY [HH:[MM[:SS]]]">`	Used to indicate the end date and time of the report data to be viewed.

Option	Description
`-ctgy`	Used to display records pertaining to a particular category for the CLI. The security-related categories are: • POLICY • JOB • STU (storage units) • STORAGESRV • POOL • AUDITCFG • AUDSVC • LOGIN • AZFAILURE (authorization failure) • USER
`-user <username[:domainname]>`	Used to indicate the name of the administrator indicated in the audit information. This is only available in enhanced auditing mode.
`Primary server > Security Management > Security Events > Select Audit Categories`	Shows the filters for the NetBackup Administration Consoles. These filters are: • Certificate (CERT) • Connection (CONNECTION) • Host (HOST) • Login (LOGIN) • Security Configuration (SEC_CONFIG) • Token (TOKEN)
`Security > Security events > Audit Events > Filters`	Shows the filters for the Web UI. These filters are: • Alert (ALERT) • Anomaly (ANOMALY) • Asset (ASSET) • Audit configuration (AUDITCFG) • Audit Database (AUDITDB) • Audit service (AUDITSVC) • Authorization failure (AZFAILURE) • bp.conf (BPCONF) • Catalog (CATALOG) • Certificate (CERT) • Config (CONFIG) • Connection (CONNECTION) • Credential (CREDENTIALS) • Credential schema (CREDENTIAL_SCHEMA) • Data access (DATAACCESS) • Discovery (DISCOVERY) • Event log (EVENT_LOG) • Hold (HOLD) • Host (HOST) • Intelligent group (ASSETGROUP) • Job (JOB) • Licensing (LICENSING) • Login (LOGIN) • Policy (POLICY) • Pool (POOL) • Protection plan (PROTECTION_PLAN_SVC) • Retention level (RETENTION_LEVEL) • Security configuration (SEC_CONFIG) • Storage lifecycle policy (SLP) • Storage server (STORAGESRV) • Storage unit (STU) • Token (TOKEN) • User (USER)

6.2.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1

The TSF shall enforce the [*Role Based Access Control Security Functional Policy (SFP)*] on [*the following:*

- *Subjects: TOE users*
- *Objects: Backup policies*
- *Operations: query, create, modify, delete*].

FDP_ACF.1 Security attribute based access control

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

FDP_ACF.1.1

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

- *Subject security attributes for TOE users – Role*
- *Object security attributes for backup policies– Policy name, backup name, data source (system)*].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*TOE users assigned a role with the appropriate privileges are able to query, create, modify, or delete backup policies*].

FDP_ACF.1.3

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

FDP_ACF.1.4

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

FDP_BCK_EXT.1 User data backup/restore

FDP_BCK_EXT.1.1

The TSF shall provide a capability to backup data and systems in accordance with the backup policy configured by authorized administrators.

FDP_BCK_EXT.1.2

The TSF shall provide a capability for authorized administrators to restore files to systems from previously created backups.

6.2.3 Class FIA: Identification and Authentication

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.

FIA_UAU.7 Protected authentication feedback

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1

The TSF shall provide only [*obscured feedback*] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

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.

6.2.4 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

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

FMT_MSA.1.1

The TSF shall enforce the [*Role Based Access Control SFP*] to restrict the ability to [query, modify, delete, create] the security attributes [*role, policy name, backup name, data source*] to [*Administrator, Default RHV Administrator, Default Security Administrator, Default Storage Administrator, Default VMware Administrator*].

FMT_MSA.3 Static attribute initialization

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

FMT_MSA.3.1

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

FMT_MSA.3.2

The TSF shall allow the [*Administrator, Default RHV Administrator, Default Security Administrator, Default Storage Administrator, Default VMware Administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

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

- *Review audit records*
- *Manage encryption policy*
- *Manage backup policy*
- *Restore data from backups*
- *Manage local accounts*].

FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [*Administrator, Default RHV Administrator, Default Security Administrator, Default Storage Administrator, Default VMware Administrator*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.5 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

Application Note: The TOE relies on the operational environment for reliable timestamps.

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 14 summarizes these requirements.

Table 14 – 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[4] 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

[4] 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 Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 15 lists the security functionality and their associated SFRs.

Table 15 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_BCK_EXT.1	User data backup/restore
Identification and Authentication	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_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TSF	FPT_STM.1	Reliable time stamps

7.1.1 Security Audit

The NetBackup Primary Server component of the TOE contains the NetBackup Audit Manager, where audit records are maintained in a database. Auditing is enabled by default and set to enhanced auditing in the evaluated configuration. With Enhanced Auditing enabled, the username of the account who performed the TOE operation is included in the audit record through all interfaces. The TOE records audit records for the events and actions listed in Table 11, the startup and shutdown of audit functions, and all auditable events at the not specified level of audit. The audit records recorded by the TOE include the fields described in Table 12.

Audit records stored in the TOE's database can be reviewed in a limited manner through the NetBackup Remote Administration Console, NetBackup Local Administration Console, and Web UI, with a more detailed view available through the CLI. When reviewing audit records through the CLI using the `nbauditreport` command or through the Web UI and Administration Consoles, TOE users may use the filtering options described in Table 13 to limit the data that is returned.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3.

7.1.2 User Data Protection

The Role Based Access Control SFP is used to govern access to the backup policies. The SFP determines which TOE users have access to query, create, change, or delete backup policies based on the role that is assigned to them. TOE users must be assigned the role of Administrator, Default RHV Administrator, Default Security Administrator, Default Storage Administrator, Default VMware Administrator to perform these actions. When managing the backup policies, a TOE user must specify the policy name, backup name, and data source for the TOE to create a backup of that system's data.

TOE users can create backup policies that set up periodic or calendar-based schedules to perform automatic, unattended backups for systems across the network. The policies can specify full or incremental backups. Full backups will back up all indicated system files, while incremental backups will back up only the files that have changed since the last backup. During a backup, the TOE's Client component on the target system will send backup data across the network to the TOE's NetBackup Media Server. The TOE's NetBackup Primary Server manages the type of storage that is specified in the backup policy. During a restore, TOE users can use the Web UI to browse to and then select the files and directories to recover. The TOE will then find the selected objects and restore them to the disk on the target machine.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_BCK_EXT.1.

7.1.3 Identification and Authentication

The TOE identifies and authenticates all TOE users before allowing access to the TSF-mediating functionality within the TOE. The authentication functionality of the host operating system is used to verify the credentials of a TOE user. The TOE also leverages the account creation service provided by the host operating system for creating and storing local accounts. All TOE users must enter their credentials into the TOE interfaces to allow the TOE to verify their identity and authenticate them with the host operating system. Passwords entered into the TOE interfaces are obscured using bullet characters in place of password characters.

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

7.1.4 Security Management

The TOE maintains the following roles and associates them to TOE users: Administrator, Default RHV Administrator, Default Security Administrator, Default Storage Administrator, Default VMware Administrator.

The Administrator role refers to the administrative account of the platform which the Primary Server is installed on. In the evaluated configuration, this is the Linux root account. The Administrator role is able to perform all administrative functions using the NetBackup Remote Administration Console, NetBackup Local Administration Console, CLI, and Web UI.

The Default Security Administrator is able to determine which accounts can access the TOE, the role or permissions that these accounts have, and the TOE assets which these accounts can access. The Default Security Administrator is also able to manage global security settings, manage NetBackup hosts and certificates, session management, manage locked NetBackup user accounts, manage API keys, and view security events. Accounts with this role are only able to perform administrative tasks through the Web UI.

The Default VMware Administrator is able to view storage units and replication-capable target storage servers. The Default VMware Administrator is also able to view, create, and delete access hosts; view and update NetBackup hosts; view, create, and delete data protection gateways; view, create, and update host properties; view NetBackup backup images; view jobs; view, create, update, and delete resource limits; view trusted Primary Servers; full permissions for protection plans; and all permissions, except "Edit transaction log schedules" for VMware assets.

The Default RHV Administrator is able to view, create, and delete access hosts; view and update NetBackup hosts; view NetBackup jobs; view, create, update, and delete resource limits; view trusted primary servers; view storage units; view replication-capable target storage servers; full permissions for RHV assets; and full permissions for protections plans.

The Default Storage Administrator is able to view data classifications, NetBackup hosts, Media Servers, Primary Server CA[5], and retention levels. Additionally, the Default Storage Administrator can view, create, update, and delete trusted Primary Servers. The Default Storage Administrator can also view policies; view, create, update, delete, and manage access to Storage Lifecycle Policies (SLP) and SLP Windows; view and create NetBackup security tokens; view details of cryptographic keys; view cloud storage; view, create, update, and delete disk pools; view, create, update and delete storage servers; view, create, and update disk volumes; view, create, delete, and update storage units; view tape media server groups and media volume pools; and view replication-capable target storage servers.

The TOE provides the following management functions:

- Review audit records – Only accounts with the Administrator or Default Security Administrator roles may review the audit records using the NetBackup Remote Administration Console, NetBackup Local Administration Console, CLI, or Web UI. Filtering of the audit records is available through the NetBackup Remote Administration Console, NetBackup Local Administration Console, Web UI and the CLI.
- Manage encryption policy – Only accounts with the Administrator role may manage the encryption policy using the NetBackup Remote Administration Console, NetBackup Local Administration Console, or CLI.
- Manage backup policy – All accounts with the Administrator or Default Storage Administrator roles may manage the backup policies using the NetBackup Remote Administration Console, NetBackup Local Administration Console, CLI, or Web UI. TOE users are allowed to query, modify, create, and delete backup policies. There are no defaults for the policy name, backup name, or data source and must be specified when creating a new backup policy.
- Restore data from backups – All accounts with one of the TOE's roles may restore data from a backup using the Web UI.
- Manage local accounts – Accounts with the Administrator or Default Security Administrator roles may manage the local accounts using the NetBackup Remote Administration Console, NetBackup Local Administration Console, CLI, or Web UI. TOE users are allowed to query, modify, and delete the role associated to accounts. There is no default role for new accounts and must be assigned as needed.

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

7.1.5 Protection of the TSF

The TOE is able to provide a reliable timestamp to audit records by leveraging the time service in the host operating system, RHEL 7.9.

[5] CA – Certificate Authority

TOE Security Functional Requirements Satisfied: FPT_STM.1.

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 5.

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 16 below provides a mapping of the objectives to the threats they counter.

Table 16 – Threats: Objectives Mapping

Threat	Objectives	Rationale
T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential unauthorized data accesses to go undetected.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDENTAUTH objective by only permitting authorized users to access TOE functions.
	O.ADMIN The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE and restrict these functions from unauthorized use.	The O.ADMIN objective ensures the TOE has all the necessary administrative functions to manage the product.
	OE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.	The OE.INSTALL objective states the authorized administrators will configure the TOE properly.
	O.AUDIT The TOE must generate audit records for security related events.	The O.AUDIT objective supports O.ACCESS by requiring the TOE to record audit data for security related events such as unauthorized access.
	O.IDENTAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDENTAUTH objective requires authentication of users prior to allowing access to TOE functions.
T.PRIVILEGE An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDENTAUTH objective by permitting only authorized users to access TOE functions.
	O.IDENTAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDENTAUTH objective requires authentication of users prior to allowing access to TOE functions.

Threat	Objectives	Rationale
	O.PROTECT The TOE must ensure the integrity of all TSF data, including audit records, by protecting itself from unauthorized access.	The O.PROTECT objective addresses the threat by providing self-protection for the TOE.
T.UNAUTH An unauthorized user may attempt to access backup data which could result in the loss of sensitive information.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective permits only authorized access to TOE data.
	O.AUDIT The TOE must generate audit records for security related events.	The O.AUDIT objective supports O.ACCESS by requiring the TOE to record audit data for security related events such as unauthorized access attempts.
	O.CRYPTO Backup data must be protected using approved cryptographic functions.	The O.CRYPTO objective ensures that user data is protected from disclosure in the case of attempted data access.

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

Table 17 below gives a mapping of policies and the objectives that support them.

Table 17 – Policies: Objectives Mapping

Policy	Objectives	Rationale
P.ACCOUNT The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.AUDIT The TOE must generate audit records for security related events.	The O.AUDIT objective requires auditing of all data access and use of TOE functions.
	O.IDENTAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDENTAUTH objective supports this policy by ensuring each user is uniquely identified and authenticated.
	O.TIME The TOE must provide reliable timestamps.	The O.TIME objective supports this policy by providing a time stamp for insertion into the resulting audit records.
P.BACKUP The TOE shall backup specified client data and make it available for restore operations.	O.BACKUP The TOE shall backup specified client data and make it available for restore operations.	The O.BACKUP objective requires the TOE to backup specified client data, and requires the TOE to make that data available for restore operations.
P.MANAGE The TOE shall be managed only by authorized users.	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDENTAUTH objective by permitting only authorized users to access TOE functions.
	O.ADMIN The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE and restrict these functions from unauthorized use.	The O.ADMIN objective ensures that there is a set of functions for administrators to use, and use is restricted to authorized users.
	OE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.	The OE.INSTALL objective ensures that administrators follow all provided documentation and maintain the security policy for installation and management of the TOE.

Policy	Objectives	Rationale
	OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.	The OE.PERSON objective ensures competent administrators will manage the TOE.
	O.IDENTAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	The O.IDENTAUTH objective requires authentication of users prior to allowing access to TOE functions.
	O.PROTECT The TOE must ensure the integrity of all TSF data, including audit records, by protecting itself from unauthorized access.	The O.PROTECT objective addresses this policy by requiring TOE self-protection.

Every policy is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 18 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 18 – Assumptions: Objectives Mapping

Assumption	Objectives	Rationale
A.CRYPTO It is assumed that the TOE's operational environment is providing cryptographic support.	OE.CRYPTO The operational environment will provide cryptographic support to the TOE with a FIPS-validated cryptographic module (Certificate #2340).	The OE.CRYPTO objective ensures that the TOE can rely on the operational environment for cryptographic support.
A.MANAGE It is assumed that there are one or more competent individuals assigned to manage the TOE. These users are not careless, willfully negligent, or hostile. They are appropriately trained and will follow the instructions provided by the TOE documentation.	OE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.	The OE.INSTALL objective ensures that the TOE is properly installed and operated.
	OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
	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.	The OE.PHYSICAL objective provides for physical protection of the TOE.
A.NETWORK It is assumed that the TOE components and their hosts are installed on an internal network which protects the data from disclosure and modification by untrusted systems or users.	OE.NETWORK The operational environment will provide a segregated, internal network that protects the traffic that passes between the TOE components from disclosure and modification by untrusted systems or users.	The OE.NETWORK objective ensures that the management traffic will be protected on an internal network.
A.PROTECT It is assumed that the hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical access.	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.	The OE.PHYSICAL objective provides for the physical protection of the TOE hardware and software components, and the hardware and software components that support the TOE implementation.

Assumption	Objectives	Rationale
A.TIMESTAMPS It is assumed that the TOE's operational environment is providing a reliable timestamp.	OE.TIMESTAMPS The operational environment receives the reliable timestamp from an NTP server through an encrypted channel.	The OE.TIMESTAMPS objective ensures that the TOE can rely on the operational environment for reliable timestamps.

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

The family FDP_BCK_EXT User data backup/restore was created to outline the functionality of performing backup and restore operations within the TOE. The User data backup/restore family was modeled after FDP_ACC: Access Control Policy from CC Part 2. The purpose of this family is to outline the requirements for performing backups and restores of user data. These requirements have no dependencies since the stated requirements embody all the necessary security functions. These requirements exhibit functionality that can be easily documented in the ADV assurance evidence and thus do 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 19 below shows a mapping of the objectives and the SFRs that support them.

Table 19 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	FIA_UAU.2 User authentication before any action	FIA_UAU.2 requires users to be authenticated prior to gaining access to TOE functions. This ensures that only authorized users gain access to TOE functions and data.
	FIA_UAU.7 Protected authentication feedback	FIA_UAU.7 protects the password from being observed, preventing unauthorized users from gaining access to the TOE.
	FIA_UID.2 User identification before any action	FIA_UID.2 requires users to be identified prior to gaining access to TOE functions. This ensures that only authorized users gain access to TOE functions and data.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 defines which user roles have permissions to read and modify user roles for other users.

Objective	Requirements Addressing the Objective	Rationale
	FMT_SMR.1 Security roles	FMT_SMR.1 ensures the TOE supports multiple roles so that appropriate data access can be provided to users with varied responsibilities.
O.ADMIN The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE and restrict these functions from unauthorized use.	FMT_MSA.1 Management of security attributes	FMT_MSA.1 defines the access permissions each role has to the security attributes of the SFP.
	FMT_MSA.3 Static attribute initialisation	FMT_MSA.3 defines the access permissions each role has to the initial values for security attributes.
	FMT_SMF.1 Specification of management functions	FMT_SMF.1 specifies the management functionality required for effective management of the TOE.
	FMT_SMR.1 Security roles	FMT_SMR.1 defines the roles required to provide effective management capabilities for users with different responsibilities.
O.AUDIT The TOE must generate audit records for security related events.	FAU_GEN.1 Audit Data Generation	FAU_GEN.1 requires audit records to be generated for security related events within the TOE.
	FAU_GEN.2 User Identity Association	FAU_GEN.2 requires audit records to contain the username of the account initiating the action.
	FAU_SAR.1 Audit review	FAU_SAR.1 requires that audit records be available to authorized users for review.
	FAU_SAR.3 Selectable audit review	FAU_SAR.3 requires that the TOE provide functionality to filter the audit records for convenient viewing.
	FPT_STM.1 Reliable time stamps	FPT_STM.1 requires accurate time stamps to be available for the audit records.
O.BACKUP The TOE shall backup specified client data and make it available for restore operations.	FDP_ACC.1 Subset access control	FDP_ACC.1 ensures that backup data is created as directed and is available to be restored as required.
	FDP_ACF.1 Security attribute based access control	FDP_ACF.1 ensure that backup data is created as directed and is available to be restored as required.
	FDP_BCK_EXT.1 User data backup/restore	FDP_BCK_EXT.1 ensures that the TOE supports backup and restore operations.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 ensures that appropriate security attributes are maintained for subjects and objects.
	FMT_MSA.3 Static attribute initialisation	FMT_MSA.3 ensures that default attributes are restrictive in nature.
O.IDENTAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	FIA_UAU.2 User authentication before any action	FIA_UAU.2 ensures that users are authenticated, thus ensuring that only authorized users have access to the TOE.
	FIA_UAU.7 Protected authentication feedback	FIA_UAU.7 protects the password from being observed, preventing unauthorized users from gaining access to the TOE.
	FIA_UID.2 User identification before any action	FIA_UID.2 ensures that users are identified, thus ensuring that only authorized users have access to the TOE.

Objective	Requirements Addressing the Objective	Rationale
O.PROTECT The TOE must ensure the integrity of all TSF data, including audit records, by protecting itself from unauthorized access.	FDP_ACC.1 Subset access control	FDP_ACC.1 defines the subject, objects, and operations applicable to the access control policy.
	FDP_ACF.1 Security attribute based access control	FDP_ACF.1 defines the security attributes and rules to the access control policy that determines access to TSF data.
	FIA_UAU.2 User authentication before any action	FIA_UAU.2 ensures that users must be authenticated prior to access to TSF data, thereby preventing unauthorized access.
	FIA_UID.2 User identification before any action	FIA_UID.2 ensure that users must be identified prior to access to TSF data, thereby preventing unauthorized access.
	FMT_MSA.1 Management of security attributes	FMT_MSA.1 provides the functionality that determines the attributes used by the access control policy.
	FMT_MSA.3 Static attribute initialisation	FMT_MSA.3 provide the functionality that determines the attributes used by the access control policy.
	FMT_SMR.1 Security roles	FMT_SMR.1 provides the roles that are used to restrict access to TSF data.
O.TIME The TOE must provide reliable timestamps.	FPT_STM.1 Reliable time stamps	FPT_STM.1 requires the provision of accurate time stamps.

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. 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

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 20 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 20 – Functional Requirements Dependencies

SFR	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.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.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FDP_ACC.1	FDP_ACF.1	✓	

SFR	Dependencies	Dependency Met	Rationale
FDP_ACF.1	FMT_MSA.3	✓	
	FDP_ACC.1	✓	
FDP_BCK_EXT.1	No dependencies		
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_UAU.7	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_UID.2	No dependencies		
FMT_MSA.1	FMT_SMR.1	✓	
	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_SMR.1	✓	
	FMT_MSA.1	✓	
FMT_SMF.1	No dependencies		
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_STM.1	No dependencies		

9. Acronyms

Table 21 defines the acronyms used throughout this document.

Table 21 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CTR	Counter Mode
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
IT	Information Technology
NIST	National Institute of Standards and Technology
OSP	Organizational Security Policy
PDF	Portable Document Format
PP	Protection Profile
RHEL	Red Hat Enterprise Linux
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SP	Special Publication
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface
UTC	Coordinated Universal Time

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Circle
Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com