Rubrik, Inc.

Security Cloud - Private and Cloud Data Management

v2.4.12-p3-81 and v9.2.3-p3-29515

Security Target

Evaluation Assurance Level (EAL): 2+
Document Version: 1.4

Prepared for:

Rubrik, Inc.
3495 Deer Creek Road
Palo Alto, CA 94304
United States of America

Phone: +1 844 478 2745
www.rubrik.com

Prepared by:

Corsec Security, Inc.
12600 Fair Lakes Drive, Suite 210
Fairfax, VA 22003
United States of America

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

Table of Contents

List of Tables

List of Figures

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is Rubrik, Inc. (Rubrik) Security Cloud - Private and Cloud Data Management and will hereafter be referred to as the TOE throughout this document.

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 and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

The following table shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	*Rubrik, Inc. Security Cloud - Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515 Security Target*
ST Version	Version 1.4
ST Author	Corsec Security, Inc.
ST Publication Date	August 27, 2026
TOE Reference	Rubrik SC-P and CDM[1][2] v2.4.12-p3-81 and v9.2.3-p3-29515

[1] SC-P – Security Cloud-Private
[2] CDM – Cloud Data Management

Product Software	Security Cloud – Private v2.4.12-p3-81 Cloud Data Management v9.2.3-p3-29515
Guidance Supplement	Rubrik; Security Cloud-Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515; Guidance Documentation Supplement; Evaluation Assurance Level (EAL): 2+; Document Version: v1.2

1.3 TOE Overview

Rubrik Security Cloud - Private and Cloud Data Management is a distributed TOE consisting of Cloud Data Management (CDM), a Data Protection product that distributes data, metadata, and task management across a cluster, and SC-P, which permits administration and management of multiple Rubrik clusters through a single web UI. A Rubrik CDM cluster is a collection of objects that include sources from where data is getting backed up, targets where backups are stored, and security principals, or the users and service accounts, that manages the cluster.

Rubrik Security Cloud - Private (SC-P) provides a global management view of the daily operations of the connected CDM clusters. SC-P apps monitor the protection and compliance status of CDM clusters, generating reports and charts using current and historical data about the health, protection, and compliance status of all of the objects that the CDM clusters protect.

SC-P runs on an on-premises Virtual Machine (VM), and consists of the components described in Table 2.

Table 2 – SC-P Components

Component	Description
Dashboard	Top-down view of all CDM clusters using aggregated summary information. Provides a large screen-type view of overall events, compliance, capacity, and alerts.
Clusters	Status-at-a-glance summary view of each of the CDM clusters and the ability to take a closer look at a selected cluster.
Inventory	Summary view of the inventory list of data sources on all CDM clusters.
SLA Domains	Continually updating view of all SLA Domains created on all CDM clusters that are managed by SC-P. The SLA Domain tab is available when this feature is enabled for the SC-P account.
Events	Continually updating view of all events on all CDM clusters, with filters to focus on a specific CDM cluster, event, protection object, or user.
Reports	Customizable reports and charts. Use reports for audit work and planning and to get a snapshot view of specific events on CDM clusters.

CDM consists of the components described in Table 3.

Table 3 – CDM Components

Component	Description
Core	• Cloud-Scale File System • Distributed Metadata Service • Cluster Management • Distributed Task Framework
Data Management	• Organizing, removing redundancy, and making data available for search • Administrative interface

1.3.1 Core

Rubrik Cloud-Scale File System

Rubrik Cloud-Scale File System is a distributed file system that stores and manages versioned data.

- Fault Tolerant: it is resilient to multiple node and disk failures, employing an intelligent replication scheme to distribute multiple copies of data throughout the cluster
- Storage Efficient: it utilizes zero-space clones to make multiple copies of data from one "golden image"
- Scale-out NAS server: it appears as a scale-out NAS[3] server to any host when a snapshot is mounted

Rubrik Distributed Metadata Service
Rubrik Distributed Metadata Service provides a high-speed index, continuous availability, linear scalability, and operational simplicity with no single point of failure in the cluster. It handles large amounts of data, distributes replicas of data across nodes, and provides low latency operations.

Rubrik Cluster Management
Rubrik Cluster Management manages the Rubrik system setup and ongoing system health. Its zero-configuration multicast DNS protocol automates appliance discovery – the cluster expands with minimal manual intervention with new nodes auto discovering each other. Post system setup, it maintains the status of each node by performing health checks on individual nodes.

Rubrik Distributed Task Framework
Rubrik Distributed Task Framework is the engine that globally assigns and executes tasks across the cluster. Tasks are load balanced across the entire cluster, and are distributed to the nodes that house the impacted data. This engine runs on all nodes and incorporates a masterless architecture where all nodes cooperatively schedule and run tasks.

1.3.2 Data Management

Rubrik Data Management

- Stores versions of data using full snapshots with forward incremental and reverse incremental copies.
- Ensures data integrity with multiple checks within the file system and data management layers.
- Applies content-aware global deduplication and compression.

Admin GUI

- Web interface for administrators.

1.4 TOE Major Security Features

The internal components of CDM include Cluster Management, Cloud-Scale File System, Distributed Metadata Service, Distributed Task Framework, Data Management, and Admin GUI. These components talk to other instances of the same component on other nodes using a Thrift RPC protocol. This protocol is implemented on top of an encrypted, TLS[4] based transport layer. To prevent man-in-the-middle attacks, all internode TLS connections are verified using a private key and a public key certificate shared by all nodes in the cluster (data in flight encryption), using both client and server certificate. The key (2048-bit RSA) and the certificate (self-signed including the clusters' UUID in the name) are generated when the customer first installs the Rubrik CDM cluster ("bootstrapping"), and are known only by nodes within that cluster. In addition, the private key and the certificate are distributed to all nodes during bootstrap via a Thrift RPC[5]. Prior to and during bootstrap, this Thrift RPC uses a

[3] NAS – Network Attached Storage
[4] TLS – Transport Layer Security
[5] RPC – Remote Procedure Call

fixed TLS certificate and private key shipped with all nodes. After bootstrap, the new per-cluster certificate and private key are used.

SC-P's and CDM major security features consist of:

- Web Admin Console
  - The Web Admin Console is a web-based graphical interface used to configure and manage SC-P's and CDM security functionality.
  - The Web Admin Console can also be configured to display a custom advisory warning when accessing the login page.
- Local Authentication and Identification
  - SC-P and CDM requires that users must be successfully authenticated and identified before the user is allowed to perform any other TSF-mediated actions.
- Cryptographic Support
  - A cryptographic module is used by SC-P and CDM for secure communication via TLS and SSH.

1.5 TOE Environment

SC-P runs in a VMware VM provisioned by an ESXi hypervisor. The ESXi cluster must meet the minimum requirements in the following table:

Table 4 – TOE Minimum ESXi Cluster Requirements

Category	Requirement
Datastore	• Fault-tolerance • 10,000 input/output operations per second (IOPS) • 1 TB of available storage
Computer hardware	• 8 CPUs • 96 GB of RAM

The VM that hosts the SC-P instance must have an IPv4 address that is reachable on port 443 by Rubrik clusters that connect to the instance.

SC-P requires an NTP Server connected to the SC-P instance to ensure the time is synchronized with the network.

SC-P also requires CDM clusters to forward audit data to it.

CDM runs in a VMware VM provisioned by an ESXi hypervisor, with the following:

- vCPU[6] - Four virtual CPUs with Reservation set to 8,000 MHz[7] and Limit set to Unlimited
- Reserved Memory - 24 GB[8] RAM[9]
- Operating System Drive – 128 GB SSD, thick provision zeroed
- Data Drive – Up to 5 TB HDD or SSD, thick provision lazy zeroed
- Minimum number of Input/Output Operations Per Second (IOPS) required on OS disk – 750 IOPS
- Minimum number of IOPS required on data disk – 50 IOPS, 100 MiB per second

[6] vCPU – Virtual Central Processing Unit
[7] MHz - Megahertz
[8] GB - Gigabyte
[9] RAM – Random Access Memory

The VM that hosts CDM must have an IPv4 address that is reachable on port 443 by Rubrik clusters that connect to the instance.

1.6 TOE Description

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

- Security Cloud – Private v2.4.12-p3-81
- Cloud Data Management v9.2.3-p3-29515

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

Rubrik SC-P pulls data from the connected CDM instance and permits administration and management of the data through a single web UI. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

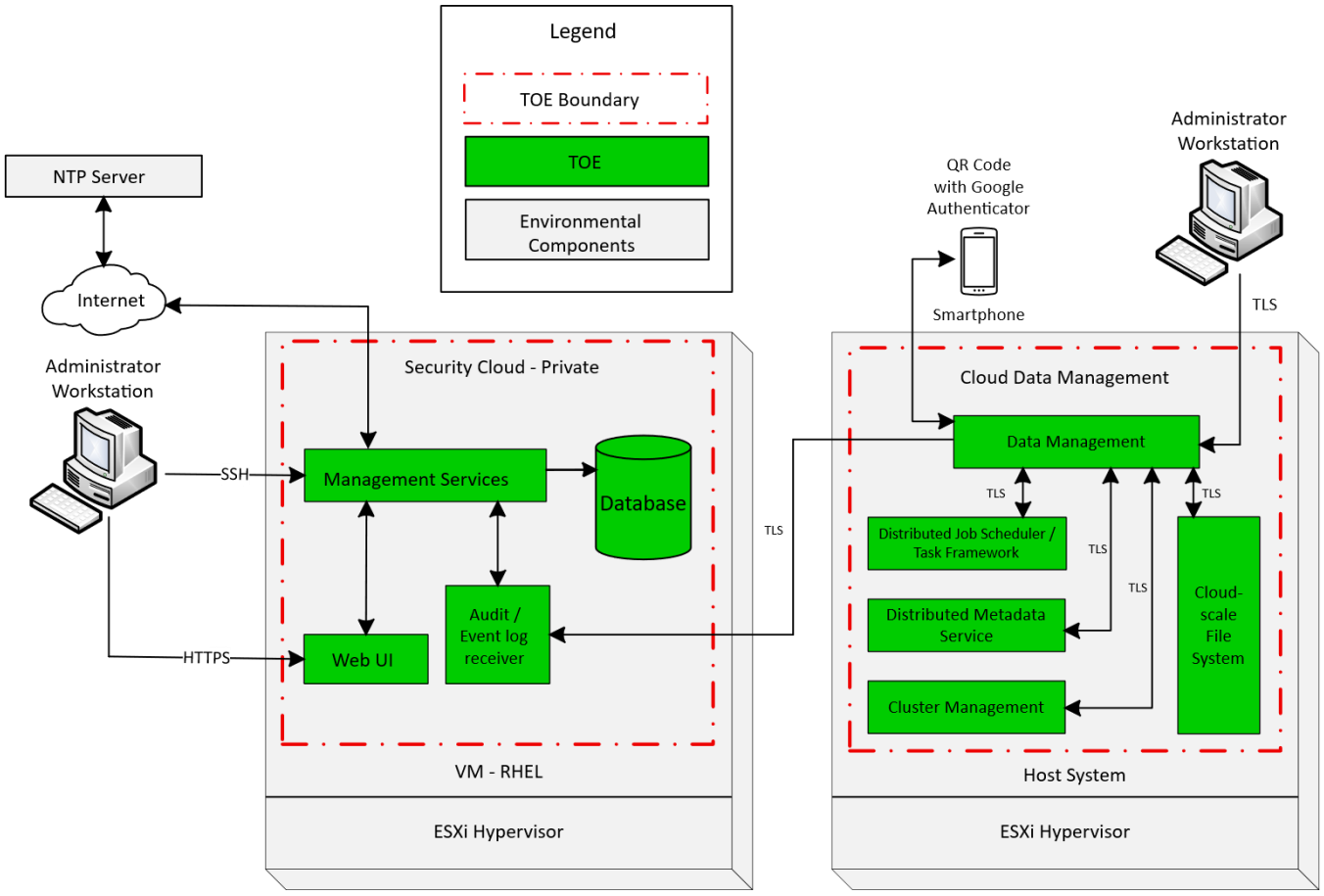

Figure 1 – Physical TOE Boundary

NOTE: The TOE should be used with Google Authenticator.

1.6.1 Physical Scope

1.6.1.1 TOE Software

The TOE is a software-only TOE and is comprised of:

- An SC-P OVA image installed in a VM for SC-P.
- A Rubrik Edge OVA[10] image installed in a VM for CDM.

The TOE is deployed on vSphere virtual machines with these OVA images.

The software is downloaded from the Rubrik Support website using a valid customer account.

1.6.1.2 Required Non-TOE Components

The TOE requires the following non-TOE components:

- Two VMware ESXi hypervisors, which are the host servers for SC-P and Rubrik Edge running in a VM (a VM running Rubrik Edge is necessary for setting up CDM). Rubrik Virtual Cluster is a set of CDM instances; within the TOE test environment there is only one CDM instance.
- Administrator Workstation, used for external communication with the SC-P Management Services via SSH, with the SC-P Web UI via HTTPS, and with the CDM Data Management via TLS.
- Smartphone, connected to CDM Data Management via a QR code using Google Authenticator, implementing time-based password for secure authentication.
- NTP Server, which provides time synchronization for the TOE.

1.6.1.3 Guidance Documentation

The following PDF guides, available for download through the Rubrik website, are required reading and part of the TOE:

- *Rubrik CDM Version 9.2 CLI Guide (Rev. A3)*
- *Rubrik CDM Version 9.2 Install Guide (Rev. A0)*
- *Rubrik CDM Version 9.2 User Guide (Rev. A4)*
- *Rubrik Security Cloud - Private 2.4.12 CLI Reference (Rev A0)*
- *Rubrik Security Cloud - Private 2.4.12 Install and Upgrade Guide (Rev A0)*
- *Rubrik Security Cloud - Private 2.4.12 User Guide (Rev A0)*
- *Rubrik; Security Cloud-Private and Cloud Data Management v2.4.12-p3-81 and v9.2.3-p3-29515; Guidance Documentation Supplement; Evaluation Assurance Level (EAL): 2+; Document Version: v1.2*

1.6.2 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
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- User Data Protection

[10] OVA – Open Virtual Appliance

- TOE Access
- Trusted path/channels

1.6.2.1 Security Audit

The TOE provides extensive auditing capabilities. For each event, the CDM and SC-P records the date and time of each event, the type of event, and the outcome of the event. SC-P and CDM components together provide audit records as claimed in FAU_GEN.1 and FAU_GEN.2. SC-P receives audit log and event log entries from the connected CDM clusters.

1.6.2.2 Cryptographic Support

The TOE provides cryptography in support of remote administrative management via TLS/HTTPS[11] with SC-P and CDM, as well as support for securing all communication with SC-P over SSH.

1.6.2.3 Identification and Authentication

CDM provides authentication services for local and AD[12] administrative users wishing to connect to CDM's Secure Web UI administrator interface.

The TOE requires authorized administrators to authenticate prior to being granted access to any of the management functionality for SC-P and CDM.

After users successfully authenticate into CDM, CDM determines the permitted level of access for a user based on the local authorization setting for that user and provides role-based access.

1.6.2.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs through a secure TLS/HTTPS session, or via a local console connection. SC-P supports an Administrator role. SC-P permits only authenticated administrators to access its functionality and perform tasks.

There are two primary use cases that shape the default CDM RBAC[13] roles: Administrator, and End User.

1.6.2.5 Protection of the TSF

The TOE provides timestamps for local audit log entries, in addition to the date/time information provided by audit log and event log entries forwarded to SC-P by connected CDM clusters.

1.6.2.6 User Data Protection

CDM limits the execution of commands and the ability to change usernames and passwords to authorized administrators only.

1.6.2.7 TOE Access

Users logging into the TOE are presented with one or more login banners, and are able to log themselves out when finished with their tasks.

1.6.2.8 Trusted Path/channels

The TOE provides trusted communication channels between itself and another trusted IT products.
The TOE provides a communication path between itself and local users, and it allows both local users and the TOE itself to initiate the trusted path.

[11] HTTPS – Hypertext Transport Protocol - Secure
[12] AD – Active Directory
[13] RBAC – Role Based Access Control

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

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

- Command Line Interface
- LDAP Server
- Custom Roles

2. Conformance Claims

This section and Table 5 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 5 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version CC:2022, Revision 1, November 2022; CC Part 2 conformant; 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; Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) v1.1 as of July 22, 2024 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	2+ augmented (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 assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings 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.

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[14] and data saved on the TOE from the Rubrik clusters on the protected network.

Table 6 – Assets

Name	Description
A.DATA	Sensitive or security functional data contained in TOE backups, both locally and archived across all mediums supported by the TOE.
A.KEY	Cryptographic keys contained in the TOE, for encryption of 'data in flight'.

Table 7 – Threat Agents

Name	Description
T.ADMIN	Authorized person/process that performs installation and configuration/setup of the TOE to ensure that the TOE operates according to the needs of the enterprise/organization.
T.ATTACKER	A person/company or process with skills and resources to mislead the system in any way necessary to reveal/divulge/misuse data and prevent the system from intended operations.

Table 8 – Threats to the TOE

Name	Threat Agent	Asset	Description
TT.ADMIN_ERROR	T.ADMIN	A.DATA	During operation, the administrator unintentionally configures the TOE incorrectly, making the TOE inoperable or resulting in ineffective security mechanisms.
TT.ADMIN_EXPLOIT	T.ATTACKER	A.DATA	A person/company uses hacking methods to exploit missing, weak or incorrectly implemented access control in the TOE.

[14] TSF – TOE Security Functionality

Name	Threat Agent	Asset	Description
TT.CRYPTO_COMPROMISE	T.ATTACKER	A.DATA and A.KEY	An attacker cause key or data associated with the cryptographic functionality to be inappropriately accessed (viewed/modified/deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
TT.HACK_ACCESS	T.ATTACKER	A.DATA	A person/company uses hacking methods to exploit missing, weak or incorrectly implemented access control in the TOE.
TT.MALFUNCTION	T.ATTACKER	A.DATA and A.KEY	A malfunction in the TOE implies unauthorized access to TOE resources.

Table 9 – Threats to the TOE Environment

Name	Threat Agent	Asset	Description
TE.EAVESDROPPING	T.ATTACKER	A.DATA	An unauthorized person with no physical access to TOE is eavesdropping on the communication between Rubrik nodes to intercept information.

3.2 Organizational Security Policies

Table 10 – OSPs

Name	Description
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHIC	The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.

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 11 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 11 – Assumptions

Name	Description
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	The administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.LOCATE	The TOE is located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.

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 12 below.

Table 12 – Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.
O.AUDIT	The TOE shall record and maintain security-related events to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.
O.CRYPTOGRAPHY	The TOE shall provide cryptographic functions to maintain the confidentiality of 'data in flight'.
O.MANAGE	The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.
O.PROTECTION	The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 13 below lists the IT security objectives that are to be satisfied by the environment.

Table 13 – IT Security Objectives

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.

4.2.2 Non-IT Security Objectives

The table below lists the non-IT environment security objectives that 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 14 – Non-IT Security Objectives

Name	Description
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines as indicated by Rubrik and any additional trusted parties in which an agreement has been entered.

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

There are no extended SFRs defined for this ST.

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

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 [underlined text within brackets].
- Completed assignment statements within a selection statement are identified using [*underlined and italicized text within brackets*].
- 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.

Note: SFRs which pertain to either CDM or SC-P, have been indicated by (CDM) or (SC-P) notation with the associated SFRs. SFR which pertain to both CDM and SC-P have been indicated with CDM & SC-P.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 15 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 15 – TOE Security Functional Requirements

Functional Class	Name	Description	S	A	I
FAU: Security audit	FAU_GEN.1	Audit data generation (CDM & SC-P)	✓	✓	
	FAU_GEN.2	User identity association (CDM & SC-P)			
	FAU_SAR.1	Audit review (CDM & SC-P)		✓	
	FAU_SAR.3	Selectable audit review (CDM & SC-P)		✓	
	FAU_SEL.1	Selective audit (SC-P)	✓	✓	
FCS: Cryptographic support	FCS_CKM.1	Cryptographic key generation (CDM & SC-P)		✓	
	FCS_CKM.3	Cryptographic Key Access (CDM & SC-P)		✓	
	FCS_CKM.6	Timing and event of cryptographic key destruction (CDM & SC-P)	✓	✓	
	FCS_COP.1(a)	Cryptographic operation (CDM)		✓	✓

Functional Class	Name	Description	S	A	I
	FCS_COP.1(b)	Cryptographic operation (SC-P)		✓	✓
	FCS_RNG.1	Random number generation (CDM & SC-P)	✓	✓	
FDP: User data protection	FDP_ACC.1	Subset Access Control (CDM)		✓	
	FDP_ACF.1	Security attribute-based access control (CDM)		✓	
FIA: Identification and authentication	FIA_ATD.1	User attribute definition (CDM)		✓	
	FIA_UAU.2	User authentication before any action (CDM & SC-P)			
	FIA_UAU.5	Multiple authentication mechanisms (CDM & SC-P)		✓	
	FIA_UID.2	User identification before any action (CDM & SC-P)			
FMT: Security management	FMT_MTD.1	Management of TSF[15] data (CDM)	✓	✓	
	FMT_SMF.1(a)	Specification of Management Functions (CDM)		✓	✓
	FMT_SMF.1(b)	Specification of Management Functions (SC-P)		✓	✓
	FMT_SMR.2	Restrictions on security roles (CDM)		✓	
	FMT_MSA.1	Management of security attributes (CDM)	✓	✓	
	FMT_MSA.3	Static attribute initialization (CDM)	✓	✓	
FPT: Protection of the TSF	FPT_STM.1	Reliable time stamps (CDM)			
FTA: TOE Access	FTA_SSL.4	User-initiated termination (SC-P)			
	FTA_TAB.1	Default TOE access banners (SC-P)			
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel (CDM & SC-P)	✓	✓	
	FTP_TRP.1	Trusted path (CDM & SC-P)	✓	✓	

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation (CDM & SC-P)

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1

The TSF shall be able to generate audit data 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) [**All administrative actions and the following security events:**

- **Resuming all protection activity,**
- **Pausing all protection activity**].

FAU_GEN.1.2

The TSF shall record within the audit data at least the following information:

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

b) For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [**None**].

[15] TSF – TOE Security Function

FAU_GEN.2 User identity association (CDM & SC-P)

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 (CDM & SC-P)

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [*authorized users*] with the capability to read [*all audit and event information*] from the audit data.

FAU_SAR.1.2

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

FAU_SAR.3 Selectable audit review (CDM & SC-P)

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1

The TSF shall provide the ability to apply [*filtering*] of audit data based on [*selections made in the web GUI*].

FAU_SEL.1 Selective audit (SC-P)

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

FAU_SEL.1.1

The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a. [event type]
b. [*time range, cluster, local, severity, status*].

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation (CDM & SC-P)

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_CKM.5 Cryptographic key derivation, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.3 Cryptographic key access
[FCS_RBG.1 Random bit generation, or
FCS_RNG.1 Generation of random numbers]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*AES Counter_DRBG*] and specified cryptographic key sizes [*128 bits*] that meet the following: [*NIST*[16] *SP*[17] *800-90A*].

FCS_CKM.3 Cryptographic Key Access (CDM & SC-P)

[16] National Institute of Standards and Technology
[17] SP – Special Publication

Dependencies:
[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes,
or FCS_CKM.1 Cryptographic key generation or
FCS_CKM.5 Cryptographic key derivation]

FCS_CKM.3.1

The TSF shall perform [*reading stored keys, writing keys to storage*] in accordance with a specified cryptographic key access method [*secure Trusted Platform Module (TPM)*] that meets the following: [*AES-256 as specified in NIST SP FIPS-197*].

FCS_CKM.6 Timing and event of cryptographic key destruction (CDM & SC-P)

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

FCS_CKM.6.1

The TSF shall destroy [*all cryptographic keys (including keying material)*] when [no longer needed].

FCS_CKM.6.2

The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [
1. For volatile memory, the destruction shall be executed by a [
a. single overwrite consisting of [
ii. zeroes,
iii. ones.]
2. For non-volatile memory
[a. that employs a wear-leveling algorithm, the destruction shall be executed by a
[i. single overwrite consisting of [
zeroes, ones]; that meets the following: [NIST SP 800-57].

FCS_COP.1(a) Cryptographic operation (CDM)

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.3 Cryptographic key access

FCS_COP.1.1

The TSF shall perform [*cryptographic operations in Table 16*] in accordance with a specified cryptographic algorithm [*see Table 16*] and cryptographic key sizes [*see Table 16*] that meet the following: [*see Table 16*].

Table 16 – Cryptographic Operations

Operation	Algorithm	Key size(s)	Standard
Encryption / decryption	AES[18]	128, 256	FIPS[19] PUB[20] 197
Encryption / decryption	RSA[21]	2048	

[18] AES – Advanced Encryption Standard
[19] FIPS - Federal Information Processing Standard
[20] PUB - Publication
[21] RSA – Rivest Shamir Adelman

Operation	Algorithm	Key size(s)	Standard
Hashing	SHA[22]-1, SHA-256, SHA-384, SHA-512		FIPS PUB 180-4
HMAC[23]	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512		FIPS PUB 198-1
Key agreement	EC[24] Diffie-Hellman	256, 384, 512	

FCS_COP.1(b) Cryptographic operation (SC-P)

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.3 Cryptographic key access

FCS_COP.1.1

The TSF shall perform [*encryption, decryption*] in accordance with a specified cryptographic algorithm [*AES-CTR*] and cryptographic key sizes [*256 bits*] that meet the following: [*FIPS[25] 197*].

FCS_RNG.1 Random number generation (CDM & SC-P)

Dependencies: No dependencies

FCS_RNG.1.1

The TSF shall provide a [deterministic] random number generator that implements [*cryptographically secure random outputs*].

FCS_RNG.1.2

The TSF shall provide [256-bits] that meet [*generation of a 96-bit nonce*].

6.2.3 Class FDP: User Data Protection

FDP_ACC.1 Subset access control (CDM)

Dependencies: FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1

The TSF shall enforce the [*Rubrik Access Control*[26]] on [*subjects: authorized administrator, objects: commands, operations: execute*].

FDP_ACF.1 Security attribute-based access control (CDM)

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

FDP_ACF.1.1

The TSF shall enforce the [*Rubrik Access Control*] to objects based on the following: [*subjects: authorized administrator; subject attributes: user name, password; object: commands; object attributes: none*].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*If a subject with the Authorized Administrator role requests access to an object, then access is granted. If the above rule does not apply, access is denied*].

FDP_ACF.1.3

[22] SHA – Simple Hashing Algorithm
[23] HMAC – Keyed Message Authentication Code
[24] EC – Elliptic Curve
[25] FIPS – Federal Information Processing Standard
[26] Set of attribute-based access control rules enforced by the TSF to regulate operation on objects based on subject roles and attributes.

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 following additional rules: [*no additional rules*].

6.2.4 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition (CDM)

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [

a) *User identity:* ***user name****;*

b) *Local authentication data:* ***password****;*

c) *Authorizations:* ***access rights***; and

d) ***Email address***].

FIA_UAU.2 User authentication before any action (CDM & SC-P)

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.5 Multiple authentication mechanisms (CDM & SC-P)

FIA_UAU.5.1

The TSF shall provide [password authentication, time-based password] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [password authentication followed by time-based password].

FIA_UID.2 User identification before any action (CDM & SC-P)

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.

6.2.5 Class FMT: Security Management

FMT_MTD.1 Management of TSF data (CDM)

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1

The TSF shall restrict the ability to [manage] the [*TSF data*[27]] to [*authorized administrators*].

[27] Data for the operation of the target of evaluation (TOE) upon which the enforcement of the security functional requirement (SFR) relies

FMT_SMF.1(a) Specification of management functions (CDM)

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*administer the TOE remotely*].

FMT_SMF.1(b) Specification of Management Functions (SC-P)

FMT_SMF.1.1

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

- *creation and deletion of local user accounts;*
- *associating a user with a default role;*
- *creating an X.509v3 certificate request;*
- *installing an X.509v3 certificate*

].

FMT_SMR.2 Restrictions on security roles (CDM)

Dependencies: FIA_UID.1 Timing of identification
Hierarchical to: FMT_SMR.1 Security roles

FMT_SMR.2.1

The TSF shall maintain the roles: [*Administrator, End User*].

FMT_SMR.2.2

The TSF shall be able to associate users with roles.

FMT_SMR.2.3

The TSF shall ensure that the conditions [*only the authorized administrator shall administer the TOE remotely*] are satisfied.

FMT_MSA.1 Management of security attributes (CDM)

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

FMT_MSA.1.1

The TSF shall enforce the [*Rubrik Access Control*] to restrict the ability to [modify] the security attributes [*authentication, logging, reporting*] to [*authorized administrators*].

FMT_MSA.3 Static attribute initialization (CDM)

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

FMT_MSA.3.1

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

FMT_MSA.3.2

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

6.2.6 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps (CDM)

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

6.2.7 Class FTA: TOE Access

FTA_SSL.4 User-initiated termination (SC-P)

FTA_SSL.4.1

The TSF shall allow user-initiated termination of the user's own interactive session.

FTA_TAB.1 Default TOE access banners (SC-P)

FTA_TAB.1.1

Before establishing a user session, the [TSF] shall display an [*advisory warning regarding unauthorized use of the TOE*] message.

6.2.8 Class FTP: Trusted path/channels

FTP_ITC.1 Inter-TSF trusted channel (CDM & SC-P)

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit [*the TSF and another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*all security functions specified in the ST that interact with another trusted IT product and no other functions*].

FTP_TRP.1 Trusted path (CDM & SC-P)

FTP_TRP.1.1

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

FTP_TRP.1.2

The TSF shall permit [*the TSF and local users*] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [*initial user authentication and management operations*].

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 2+ augmented with ALC_FLR.2. Table 17 summarizes these requirements.

Table 17 – 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 system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Basic Flaw Remediation
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

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 18 lists the security functionality and their associated SFRs.

Table 18 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security audit	FAU_GEN.1	Audit data generation (CDM & SC-P)
	FAU_GEN.2	User identity association (CDM & SC-P)
	FAU_SAR.1	Audit review (CDM & SC-P)
	FAU_SAR.3	Selectable audit review (CDM & SC-P)
	FAU_SEL.1	Selective audit (SC-P)
Cryptographic support	FCS_CKM.1	Cryptographic key generation (CDM & SC-P)
	FCS_CKM.3	Cryptographic Key Access (CDM & SC-P)
	FCS_CKM.6	Timing and event of cryptographic key destruction (CDM & SC-P)
	FCS_COP.1(a)	Cryptographic operation (CDM)
	FCS_COP.1(b)	Cryptographic operation (SC-P)
	FCS_RNG.1	Random number generation (CDM & SC-P)
User data protection	FDP_ACC.1	Subset Access Control (CDM)
	FDP_ACF.1	Security attribute-based access control (CDM)
Identification and Authentication	FIA_ATD.1	User attribute definition (CDM)
	FIA_UAU.2	User authentication before any action (CDM & SC-P)
	FIA_UAU.5	Multiple authentication mechanisms (CDM & SC-P)
	FIA_UID.2	User identification before any action (CDM & SC-P)
Security management	FMT_MTD.1	Management of TSF[28] data (CDM)
	FMT_SMF.1(a)	Specification of Management Functions (CDM)
	FMT_SMF.1(b)	Specification of Management Functions (SC-P)
	FMT_SMR.2	Restrictions on security roles (CDM)
	FMT_MSA.1	Management of security attributes (CDM)
	FMT_MSA.3	Static attribute initialization (CDM)
Protection of the TSF	FPT_STM.1	Reliable time stamps (CDM)
TOE Access	FTA_SSL.4	User-initiated termination (SC-P)

[28] TSF – TOE Security Function

TOE Security Functionality	SFR ID	Description
	FTA_TAB.1	Default TOE access banners (SC-P)
Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel (CDM & SC-P)
	FTP_TRP.1	Trusted path (CDM & SC-P)

7.1.1 Security Audit

SC-P and CDM together generate audit logs that identify specific TOE operations whenever an auditable event occurs. This includes audit records for start-up and shutdown of the audit function, all administrative actions, and the pausing and resuming of protection activity. Each audit event includes the date and time of the event, type of event, outcome, and a reliable time stamp so that the TOE can accurately record the time each event occurred. Also, potentially time-sensitive notifications and completed replication tasks are recorded.
FAU_GEN.1

SC-P and CDM together ensure that each auditable event is associated with the user that triggered the event. For an IT entity or device, the VM name of the endpoint is included in the audit record.
FAU_GEN.2

The administrators are allowed to read the audit records and event information, but they have no other access privileges to the buffer containing the audit log. Audit events can be filtered based on various parameters which is suitable for the user to interpret the data.
FAU_SAR.1.

The TOE allows administrators to filter audit data based off the options in the Web GUI. For CDM, this includes status, object, type, and time range. For SC-P, this includes time range, connected clusters, severity, status, event type, and object type.
FAU_SAR.3

SC-P receives audit log and event log entries from the connected CDM clusters. The filters for each audit record include:

Table 19 – Audit Record Filters for SC-P

Filter	Description
Time range	Displays a sequential view of the events that occur during the selected period. • Past 2 hours • Past 24 hours • Past 7 days • Past 30 days
Clusters	Lists all connected Rubrik clusters. Selecting a value changes the display to only show audit log messages for the selected Rubrik cluster.
Severity	Lists events of all severity levels. • Critical • Warning • Informational Selecting a value changes the display to only show audit log messages for the selected severity level.

Filter	Description
Status	Displays events with the selected status. Clear selection to see all events. • Failure • Running • Completed • Canceled • Queued
Event Type	Displays audit records of a specific event type.
Object Type	Displays audit records associated with a specific object.

FAU_SEL.1

7.1.2 Cryptographic Support

CDM uses TLS 1.2/1.3 to protect administrative communications using the Web GUI. TLS 1.2/1.3 is also used to protect communications between the components of the TOE, and the TOE's communication with clusters that it remotely administers. For TLS session keys, the TOE uses symmetric AES keys to encrypt and decrypt data.

For SC-P, The TOE uses SSH and HTTPS to protect administrative communications. TOE administrators access the TOE's CLI/API remotely via an SSH connection. TOE administrators access the web GUI remotely via an HTTPS connection. TLS 1.2/1.3 is used for forwarding of audit data to the TOE from clusters, using X.509v3 certificates for endpoint authentication. Additionally, TLS 1.2/1.3 is also used to protect communications with a remote authentication server. For both TLS and SSH session keys, the TOE uses symmetric AES keys to encrypt and decrypt data.

CDM utilizes Bouncy Castle FIPS Java API (CMVP[29] #4743), Boring Crypto (CMVP #4407), and Open SSL FIPS Provider (CMVP #4282) for all cryptographic functions. SC-P utilizes Bouncy Castle FIPS Java API (CMVP #4743) for all cryptographic functions.

Keys are generated via the use of the Counter_DRBG (CMVP #4743) to provide random keying material.
FCS_CKM.1

The TOE reads the stored keys and writes the keys to Trusted Platform Module (TPM) which meets AES-256 as specified in NIST SP FIPS-197.
FCS_CKM.3

A passphrase configured at bootstrap serves as the Master Secret. The passphrase must then be entered manually during the boot process to unwrap the Cluster Key and Data Encryption Key (KEK, DEK). The master passphrase is not stored persistently within the TOE. The Cluster KEK and DEK reside in volatile memory, and they must remain present in memory at all times to facilitate constant disk I/O and operations for data protection.

The master passphrase is regenerated during system bootstrap and each reboot. The Cluster KEK and DEK in-memory destruction occurs immediately upon power off or reset of the system.

All keys (TLS, master, KEK, and DEK) are zeroized due to the inherent properties of volatile RAM. Due to the keys never being written to non-volatile storage, removing the power zeroizes the key material and they cannot be

[29] CMVP – Cryptographic Module Validation Program

retained without electrical charge. As such, there is no evidence for the zeroization since logs and memory dumps for this cannot be captured after the system is powered off.
FCS_CKM.6

CDM provides cryptographic capabilities to support the operations listed in Table 16.

SC-P utilizes Bouncy Castle FIPS Java API (CMVP #4743) for all cryptographic functions.
FCS_COP.1(a), FCS_COP.1(b)

The TOE uses ChaCha20-Poly1305 to generate random numbers for TLS and key generation.
FCS_RNG.1

7.1.3 User Data Protection

The ability to execute commands for CDM is restricted by Rubrik Access Control to authorized administrators. Rubrik Access Control consists of a set of attribute-based access control rules enforced by the TSF to regulate operation on objects based on subject roles and attributes.
FDP_ACC.1

The ability to change usernames and passwords for CDM is restricted to authorized administrators. If an authorized administrator requests access to an object, access is granted.
FDP_ACF.1

7.1.4 Identification and Authentication

User account information is stored in CDM and contains the following attributes for local users:

- User name – The logon name of the user.
- Email address – The valid email address for the user.
- Password – The user must use a strong password.
- Access rights - By default, the TOE sets all new local user accounts to the Administrator authorization level.

FIA_ATD.1

Each individual must be successfully identified and authenticated with a username and password by the TSF before access is allowed to the TOE. The TOE supports password-based authentication and time-based password. Users must authenticate using a password followed by time-based password. Upon both authentication methods succeeding, the user is allowed access to the TOE. No actions are allowed, other than entry of identification and authentication data, until successful identification and authentication.
FIA_UAU.2, FIA_UAU.5, FIA_UID.2

7.1.5 Security Management

The ability to modify the security attributes for CDM is restricted to authorized administrators.
FMT_MTD.1

The TOE restricts management activities to authorized administrators.

CDM allows the TOE to be administered remotely by authorized administrators.

SC-P management activities include the creation and deletion of local user accounts, associating a user with a default role, creating an X.509v3 certificate request, and installing an X.509v3 certificate.
FMT_SMF.1(a), FMT_SMF.1(b)

CDM supports the following roles:

- Administrator –operator with full access to all functionality that is available through the Web UI
- End User –operator with access only to assigned objects

FMT_SMR.2

CDM restricts the ability to modify security attributes to authorized administrators by enforcing the attribute-based rules defined in Rubrik Access Control.
FMT_MSA.1

CDM provides permissive default values for security attributes. CDM provides the ability to modify the security attributes, which is restricted to authorized administrators. The default values for security attributes are listed below.

- Local authentication data (password):
  - Minimum characters: 8
  - Minimum lower-case characters: 0
  - Minimum upper-case characters: 0
  - Minimum numerical characters: 0
  - Minimum special characters: 0
  - Use zxcvbn algorithm: Disabled
  - Prevent password reuse: Disabled

FMT_MSA.3

7.1.6 Protection of the TSF

The TOE provides a source of date and time information used in audit event timestamps.
FPT_STM.1.

7.1.7 TOE Access

Users can log out of the TOE when they have finished their tasks.
FTA_SSL.4

Users logging into TOE's Web UI are presented with one security login banner. This banner can be configured by authorized administrators.
FTA_TAB.1

7.1.8 Trusted path/channels

The TOE provides trusted communication channels between itself and another trusted IT products. Its configuration covers the following list of cipher suites:

- SC-P:
  - TLS 1.2: ECDHE_RSA_WITH_AES_128_GCM_SHA256, ECDHE_RSA_WITH_AES_256_GCM_SHA384, ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS 1.3: TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256

- CDM:
  - TLS 1.2:
    ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES128-GCM-SHA256 (disabled by default), ECDHE-RSA-AES128-GCM-SHA256 (disabled by default).
  - TLS 1.3:
    TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256.

ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 and TLS_CHACHA20_POLY1305_SHA256 are out of scope for this evaluation; therefore, all ChaCha20-Poly1305 cipher suites must be disabled on client devices. Internal TOE communication (CDM–RSC-P) uses TLS v1.3 with TLS_AES_256_GCM_SHA384 by default and does not rely on ChaCha20-Poly1305.

The CDM CLI allows configuration of the maximum supported TLS version and cipher suites for all nodes in a Rubrik cluster. CDM supports TLS 1.2 (default) and TLS 1.3, and enforces TLS 1.2 as the minimum supported version, which cannot be changed. Although TLS 1.3 is supported and can be enabled, certain internal communications between CDM and SC-P may continue to use TLS 1.2. This is an expected behavior due to implementation limitations of internal gRPC client calls. These communications are limited to non-sensitive operational procedure calls and occur only within the customer's protected internal network.

FTP_ITC.1

The TOE provides a communication path between itself and local users, and it allows both local users and the TOE itself to initiate said path.

FTP_TRP.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*, CC:2022, Revision 1.

8.2 Security Objectives Rationale

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

8.2.1 Security Objectives Rationale Relating to Threats

Table 20 below provides a mapping of the objectives to the threats they counter.

Table 20 – Threats: Objectives Mapping

Threats	Objectives	Rationale
TT.ADMIN_ERROR An administrator unintentionally configures the TOE incorrectly, making the TOE inoperable or resulting in ineffective security mechanisms.	O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	The objective O.MANAGE provides administrators the capability to view and manage configuration settings.
	OE.TRUSTED_ADMIN The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines as indicated by Rubrik and any additional trusted parties in which an agreement has been entered.	The objective OE.TRUSTED_ADMIN ensures that the administrators are non-hostile and are trained to appropriately manage and administer the TOE.
TT.ADMIN_EXPLOIT A person/company uses hacking methods to exploit missing, weak or incorrectly implemented access control in the TOE.	O.ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	The objective O.ACCESS includes mechanisms to authenticate TOE administrators and place controls on administrator sessions.
	O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	The objective O.MANAGE restricts access to administrative functions and management of TSF data to the administrator.
	OE.TRUSTED_ADMIN The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines as indicated by Rubrik and any additional trusted parties in which an agreement has been entered.	The objective OE.TRUSTED_ADMIN ensures that the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.

Threats	Objectives	Rationale
TT.CRYPTO_COMPROMISE An attacker causes key or data associated with the cryptographic functionality to be inappropriately accessed (viewed/modified/deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.	O.PROTECTION The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.	The objective O.PROTECTION ensures that the TOE will have adequate protection from external sources and that all TOE Security Policy functions are invoked.
TT.HACK_ACCESS A person/company uses hacking methods to exploit missing, weak or incorrectly implemented access control in the TOE.	O.AUDIT The TOE shall record and maintain security-related events to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.	The objective O.AUDIT provides the TOE the capability to detect and create records of security-relevant events associated with users.
	O.ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	The objective O.ACCESS includes mechanisms to authenticate TOE administrators and place controls on administrator sessions.
	O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	The objective O.MANAGE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the administrator. These objectives ensure that no other user can modify the information flow policy to bypass the intended TOE security policy.
	O.PROTECTION The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.	The objective O.PROTECTION ensures that the TOE will have adequate protection from external sources and that all TOE Security Policy functions are invoked.
	OE.TRUSTED_ADMIN The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines as indicated by Rubrik and any additional trusted parties in which an agreement has been entered.	The objective OE.TRUSTED_ADMIN ensures that the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.
TT.MALFUNCTION A malfunction in the TOE implies unauthorized access to TOE resources.	O.AUDIT The TOE shall record and maintain security-related events to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.	The objective O.AUDIT provides the TOE the capability to detect and create records of security-relevant events associated with users.
	O.ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	The objective O.ACCESS includes mechanisms to authenticate TOE administrators and place controls on administrator sessions.
	O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality of 'data in flight'.	The objective O.CRYPTOGRAPHY requires the TOE to implement cryptographic services to provide confidentiality protection of data in flight.
	O.PROTECTION The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.	The objective O.PROTECTION ensures that the TOE will have adequate protection from external sources and that all TOE Security Policy functions are invoked.

Threats	Objectives	Rationale
TE.EAVESDROPPING	O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality of 'data in flight'.	The objective O.CRYPTOGRAPHY requires the TOE to implement cryptographic services to provide confidentiality protection of data in flight.
	O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	The objective O.MANAGE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the administrator.

This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Assumptions

Table 21 provides a mapping of assumptions and the environmental objectives that uphold them.

Table 21 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system.	O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	The objective O.MANAGE ensures that the download of the TOE is limited to users with the appropriate privileges.
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.	OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	The objective OE.PHYSICAL ensures that the environment provides physical security, commensurate with the value of the TOE and the data it contains.
A.TRUSTED_ADMIN The administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines..	OE.TRUSTED_ADMIN The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines as indicated by Rubrik and any additional trusted parties in which an agreement has been entered.	The objective OE.TRUSTED_ADMIN ensures that the administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
A.LOCATE The TOE is located within a controlled access facility.	OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. OE.PHYSICAL satisfies this assumption.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	O.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.

Assumptions	Objectives	Rationale
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	O.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.

This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.2.3 Security Objectives Rationale Relating to Organizational Security Policies

Table 22 a mapping of policies effectively addressed by the security objectives.

Table 22– Policies: Objectives Mapping

Assumptions	Objectives	Rationale
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	The objective O.ACCESS requires the TOE to identify and authenticate users prior to allowing any TOE access or any TOE mediated access on behalf of those users
	O.AUDIT The TOE shall record and maintain security-related events to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.	The objective O.AUDIT provides the administrator with the capability of recording the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the administrator's user identifier is recorded when any security relevant change is made to the TOE (e.g., modifying TSF data).
	OE.TRUSTED_ADMIN The administrator of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines as indicated by Rubrik and any additional trusted parties in which an agreement has been entered.	The objective OE.TRUSTED_ADMIN ensures that the TOE administrators have guidance that instructs them how to administer the TOE in a secure manner.
P.CRYPTOGRAPHIC The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.	O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality of 'data in flight'.	The objective O.CRYPTOGRAPHY requires the TOE to implement cryptographic services to provide confidentiality protection of the TOE.

8.3 Rationale for Extended Security Functional Requirements

There are no extended SFRs defined for this ST.

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 23 provides a mapping of the objectives and the SFRs that support them.

Table 23 – Objectives: SFRs Mapping

Objective	SFR	Rationale
O.ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.	FIA_ATD.1 User attribute definition (CDM)	FIA_ATD.1 defines the attributes of users, including a user identifier that is used by the TOE to determine a user's identity and enforce what type of access the user has to the TOE, and ensures that untrusted users cannot be associated with a role and reduces the possibility of a user obtaining administrative privileges.
	FIA_UAU.2 User authentication before any action (CDM & SC-P)	FIA_UAU.2 ensures that users are authenticated before they are provided access to the TOE or its services. In order to control logical access to the TOE an authentication mechanism is required. The local user authentication mechanism is necessary to ensure that an administrator has the ability to login to the TOE regardless of network connectivity (e.g., it would be unacceptable if an administrator could not login to the TOE because the authentication server was down, or that the network path to the authentication server was unavailable).
	FIA_UAU.5 Multiple authentication mechanisms (CDM & SC-P)	FIA_UAU.5 defines that two authentication methods are used to access the TOE. Time-based authentication must be used after password authentication to access the TOE. This is to secure logical access to the TOE.
	FIA_UID.2 User identification before any action (CDM & SC-P)	FIA_UID.2 ensures that every user is identified before the TOE performs any mediated functions.
	FMT_MSA.3 Static attribute initialization (CDM)	FMT_MSA.3 defines static attribute initialization for the Rubrik Access Control.. FMT_MSA.1 specifies which roles can access security attributes.
	FDP_ACC.1 Subset Access Control (CDM)	FDP_ACC.1 requires the TOE to enforce Access Control SFP.
	FDP_ACF.1 Security attribute based access control (CDM)	FDP_ACF.1 specifies the attributes used to enforce Access Control SFP.
	FTA_SSL.4 User-initiated termination (SC-P)	FTA_SSL.4 meets the objective by allowing TOE users to terminate their own session.
	FTA_TAB.1 Default TOE access banners (SC-P)	FTA_TAB.1 meets the objective by allowing the user to configure an access banner warning against unauthorized access.
O.AUDIT The TOE shall record and maintain security-related events to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.	FAU_GEN.1 Audit data generation (CDM & SC-P)	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant event that takes place in the TOE.
	FAU_GEN.2 User identity association (CDM & SC-P)	FAU_GEN.2 ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID.

Objective	SFR	Rationale
	FAU_SAR.1 Audit review (CDM & SC-P)	FAU_SAR.1 provides administrators the capability to read the audit records.
	FAU_SAR.3 Selectable audit review (CDM & SC-P)	FAU_SAR.3 meets the objective by ensuring that the user can search and filter the audit data.
	FAU_SEL.1 Selective audit (SC-P)	FAU_SEL.1 meets this objective by ensuring the user is able to select the set of events to be audited from the set of all auditable events based on their attributes.
	FPT_STM.1 Reliable time stamps (CDM)	FPT_STM.1 supports the audit functionality by ensuring that the TOE is capable of obtaining a time stamp for use in recording audit events.
O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality of 'data in flight'.	FCS_CKM.1 Cryptographic key generation (CDM & SC-P)	FCS_CKM.1 ensures that the TOE is capable of generating cryptographic keys.
	FCS_CKM.3 Cryptographic key access (CDM & SC-P)	FCS_CKM.3 specifies the type of cryptographic key access, methods which meets a particular NIST standard.
	FCS_CKM Timing and event of cryptographic key destruction (CDM & SC-P)	FCS_CKM.6 provides the functionality for ensuring that keys and key material for CDM & SC-P are zeroized.
	FCS_COP.1(a) Cryptographic operation (CDM)	FCS_COP.1 requires that for data decryption and encryption an approved algorithm is used, and that the algorithm meets the standard.
	FCS_COP.1(b) Cryptographic operation (SC-P)	FCS_COP.1 requires that for data decryption and encryption an approved algorithm is used, and that the algorithm meets the standard.
	FCS_RNG.1 Random number generation (CDM & SC-P)	FCS_RNG.1 requires that the random generation of numbers for key generation is performed according to defined standards.
	FTP_ITC.1 Inter-TSF trusted channel (CDM & SC-P)	FTP_ITC.1 ensures that the TOE establishes a trusted channel with other trusted IT entities using cryptographic mechanisms that protect the data from disclosure and modification during transmission.
	FTP_TRP.1 Trusted path (CDM & SC-P)	FTP_TRP.1 ensures that the TOE provides a trusted path for users to communicate securely with the TSF for initial authentication and management operations.
O.MANAGE The TOE shall provide means for the administrators of the TOE to efficiently manage the TOE in a secure manner, and restrict these means from unauthorized use.	FAU_SAR.1 Audit Review (CDM & SC-P)	FAU_SAR.1 provides the administrators the capability to read all information from the audit records.
	FMT_MSA.1 Management of security attributes (CDM)	FMT_MSA.1 specifies which roles can access security attributes.
	FMT_MSA.3 Static attribute initialization (CDM)	FMT_MSA.3 defines static attribute initialization for the Rubrik Access Control.
	FMT_MTD.1 Management of TSF data (CDM) FMT_SMF.1(a) Specification of Management Functions (CDM) FMT_SMF.1(b) Specification of Management Functions (SC-P) FMT_SMR.2 Restrictions on security roles (CDM)	FMT_MTD.1, FMT_SMF.1(a), FMT_SMF(b) and FMT_SMR.2 ensure that only the Administrator role can manage the entire TOE, and that the TOE supports both local administration and remote administration.

Objective	SFR	Rationale
O.PROTECTION The TOE must protect itself and its resources from unauthorized modifications and access to its functions and data.	FMT_MTD.1 Management of TSF data (CDM) FMT_SMF.1(a) Specification of Management Functions (CDM) FMT_SMF.1(b) Specification of Management Functions (SC-P) FMT_SMR.2 Restrictions on security roles (CDM)	FMT_MTD.1, FMT_SMF.1(a), FMT_SMF.1(b), and FMT_SMR.2 ensure that only authorized administrators of the TOE may manage the TOE and TSF data.
	FMT_MSA.1 Management of security attributes (CDM)	FMT_MSA.1 specifies which roles can access security attributes.
	FDP_ACC.1 Subset Access Control (CDM)	FDP_ACC.1 requires the TOE to enforce Access Control SFP.
	FDP_ACF.1 Security attribute based access control (CDM)	FDP_ACF.1 specifies the attributes used to enforce Access Control SFP.
	FIA_UAU.2 User authentication before any action (CDM & SC-P)	FIA_UAU.2 meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authenticated users are allowed access to TOE functions.
	FIA_UAU.5 Multiple authentication mechanisms (CDM & SC-P)	FIA_UAU.5 meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authenticated users are allowed access to TOE functions.
	FIA_UID.2 User identification before any action (CDM & SC-P)	FIA_UID.2 meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only identified users are allowed access to TOE functions.

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. 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

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. The following table lists each SFR to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 24 – SFR Dependencies and Rationales

SFR	Dependency	Rationale
FAU_GEN.1 Audit data generation (CDM & SC-P)	FPT_STM.1 Reliable time stamps	Included

SFR	Dependency	Rationale
FAU_GEN.2 User identity association (CDM & SC-P)	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	Included[30]
FAU_SAR.1 Audit review (CDM & SC-P)	FAU_GEN.1 Audit data generation	Included
FAU_SAR.3 Selectable audit review (CDM & SC-P)	FAU_SAR.1 Audit Review	Included
FAU_SEL.1 Selective audit (SC-P)	FAU_GEN.1 Audit data generation FMT_MTD.1 Management of TSF data	Included
FDP_ACC.1 Subset access control (CDM)	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control (CDM)	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization	Included
FCS_CKM.1 Cryptographic key generation (CDM & SC-P)	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction	Included[31]
FCS_CKM.3 Cryptographic Key Access (CDM & SC-P)	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation]	Included[32]
FCS_CKM.6 Cryptographic key destruction (CDM & SC-P)	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Included[33]
FCS_COP.1(a) Cryptographic Operation (CDM)	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	Included[35]
FCS_COP.1(b) Cryptographic Operation (SC-P)	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access	Included[32]
FCS_RNG.1 Random number generation (CDM & SC-P)	None	
FIA_ATD.1 User attribute definition (CDM)	None	
FIA_UAU.2 User authentication before any action (CDM & SC-P)	FIA_UID.1 Timing of identification	Included[33]
FIA_UAU.5 Multiple authentication mechanisms	None	
FIA_UID.2 User identification before any action (CDM & SC-P)	None	
FMT_MTD.1 Management of TSF data (CDM)	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions	Included[34]

[30] FAU_GEN.2 has a dependency to FIA_UID.1 which is covered by FIA_UID.2 because it is hierarchical to FIA_UID.1.
[31] FCS_CKM.1 has dependencies that are satisfied by FCS_COP.1, FCS_CKM.3, FCS_RNG.1, and FCS_CKM.6.
[32] FCS_CKM.3 Cryptographic Key Access dependency is satisfied by FCS_CKM.1.
[33] FCS_CKM.6 Cryptographic key destruction dependency is satisfied by FCS_CKM.1.

[32] FCS_COP.1(b) has dependencies for FCS_CKM.1 and FCS_CKM.3, which are satisfied by the TOE.
[33] FIA_UAU.2 has a dependency to FIA_UID.1 which is covered by FIA_UID.2 because it is hierarchical to FIA_UID.1.
[34] FMT_MTD.1 has a dependency to FMT_SMR.1 which is covered by FMT_SMR.2 because it is hierarchical to FMT_SMR.1.

SFR	Dependency	Rationale
FMT_SMF.1(a) Specification of Management Functions (CDM)	None	
FMT_SMF.1(b) Specification of Management Functions (SC-P)	None	
FMT_SMR.2 Restrictions on security roles (CDM)	FIA_UID.1 Timing of identification	Included[35]
FMT_MSA.1 Management of security attributes (CDM)	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Included[36]
FMT_MSA.3 Static attribute initialization (CDM)	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Included[5]
FPT_STM.1 Reliable time stamps (CDM)	None	
FTA_SSL.4 User-initiated termination (SC-P)	None	
FTA_TAB.1 Default TOE access banners (SC-P)	None	

[35] FIA_UID.1 is covered by FIA_UID.2 because it is hierarchical to FIA_UID.1.
[36] FMT_MSA.1 and FMT_MSA.3 have a dependency to FMT_SMR.1 which is covered by FMT_SMR.2 because it is hierarchical to FMT_SMR.1.

9. Acronyms and Terms

Table 25 defines the acronyms and terms used throughout this document.

Table 25 – Acronyms and Terms

Acronym / Term	Definition
AD	Active Directory Microsoft Windows directory service that facilitates working with interconnected, complex and different network resources in a unified manner
AES	Advanced Encryption Standard
API	Application Programming Interface Set of routines, protocols, and tools for building software and applications
Authorized users	Authorized users are responsible for the management of the TOE.
CC	Common Criteria
CDM	Cloud Data Management A system that distributes data, metadata, and task management across the cluster in order to deliver predictive scalability and eliminate performance bottlenecks.
CEM	Common Evaluation Methodology
CM	Configuration Management
CPU	Central Processing Unit
Data deduplication	Specialized data compression technique for eliminating duplicate copies of repeating data
DNS	Domain Name Service
EAL	Evaluation Assurance Level
EC	Elliptic Curve
FIPS	Federal Information Processing Standard
GB	Gigabyte
GHz	Gigahertz
HMAC	Keyed Message Authentication Code
Hypervisor	Hypervisor (or VM monitor) is a piece of computer software, firmware or hardware that creates and runs VMs
HTTPS	Hypertext Transport Protocol - Secure
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol An open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network
NIST	National Institute of Standards and Technology
OS	Operating System
OVA	Open Virtual Appliance
PP	Protection Profile
PUB	Publication
RAM	Random Access Memory

Acronym / Term	Definition
RBAC	Role Based Access Control Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file.
RPC	Remote Procedure Call Client/Server system in which a computer program causes a subroutine or procedure to execute in another address space without the programmer explicitly coding the details for this remote interaction
RSA	Rivest Shamir Adelman
SAR	Security Assurance Requirement
SC-P	Security Cloud-Private
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Simple Hashing Algorithm
SLA	Service Level Agreement
Snapshot	Backup copy of a virtual machine. Each snapshot is a file. The first snapshot is a full copy of the virtual machine. Each subsequent snapshot is an incremental delta from the previous file. Every snapshot is a fully functional, point-in-time copy of the source VM.
SP	Special Publication
SSH	Secure Shell A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels
ST	Security Target
TLS	Transport Layer Security A protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
VM	Virtual Machine
VMDK	Virtual Machine Disk File format that describes containers for virtual hard disk drives to be used in virtual machines like VMware Workstation or VirtualBox (hypervisor)

Prepared by:

Corsec Security, Inc.

12600 Fair Lakes Drive, Suite 210
Fairfax, VA 22003
United States of America

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