Rubrik Inc.

Security Cloud - Private

v2.3

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.0

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 Figures

List of Tables

1. Introduction

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

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 v2.3 Security Target*
ST Version	Version 1.0
ST Author	Corsec Security, Inc.
ST Publication Date	2024-05-09
TOE Reference	Rubrik SC-P v2.3

1.3 TOE Overview

Rubrik Security Cloud - Private permits administration and management of multiple Rubrik clusters through a single web UI. A Rubrik cluster is a collection of objects that includes sources from where data is getting backed

up, targets where backups are stored, and security principals, 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 Rubrik clusters. SC-P apps monitor the protection and compliance status of Rubrik clusters. Generate reports and charts using current and historical data about the health, protection and compliance status of all of the objects that the Rubrik clusters protect.

The TOE's major security features consist of:

- Web Admin Console
  - The Web Admin Console is a web-based graphical interface used to configure and manage the TOE's 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
  - The TOE 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 the TOE for secure communication via TLS and SSH.

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

Table 2 – TOE Components

Component	Description
Dashboard	Top-down view of all Rubrik 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 Rubrik 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 Rubrik clusters.
SLA Domains	Continually updating view of all SLA Domains created on all Rubrik 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 Rubrik clusters, with filters to focus on a specific Rubrik 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 Rubrik clusters.

1.3.1 TOE Environment

This section details the non-TOE hardware and software required by the TOE.

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 3 – TOE Minimum ESXi Cluster Requirements

Category	Requirement
Datastore	• Fault-tolerance • 10,000 input/output operations per second (IOPS) • 1 TB of available storage

Category	Requirement
Compute 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.

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

The TOE also requires Rubrik clusters to forward audit data to it.

1.4 TOE Description

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

1.4.1 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 software application which runs on a VM whose hypervisor is compliant to the minimum software and hardware requirements as listed in Table 3. The TOE is installed as depicted in the figure below. The essential physical components for the proper operation of the TOE in the evaluated configuration are:

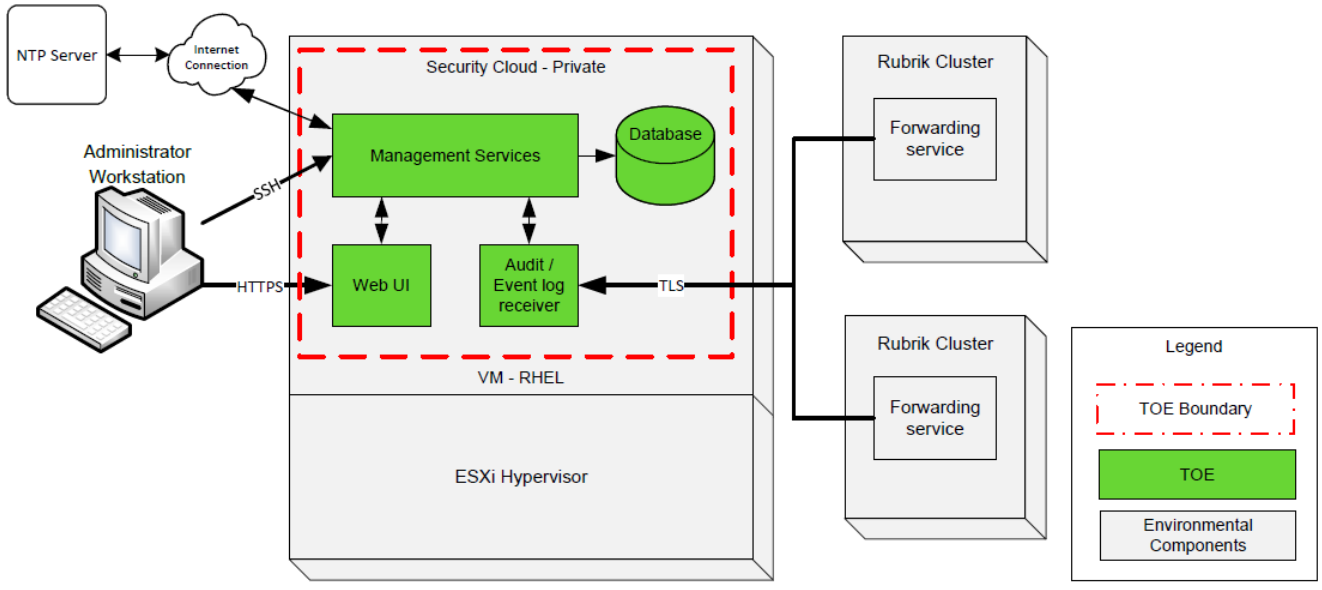

Figure 1 – Physical TOE Boundary

1.4.1.1 TOE Software

The TOE is a software-only TOE and is comprised of the SC-P v2.3 as an image in an OVA format installed in a VM.

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

1.4.1.2 Guidance Documentation

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

- *Rubrik Security Cloud - Private 2.3 CLI Reference (Rev. A0)*
- *Rubrik Security Cloud - Private 2.3 Install and Upgrade Guide (Rev. A0)*
- *Rubrik Security Cloud - Private 2.3 User Guide (Rev. A0)*
- *Rubrik Security Cloud – Private 2.3 Guidance Documentation Supplement v0.6*

1.4.2 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
- TOE Access

1.4.2.1 Security Audit

The TOE receives audit log and event log entries from the connected Rubrik clusters.

1.4.2.2 Cryptographic Support

The TOE relies on a cryptographic module to provide support for securing all communication with the TOE over TLS and SSH.

1.4.2.3 Identification and Authentication

The TOE authenticates users who are then able to perform tasks as administrators.

1.4.2.4 Security Management

The TOE only permits authenticated administrators to access its functionality and perform tasks.

1.4.2.5 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 it by Rubrik clusters.

1.4.2.6 TOE Access

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

1.4.3 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:

- Two-factor authentication
- LDAP Server
- Custom Roles

2. Conformance Claims

This section and Table 4 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 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017; 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.
PP Identification	None
Evaluation Assurance Level	EAL2+ 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[1] and data saved on the TOE from the Rubrik clusters on the protected network. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 5 below lists the applicable threats.

Table 5 – Threats

Name	Description
T.NOAUTH	An attacker may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.

3.2 Organizational Security Policies

There are no Organizational Security Policies (OSPs) defined for this ST.

3.3 Assumptions

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

[1] TSF – TOE Security Functionality

Name	Description
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.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 7 below.

Table 7 – Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must receive events of security relevance at the "not specified level" of audit. The TOE must receive the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide the authorized administrators with the ability to review the audit trail.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.AUTHENTICATE	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.PROTECT	The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.
O.ACCESS	The TOE must provide functionality that will warn TOE users about usage of the TOE below logging in, and allow TOE users to terminate their own sessions after logging in.
O.CRYPTOGRAPHY	The TOE shall provide cryptographic functions to maintain the confidentiality of 'data in flight'.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

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

Table 8 – 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

Table 9 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 9 – Non-IT Security Objectives

Name	Description
OE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
OE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

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

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 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_SAR.1	Audit review		✓		
FAU_SAR.3	Selectable audit review		✓		
FAU_SEL.1	Selective audit	✓	✓		
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FIA_UAU.2	User authentication before any action				
FIA_UID.2	User identification before any action				
FMT_SMF.1	Specification of Management Functions	✓			
FPT_STM.1	Reliable time stamps				

Name	Description	S	A	R	I
FTA_SSL.4	User-initiated termination				
FTA_TAB.1	Default TOE access banners				

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

6.2.1 Class FAU: Security Audit

FAU_SAR.1 Audit review

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 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 [*selections made in the web GUI*].

FAU_SEL.1 Selective audit

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

Dependencies: FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*AES Counter_DRBG*] and specified cryptographic key sizes [*256 bits*] that meet the following: [*NIST[2] SP[3] 800-90A*].

FCS_CKM.4 Cryptographic key destruction

Dependencies: FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwrite with 0s and 1s*] that meets the following: [*NIST SP 800-88 R1*].

[2] NIST - National Institute of Standards and Technology
[3] SP – Special Publication

FCS_COP.1 Cryptographic operation

Dependencies: FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

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*[4] *197*].

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_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_SMF.1 Specification of Management Functions

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

].

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.

6.2.6 Class FTA: TOE Access

FTA_SSL.4 User-initiated termination

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

FTA_TAB.1.1

[4] Federal Information Processing Standard

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

6.3 Security Assurance Requirements

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

Table 11 – Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC: Life Cycle Support	ALC_CMC.2 Use of a CM 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 12 lists the security functionality and their associated SFRs.

Table 12 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Identification and Authentication	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Security Management	FMT_SMF.1	Specification of management functions
Protection of TOE Security Functionality	FPT_STM.1	Reliable time stamps
TOE Access	FTA_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners

7.1.1 Security Audit

The TOE receives audit log and event log entries from the connected Rubrik clusters.

Table 13 – Audit Record Filters

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 • N/A 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 • Completed

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

7.1.2 Cryptographic Support

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 is used for forwarding of audit data to the TOE from clusters, using X.509v3 certificates for endpoint authentication. Additionally, TLS 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.

The TOE utilizes the Rubrik Cryptographic Library (CMVP[5] #2658) for all cryptographic functions.

Keys are generated via the use of the Counter_DRBG to provide random keying material.

The TOE provides zeroization techniques that meets the FIPS[6] 140-2 zeroization requirement for all plaintext secret and private keys. TLS and SSH session keys reside in volatile memory only and are never stored persistently.

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

7.1.3 Identification and Authentication

Each individual must be successfully identified and authenticated with a username and password by the TSF before access is allowed to the TOE.

No actions are allowed, other than entry of identification and authentication data, until successful identification and authentication.

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

7.1.4 Security Management

The TOE only permits authenticated administrators to access its functionality and perform tasks. These tasks 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.

TOE Security Functional Requirements Satisfied: FMT_SMF.1.

[5] CMVP – Cryptographic Module Validation Program
[6] FIPS – Federal Information Processing Standard

7.1.5 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 it by Rubrik clusters.

TOE Security Functional Requirements Satisfied: FPT_STM.1.

7.1.6 TOE Access

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

TOE Security Functional Requirements Satisfied: FTA_SSL.4, FTA_TAB.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 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 14 provides a mapping of the objectives to the threats they counter.

Table 14 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.NOAUTH An attacker may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.	O.AUDIT The TOE must receive events of security relevance at the “not specified level” of audit. The TOE must receive the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide the authorized administrators with the ability to review the audit trail.	The objective O.AUDIT ensures that unauthorized attempts to access the TOE are recorded.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	The objective O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	The objective O.AUTHENTICATE ensures that users are identified and authenticated prior to gaining access to TOE security data.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	The objective O.PROTECT ensures that the TOE will have adequate protection from external sources and that all TOE Security Policy functions are invoked.
	O.ACCESS The TOE must provide functionality that will warn TOE users about usage of the TOE below logging in, and allow TOE users to terminate their own sessions after logging in.	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.

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

8.2.2 Security Objectives Rationale Relating to Assumptions

Table 15 provides a mapping of assumptions and the environmental objectives that uphold them.

Table 15 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	The objective O.ADMIN ensures that the download of the TOE is limited to users with the appropriate privileges.
	OE.PLATFORM The TOE hardware and OS must support all required TOE functions.	OE.PLATFORM ensures that the TOE hardware and OS supports the TOE functions.
	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	Those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. OE.MANAGE satisfies this assumption.
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.LOCATE The TOE is located within a controlled access facility.	OE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. OE.PHYSICAL satisfies this assumption.
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.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.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.

8.3 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 16 provides a mapping of the objectives and the SFRs that support them.

Table 16 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must receive events of security relevance at the "not specified level" of audit. The TOE must receive the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide the authorized administrators with the ability to review the audit trail.	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.
	FAU_SAR.3 Selectable audit review	The requirement meets the objective by ensuring that the user can search and filter the audit data.
	FAU_SEL.1 Selective audit	The requirement 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	The requirement meets the objective by ensuring that the TOE is capable of obtaining a time stamp for use in recording audit events
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring that users are authenticated before access to TOE administrative functions is allowed.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the users are identified before access to TOE administrative functions is allowed.
O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FIA_UAU.2 User authentication before any action	The requirement 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	The requirement 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.
O.ACCESS	FTA_SSL.4 User-initiated termination	The requirement meets the objective by allowing TOE users to terminate their own session.

Objective	Requirements Addressing the Objective	Rationale
The TOE must provide functionality that will warn TOE users about usage of the TOE below logging in, and allow TOE users to terminate their own sessions after logging in.	FTA_TAB.1 Default TOE access banners	The requirement meets the objective by allowing the user to configure an access banner warning against unauthorized access.
O.CRYPTOGRAPHY The TOE shall provide cryptographic functions to maintain the confidentiality of 'data in flight'.	FCS_CKM.1 Cryptographic key generation	The requirement meets the objective by ensuring that the TOE is capable of generating cryptographic keys.
	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that keys and key material is zeroized.
	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that for data decryption and encryption an approved algorithm is used, and that the algorithm meets the standard.

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. Table 17 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 17 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_SAR.1	FAU_GEN.1		The audit data that is generated, is forwarded to the TOE from external entities.
FAU_SAR.3	FAU_SAR.1	✓	
FAU_SEL.1	FAU_GEN.1		The audit data that is generated, is forwarded to the TOE from external entities.
	FMT_MTD.1		The evaluated TOE does not support custom roles (the FMT_SMR.1 dependency for FMT_MTD.1), but it does permit subsets of all forwarded audit data to be displayed, which is the query capability identified in FMT_MTD.1.
FCS_CKM.1	FCS_COP.1 FCS_CKM.4	✓ ✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.1 FCS_CKM.4	✓ ✓	
FIA_UAU.2	FIA_UID.1		Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies		
FMT_SMF.1	No dependencies		

SFR ID	Dependencies	Dependency Met	Rationale
FPT_STM.1	No dependencies		
FTA_SSL.4	No dependencies		
FTA_TAB.1	No dependencies		

9. Acronyms and Terms

Table 18 defines the acronyms and terms used throughout this document.

Table 18 – Acronyms and Terms

Acronym	Definition
CC	Common Criteria
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
OS	Operating System
OVA	Open Virtualization Unit
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy

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