WHITE PAPER

# Rubrik Security Cloud Architecture and Security Implementation

# Table of Contents

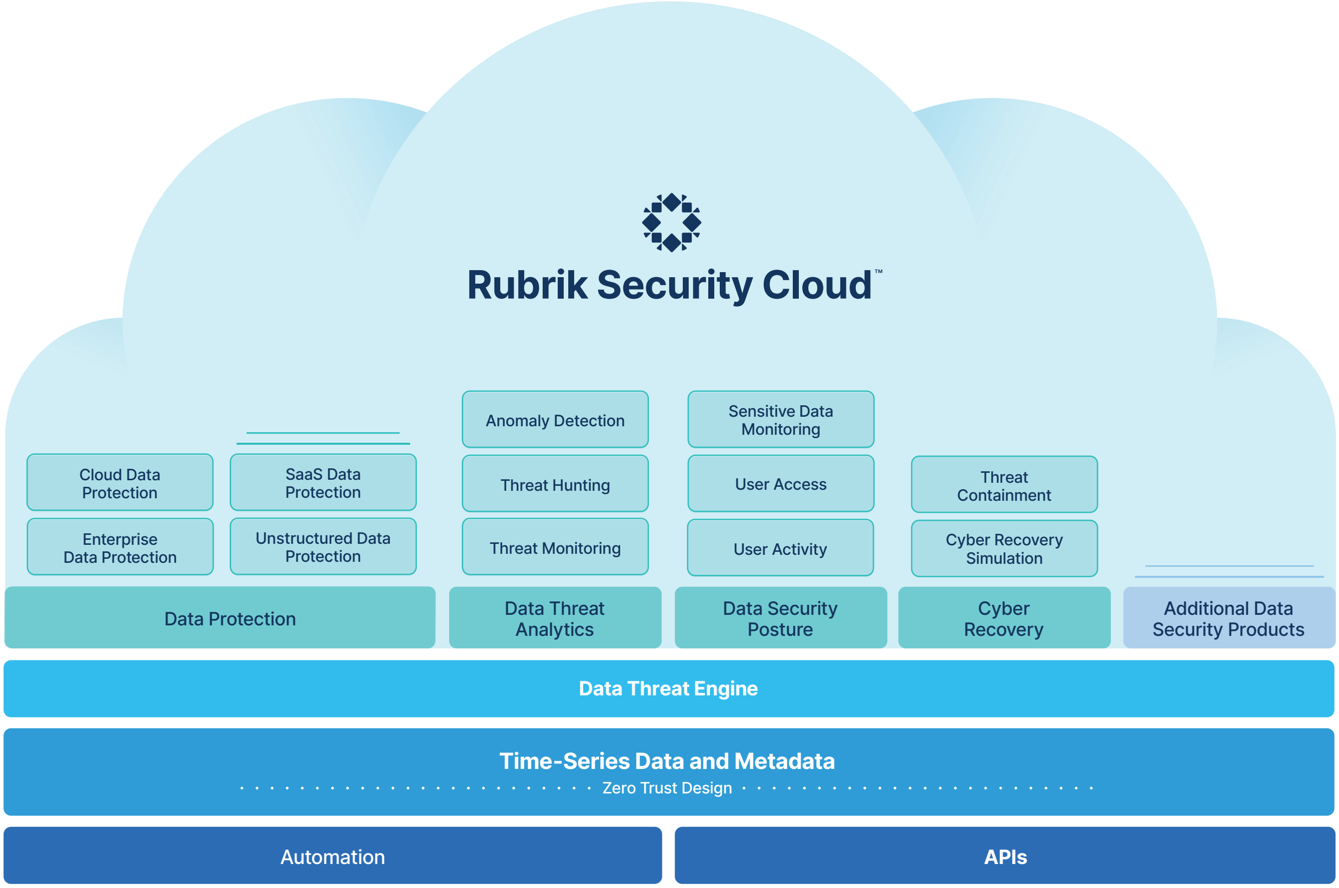
## EXECUTIVE SUMMARY

Rubrik is a cybersecurity company, and our mission is to secure the world's data. We pioneered Zero Trust Data Security™ to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, delivers data protection and cyber resilience in a single platform across enterprise, cloud, and SaaS applications. It helps organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

Rubrik is committed to maintaining customer trust and implementing robust security and privacy practices to protect data across our suite of services is integral to our mission. In this white paper, we will discuss the architecture of Rubrik Security Cloud, including infrastructure, encryption, where data is stored, and how the data is kept immutable and available.

## CHAPTER 1: INTRODUCTION TO RUBRIK SECURITY CLOUD

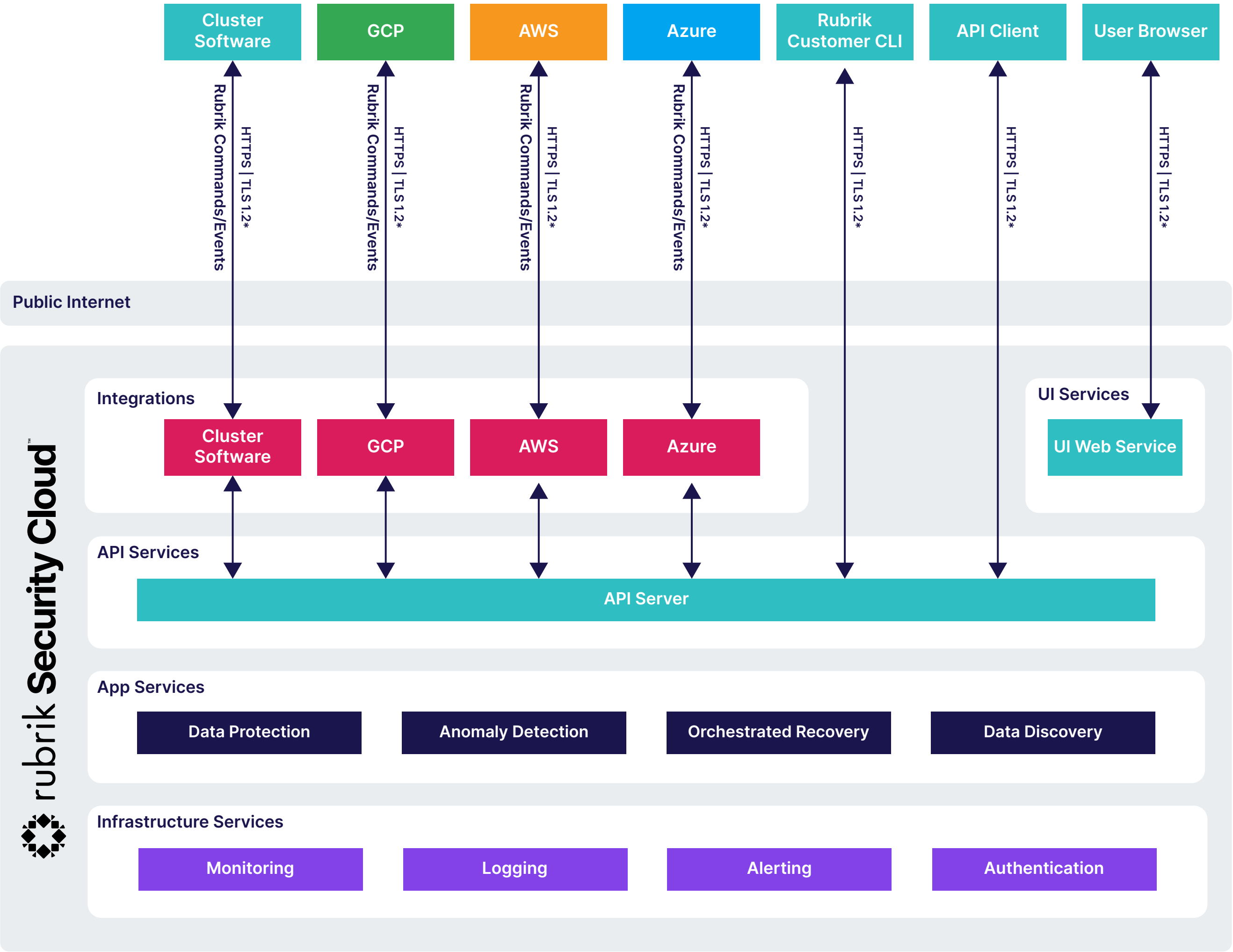
Rubrik Security Cloud is a Software-as-a-Service (SaaS) platform that enables you to keep your data secure, monitor data risk, and quickly recover your data, wherever it lives—across the enterprise, in the cloud, and in SaaS applications. Rubrik offers many data protection and security solutions with air-gapped, immutable, access-controlled backups.



## CHAPTER 2: ARCHITECTURE DESIGN

Rubrik Security Cloud is built upon a secure microservices-based architecture using high-availability services and infrastructure running in Google Cloud Platform (GCP). By using these services, Rubrik can:

- Securely scale services to meet demand
- Store data with strong security and privacy safeguards
- Implement secure communication channels between services
- Secure communication with customers over the public internet



# CHAPTER 3: SECURE BY DESIGN

ACCESS MANAGEMENT

PLATFORM SECURITY

SERVICE MONITORING AND AVAILABILITY

PHYSICAL SECURITY

## ACCESS MANAGEMENT

Rubrik Security Cloud was built with security in mind, using a defense-in-depth approach. From strong access controls to using a Secure Software Development Lifecycle (SSDLC) to ongoing monitoring, security was factored into every aspect of the platform.

**AAA Framework**
Rubrik's approach to security incorporates the AAA framework (Authentication, Authorization, and Accounting). All the access to Rubrik Security Cloud is secured and controlled through Application Programming Interfaces (APIs) built atop the access control model. Whether using the web application, directly accessing APIs, or using a third-party integration, customers control access to their Rubrik Security Cloud accounts via role-based access controls.

### Authentication

**USER ACCOUNTS**
Rubrik Security Cloud provides customers the ability to secure their end users via native accounts or optional integration with a SAML 2.0 compliant identity provider (IdP). When using native Rubrik Security Cloud accounts, Rubrik Security Cloud requires and enforces the use of strong passwords for user authentication and locks accounts after multiple failed attempts.

**API / SERVICE ACCOUNTS**
Rubrik APIs leverage service accounts for authentication and authorization as opposed to user accounts. Service Accounts are used for automation tasks and can be narrowly limited to specific tasks via timed expiration and role-based access controls.

**SINGLE-SIGN ON (SSO)**
Rubrik Security Cloud supports single sign-on (SSO) using the Security Assertion Markup Language (SAML) 2.0 standard. SSO allows customers to log into Rubrik Security Cloud using credentials associated with an identity provider (IdP) of their choice. SAML IdPs allow customers to centrally manage identity, policy (password complexity, MFA requirements), and role mapping across their enterprise.

Rubrik can be integrated with any SAML 2.0-enabled IdP that supports SP-initiated SSO, such as ADFS, Azure AD, Okta, and OneLogin.

### MULTI-FACTOR AUTHENTICATION (MFA)

Rubrik Security Cloud requires multi-factor authentication (MFA) for native accounts and Rubrik Clusters through mobile authentication applications—such as those provided by Microsoft, Google, and Okta—that provide time-based one-time passwords (TOTP) in the form of a numeric code.

For SSO accounts, customers can leverage their IdP's support for MFA to protect the credentials used to access Rubrik Security Cloud.

## Authorization

Rubrik Security Cloud provides fine-grained, role-based access controls (RBAC) that allow for the creation of roles with the least amount of privileges needed to complete a task. These roles can then be assigned to users (both end users and Service Accounts) for authorization.

## Accounting

Rubrik Security Cloud aggregates logs from all connected clusters, so customers can easily monitor changes across all Cluster Software deployments.

Rubrik Security Cloud identifies, isolates, and prioritizes incidents with a unified view of global Rubrik events. Users can find point-in-time events (by event and object type) with easy-to-use filters and real-time search. Events can also be forwarded to Security Information and Event Management (SIEM) or log management systems through webhooks.

2

# PLATFORM SECURITY

## Infrastructure Access Management

Rubrik personnel can only access the areas of infrastructure that are associated with their specific job duties. Access is governed through role-based profiles and groups and single sign-on that requires strong passwords and multi-factor authentication. Rubrik also performs periodic validation reviews to confirm that access to the production environment is limited to necessary personnel.

## Secure Software Development

Rubrik's SSDLC spans a multi-step process that focuses on delivery, review, and merge processes to minimize rollbacks, downtime, design flaws, and security incidents. Rubrik's SSDLC relies on industry frameworks such as the OWASP Top 10, SANS Top 20, and CIS Control Benchmarks. The SSDLC steps are:

- **Definition:** During the Definition phase, the Engineering, Product, Information Security, Privacy, and Legal teams finalize content and features for release and review upcoming plans and product requirements.

- **Secure Development:** During the Secure Development stage, designs are documented, tests are planned, static code analysis is performed, and code is reviewed according to secure coding standards. For large projects, testing, development, and validation are ongoing.

- **Security Hardening:** In the Security Hardening stage, feature tests are automated and executed. There is an additional focus on the system, scale, and stress tests, as well as scanning for security findings through vulnerability scanning and penetration testing.

- **General Availability:** In the general availability phase, new features and functionality are made available for customer use.

Rubrik also uses these key principles to build security into Rubrik Security Cloud:

- Hardened microservices with minimized system modeling
- Secure system design with consistent updates and patching
- Continuous integration, end-to-end test automation, and release qualification
- Phased product rollout with continuous customer feedback
- Root Cause Analysis (RCA) process for continuous improvement
- Ongoing scanning and threat detection through extensive use of logging and monitoring

## Encryption

Rubrik Security Cloud uses industry-standard AES-256 for data-at-rest and data in-flight encryption, with per customer data segmentation for critical security information. All Rubrik Security Cloud service configuration data is encrypted using modern cryptography and Google Managed Encryption Keys. Sensitive fields in the database are encrypted using an encryption framework built on top of GCP's Cloud Key Management Service and Cloud IAM. A key management process is in place to facilitate key rotation and revocation.

Rubrik secures all network traffic between customer environments and Rubrik Security Cloud using industry-standard HTTPS/TLS (TLS 1.2+) encryption.

## Network Security

Rubrik uses secure networking principles and industry standard practices to secure the Rubrik Security Cloud network and any communication to and from. This includes:

- Industry standard encryption (TLS 1.2+) for all communication between Rubrik Security Cloud and customer environments, whether accessed via API, the web application, or through integration.
- Web application firewall (WAF)-based edge protection from DDoS, application attacks, and top OWASP risks like cross-site scripting (XSS) and SQL injection (SQLi) attacks.
- Intra-service communications that are scoped and limited to networking required for service interactions.

In addition, customers are able to use an IP allowlist feature to restrict their Rubrik Security Cloud login access to a specific list of IP addresses, address ranges, or subnets.

## Network Segmentation

Rubrik's networks are logically isolated by purpose and function. Access between development and product networks is separated, using access rules and security groups that restrict access to necessary network ranges, ports, protocols, and/or users. This segmentation is a core part of Rubrik's design.

## Customer Network Configurations

Rubrik relies on multiple services to enable Rubrik Security Cloud and Rubrik's Cluster Software to work effectively and enable full functionality. In order to enable full functionality of Rubrik Security Cloud and Cluster Software, outbound network connectivity from a customer's environment to Rubrik Security Cloud services and third-party services used by Rubrik Security Cloud is needed. Customers may limit the connectivity between their on-premises environment and Rubrik Security Cloud via their edge firewall configuration. Specific ports and protocols required for operation can be found in the User Guide.

In addition, the use of integrations that rely on webhooks, such as using Rubrik Security Cloud with Splunk, may require additional port or network configuration changes.

## SERVICE MONITORING AND AVAILABILITY

### Availability

Rubrik maintains a 99.9% service availability commitment for Rubrik Security Cloud and all the cloud-based SaaS services. Components of Rubrik's services that interact with Rubrik Security Cloud, such as Cluster Software, that are maintained in a customer's premises are highly available. In situations like internet connectivity outages, a break-glass mode is automatically triggered that enables local workloads, backups, and restorations managed by Cluster Software to continue working without interruption. Rubrik recognizes how important it is to keep customers informed about Rubrik Security Cloud's availability, scheduled maintenance, and overall reliability. Rubrik provides visibility into the system status at https://status.rubrik.com as well as historical reports of Rubrik Security Cloud system uptime.

### Logging

Rubrik logs Rubrik employee activity and internal system activity within the Rubrik Security Cloud services using a SIEM for monitoring and analysis. All logs are maintained and reviewed for unusual activity and events. If unusual events occur, Rubrik uses a combination of automated SIEM and manual analysis to review and assess events for impact and take action accordingly.

### Incident Management

Rubrik maintains a defined incident response process for identifying, classifying, escalating, communicating, containing, eradicating, and resolving security events identified or reported to Rubrik for the Rubrik Security Cloud service. Rubrik's incident response process includes an escalation plan based on the nature and severity of the incident and a post-mortem exercise to prevent similar incidents in the future. The incident response plan is tested on an annual basis and corrective action plans are created, as warranted.

Rubrik does not monitor events or incidents in a customer's environment and when using Rubrik Security Cloud, customers are responsible for monitoring their use of the Rubrik Security Cloud services for any incidents or issues.

### Vulnerability and Threat Management

Rubrik employs security tooling to continuously and dynamically scan Rubrik products and related infrastructure against common security vulnerabilities. Rubrik maintains a dedicated, in-house product security team to continuously test and drive remediation of any discovered issues based on internally defined service level agreements (SLAs). Rubrik Security Cloud source code is scanned regularly to detect security issues.

In addition to Rubrik's internal vulnerability management and security testing program, Rubrik employs independent, third-party security experts to perform penetration tests at least annually and prior to new, major product releases.

### PHYSICAL SECURITY

Rubrik relies on third-party cloud service providers, including Google Cloud Platform, Microsoft Azure, and Amazon Web Services, for physical security and management of the facilities used in providing Rubrik Security Cloud. Key aspects of GCP's, Azure's, and AWS's physical security measures include:

- 24×7 physical security
- Secure perimeters
- Security cameras and video surveillance
- Strict access policies
- Biometric authentication

Google Cloud Platform, Microsoft Azure, and Amazon Web Services are regularly assessed by independent auditors as part of security certifications such as the SOC 2. For more information about the physical security measures implemented, please visit the Google Cloud Platform, Microsoft Azure, and Amazon Web Services websites.

## CHAPTER 4: DATA COLLECTION AND SECURITY

DATA COLLECTION

SECURE HOSTING

LOGICAL DATA SEPARATION

DATA DURABILITY

SUBPROCESSORS

### DATA COLLECTION

#### Service Configuration Data

Rubrik Security Cloud works seamlessly with the Rubrik Cluster Software and cloud-native functionality to enable advanced data resilience, data observability, and data remediation capabilities that let customers secure and manage their backup data according to custom, customer-configured policies. Based on how customers configure Rubrik Security Cloud to protect their data and systems, Rubrik collects service configuration data to enable critical functionality. Examples include:

| Data Category | Description | Example |
|---|---|---|
| Service Configuration Data | Data input into Rubrik Security Cloud by customers and/or required for Rubrik Security Cloud to protect and manage customer data based on customer-defined SLAs | • Cluster names, location, and capacity<br>• Machine-legible data such as object names (fileset, name, etc.), host names, IP addresses, and unique identifiers (UUIDs)<br>• SLAs, snapshot size and time<br>• Audit and event log stream<br>• Cloud account IDs, names, instances, regions, paths and other details related to the data managed |

### Performance Metrics

Rubrik collects product performance metrics to measure and improve service performance and features when customers use Rubrik Security Cloud as well as Rubrik Cluster Software. To realize the full benefits of all the features and functions provided by Rubrik Security Cloud and Cluster Software, Cluster Software is configured by default to collect:

| Data Category | Description | Example |
|---|---|---|
| Report and Log Bundles | Reports and log bundles contain system logs and system events to assist with troubleshooting. | • Rubrik Backup Agent host logs<br>• IPMI events log<br>• Contents of /var/log |
| Service Operations Information, Stats, and Error Logs | Numeric stats with an attached timestamp. These are used to monitor general system and application health. | • Rubrik OS version<br>• Cluster Software information (UUID, ARP table, file system size and utilization, network routing, uptime reporting, memory and CPU usage, filesystem mounts, RAID/md devices, etc.)<br>• Cloud data management operations success and failure, system logs, etc. |

### Managed Services

Rubrik also offers highly available managed storage services—Rubrik Cloud Vault and Microsoft 365 Protection—that enable customers to seamlessly and securely store backups without having to worry about managing storage accounts. Customers have the ability to choose from a variety of regions for redundancy or data locality reasons. For more information about Rubrik Cloud Vault or Microsoft 365 Protection, including information about the security practices related to those services and in what regions data can be stored, please contact Rubrik through your account team or at inquiries@rubrik.com.

2

### SECURE HOSTING

Rubrik Security Cloud currently has multiple regional deployments on GCP in North America, Europe, and Asia. Rubrik's publicly accessible Status Portal provides visibility into the operational status of the Rubrik Security Cloud service within each region. Customers can sign up to be notified of updates to the status portal, including announcements related to scheduled maintenance.

3

### LOGICAL DATA SEPARATION

Rubrik built Rubrik Security Cloud with logical data separation as a core feature and capability. Rubrik logically separates customer data within Rubrik Security Cloud's internal infrastructure to ensure that each customer only has access to their own account and information.

4

### DATA DURABILITY

Rubrik Security Cloud is built on top of Google Cloud Platform's secure cloud services, which provide industry-leading data security and durability. Through GCP, customer data stored in Rubrik Security Cloud is protected by GCP's highly durable storage services.

5

### SUBPROCESSORS

Rubrik works with leading service third-party providers to support the operations and delivery of Rubrik Security Cloud. More information about Rubrik's sub-processors is available at www.rubrik.com/en/legal/rubrik-subprocessors, where customers can subscribe to receive updates.

## CHAPTER 5: SECURITY AND COMPLIANCE ASSESSMENTS

Rubrik continually improves the security of Rubrik Security Cloud based on the evolving threat landscape. We implement security controls aligned to security standards and frameworks including ISO 27001, the AICPA Trust Services Criteria, and the NIST Cybersecurity Framework.

In addition, Rubrik Security Cloud is regularly assessed through independent third-party security and compliance assessments. The assessments of Rubrik Security Cloud include checking for adherence to security and privacy standards, such as SOC 2 Type 2, SOC 3, ISO 27001, ISO 27017, and ISO 27018. For the latest information about the current security and compliance assessments that are performed for Rubrik Security Cloud, please visit www.rubrik.com/compliance-program.

## CONCLUSION

Rubrik is committed to securing the world's data. When you secure your data with Rubrik, your data is protected by strong security standards, SSDLC, ongoing security logging, and monitoring, and the use of industry-standard encryption. With security as a fundamental part of Rubrik Security Cloud, your data is logically isolated and protected so you can keep your data secure, monitor data risk, and quickly recover your data, wherever it lives.

To learn more about the latest developments with Rubrik Security Cloud, visit www.rubrik.com or contact us at inquiries@rubrik.com

**Global HQ**
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
**www.rubrik.com**

Rubrik is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.

wp-rubrik-security-cloud-architecture-and-security-implementation / 20230917