rubrik

TECHNICAL WHITE PAPER

Rubrik Security Cloud – Government

Architecture and Security Implementation

Table of Contents

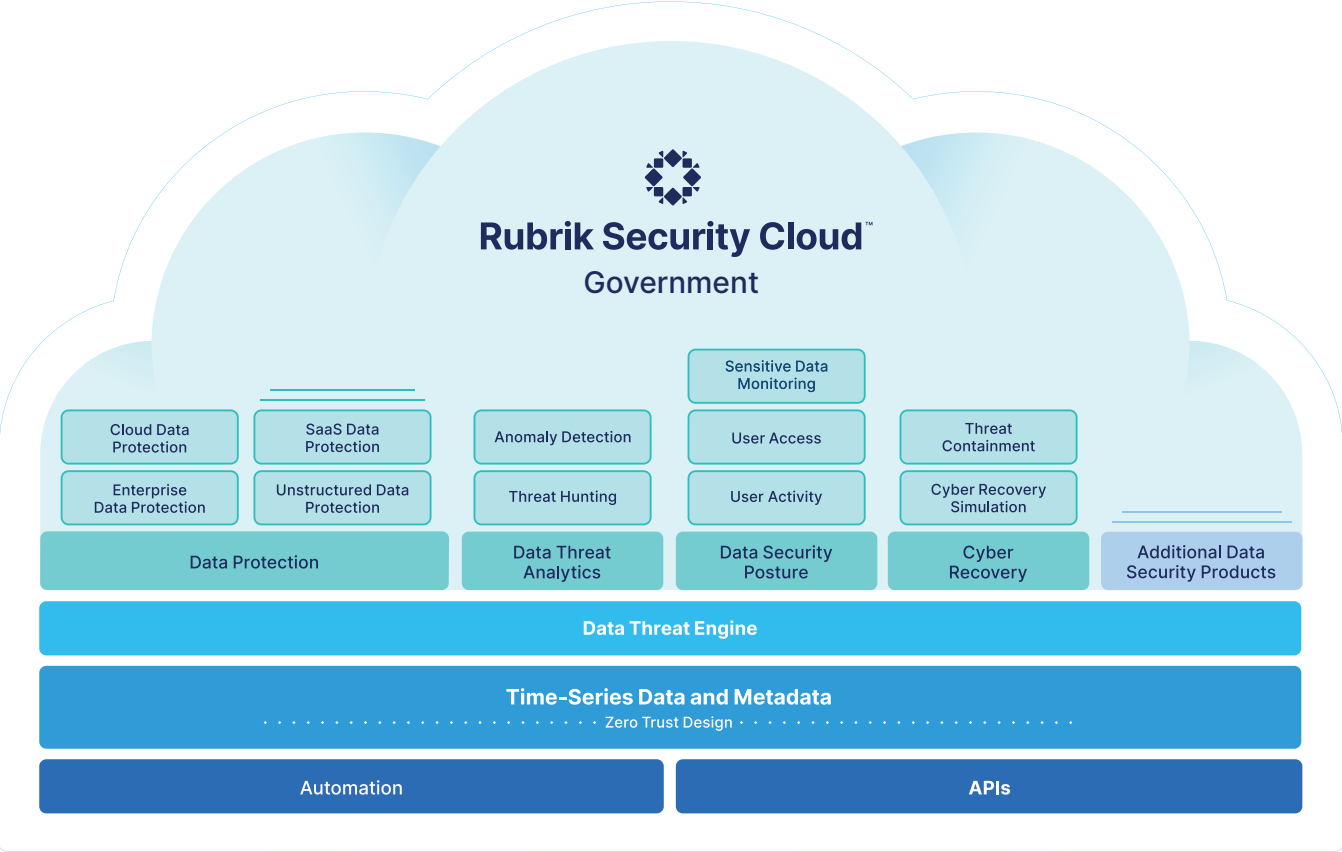
EXECUTIVE SUMMARY

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 – Government, 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 – Government, including infrastructure, encryption, where data is stored, and how the data is kept immutable and available.

CHAPTER 1 | INTRODUCTION TO RUBRIK SECURITY CLOUD – GOVERNMENT

Rubrik Security Cloud – Government 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.



AUTHORIZATION FOR US GOVERNMENT

Attestation
Received

Attestation
Received

Moderate
Authorized
(incl. **TX-RAMP** Level 2)

Moderate
Authorized

These programs require Rubrik to successfully complete and pass an audit of approximately 324 security controls. Rubrik utilizes the FedRAMP Moderate controls to maintain its StateRAMP authorization. Rubrik leverages the authorizations of its partners such as AWS for Government, Google Cloud Platform (GCP) Assured Workloads, and Azure for Government.

BUILT FOR US GOVERNMENT ENTITIES

- Dedicated instance for federal, state, and local agencies and contractors
- Rigorous security monitoring and remediation
- FIPS 140-2 end-to-end encryption of data at rest and in transit
- Secure processing of data within the U.S.
- 24×7×365 support by qualified U.S. citizens located on U.S. soil

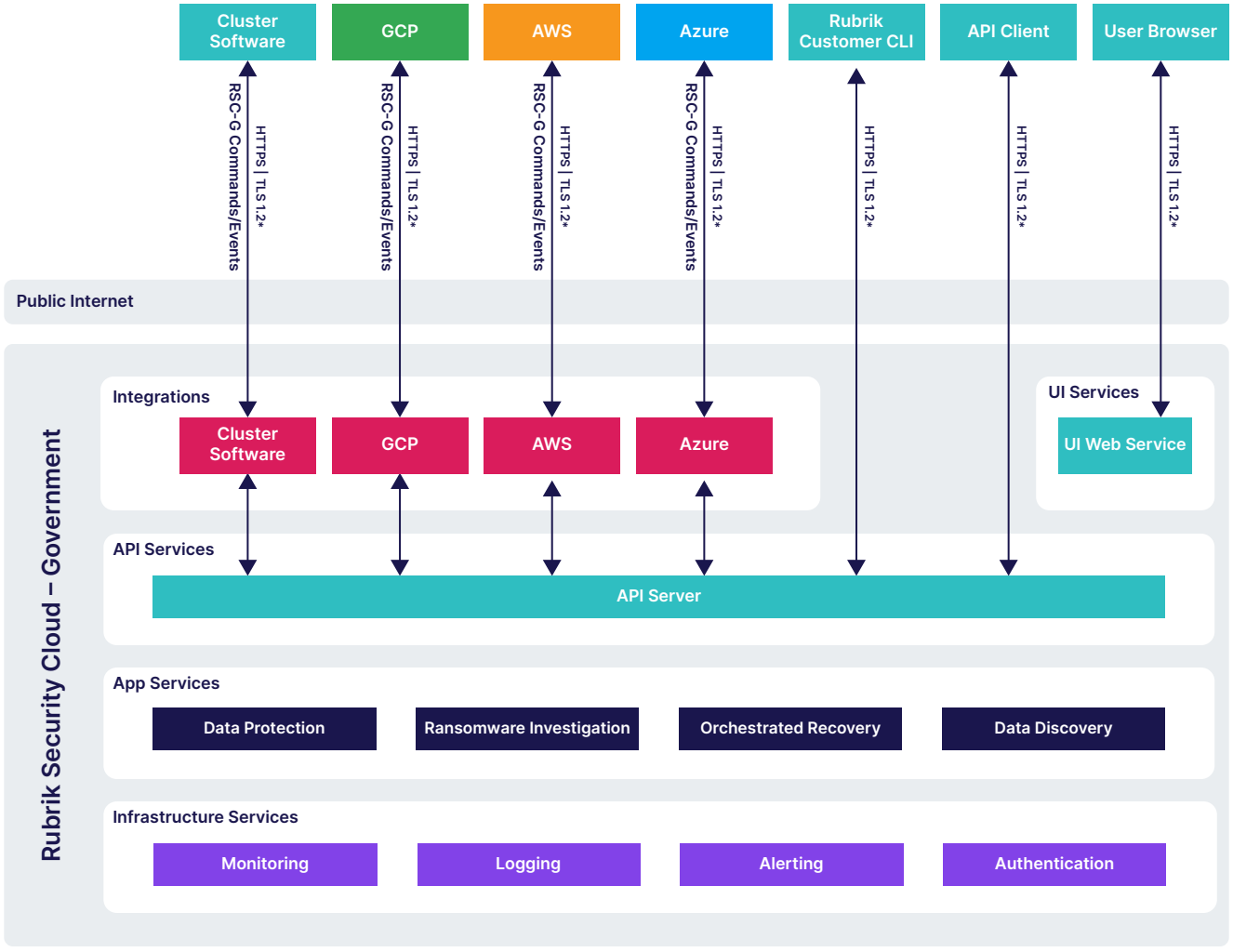
RSC-G implements comprehensive security control baselines engineered to safeguard sensitive US government information. This ensures compliance with stringent federal regulations and exceeds industry best practices.

To further enhance security and resilience, RSC-G is hosted across FedRAMP High and JAB-authorized Infrastructure-as-a-Service (IaaS) platforms. The system utilizes both primary and disaster recovery regions, located within the continental United States. This architecture ensures data sovereignty, high availability, and rapid disaster recovery capabilities, providing unparalleled protection for government data throughout its lifecycle.

CHAPTER 2 | ARCHITECTURE DESIGN

RSC-G is built upon a secure, microservices-based architecture that utilizes high-availability services and infrastructure. It is delivered and integrated across three premier FedRAMP High, JAB-authorized IaaS platforms: Google Cloud Platform, Microsoft Azure Government, and Amazon AWS GovCloud. These top-tier hosting clouds ensure the highest levels of security and compliance. By leveraging these services, Rubrik can:

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



ACCESS MANAGEMENT | PLATFORM SECURITY | SERVICE MONITORING AND AVAILABILITY | PHYSICAL SECURITY

ACCESS MANAGEMENT

RSC-G 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.

From a human resources standpoint, our internal staff who develop and operate the RSC-G platform undergo rigorous personnel security controls, which include employing US Citizens on US Soil. Our measures also encompass comprehensive background checks, specialized role-based training, and ongoing security and privacy awareness education. These initiatives underscore our commitment to maintaining the highest standards of security and privacy within our organization on behalf of our customers.

AAA Framework

Rubrik's approach to security incorporates the AAA framework (Authentication, Authorization, and Accounting). All the access to RSC-G 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 RSC-G accounts via role-based access controls.

Authentication

USER ACCOUNTS | API/SERVICE ACCOUNTS | SINGLE-SIGN ON (SSO) | MULTI-FACTOR AUTHENTICATION (MFA)

USER ACCOUNTS

RSC-G 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 RSC-G accounts, RSC-G 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)

RSC-G supports single sign-on (SSO) using the Security Assertion Markup Language (SAML) 2.0 standard. SSO allows customers to log into RSC-G 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)

RSC-G requires multi-factor authentication (MFA) for native accounts and Rubrik Secure Vaults 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 RSC-G.

Authorization

RSC-G 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.

Auditing and Logging

RSC-G aggregates logs from all connected Rubrik Secure Vaults, so customers can easily monitor changes across all Rubrik Secure Vault software deployments.

RSC-G 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.

PLATFORM SECURITY

Infrastructure Access Management

Rubrik personnel can only access the areas of infrastructure that are associated with their specific job duties. Access is restricted to US-citizen personnel only and requires FIPS 140-2 compliant VPNs with multi-factor authentication (MFA). Access is governed through role-based profiles and groups to enforce least privileges. Single sign-on is also employed, requiring 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 RSC-G:

- 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

3PAO ATTESTATION OF COMPLIANCE

Rubrik has achieved an Attestation of Compliance with the Cybersecurity and Infrastructure Security Agency (CISA) Secure Software Development Requirements, as outlined in the White House Executive Order 14028 on Improving the Nation's Cybersecurity. This Attestation affirms RSC-G's adherence to secure software development practices.

Rubrik's Secure Software Development Life Cycle (SSDLC) leverages industry-standard frameworks, including the OWASP Top 10, SANS Top 20, and CIS Control Benchmarks. The SSDLC focuses on delivery, review, and merge processes to minimize rollbacks, downtime, design flaws, and security incidents.

The Attestation confirms that Rubrik development environments are secured, multi-factor authentication (MFA) is enforced, sensitive data is encrypted, and automated tools are deployed to manage vulnerabilities. This ensures the maintenance of a trusted source code supply chain.

Encryption

RSC-G uses industry-standard AES-256 (or better) encryption for both data at-rest and in-flight, providing per-customer data segmentation for enhanced security. All customer data and metadata are securely stored in dedicated cloud-native storage devices, encrypted at rest with FIPS 140-2 cryptographic modules.

All RSC-G 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 RSC-G using industry-standard HTTPS/TLS (TLS 1.2+) encryption.

All encryption must utilize FIPS-140-2 or greater cryptography. Refer to the NIST FIPS-140 validation program.

Network Security

Rubrik uses secure networking principles and industry standard practices to secure the RSC-G network and any communication to and from. This includes

- Industry standard encryption (TLS 1.2+) for all communication between RSC-G 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.
- Stateful firewall services implicitly deny unless explicitly allowed.

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

Network Segmentation

Rubrik's networks are logically isolated by their purpose and function. This separation ensures that access between development, pre-production, and production networks is rigorously controlled through network segmentation, creating isolated environments.

The pre-production environment is a specialized in-boundary platform designed to closely resemble the RSC-G (RSC-G) production environment. It provides an ideal space for testing hotfixes and addressing customer support issues that require detailed engineering analysis.

To maintain security, no customer data is permitted in the pre-production environment. Fixes tested here must pass strict change control and pipeline release procedures before being moved to production, ensuring high quality and reliability.

This structured segmentation is a fundamental part of Rubrik's design, underscoring our commitment to secure and efficient network management.

Customer Network Configurations

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

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

SERVICE MONITORING AND AVAILABILITY

Availability

Rubrik commits to a 99.9% service availability for RSC-G and all the cloud-based SaaS services. Components of Rubrik's services that interact with RSC-G, such as Rubrik Secure Vault, 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 Rubrik Secure Vault to continue working without interruption. Rubrik recognizes how important it is to keep customers informed about RSC-G'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 RSC-G system uptime.

Logging

Rubrik logs Rubrik employee activity and internal system activity within the RSC-G service. To accomplish this, Rubrik has implemented comprehensive monitoring and analysis of employee and internal system activity through a Security Information and Event Management (SIEM) system coupled with Security Orchestration and Automation (SOAR). This ensures that all logs are maintained and reviewed for unusual activity and events. In case of any anomalies, Rubrik uses a combination of cloud native logging and monitoring services, automated SIEM, SOAR, and manual analysis to quickly and effectively assess and address potential impacts.

Additionally, RSC-G custom services and components are configured to generate audit logs throughout the System Development Life Cycle. These configurations adhere to stringent Security Technical Implementation Guides (STIG), Center for Internet Security (CIS) Level 2 Benchmarks, and vendor-recommended best practices.

By aligning with these standards, Rubrik ensures that all RSC-G managed components meet and exceed minimum audit logging requirements, establishing a strong foundation of security and compliance that supports government and industry baselines.

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 RSC-G 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 RSC-G, customers are responsible for monitoring their use of the RSC-G services for any incidents or issues.

Vulnerability and Threat Management

Rubrik maintains a dedicated, US-based product security team to continuously test and drive remediation of any discovered issues based on internally defined service level agreements (SLAs). Furthermore, FedRAMP requires a remediation timeline for discovered vulnerabilities based on their severity.

RSC-G source code is scanned regularly to detect security issues. Rubrik must report compliance on a monthly basis to both the sponsor and the FedRAMP PMO, based on continuous monitoring requirements. Additionally, independent, third-party security experts perform penetration tests at least annually and before product releases. This comprehensive approach ensures Rubrik not only adheres to FedRAMP standards but also maintains a robust internal vulnerability management and security testing program.

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 RSC-G. 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.

DATA COLLECTION

Service Configuration Data

RSC-G works seamlessly with Rubrik Secure Vault 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 RSC-G 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 RSC-G by customers and/or required for RSC-G to protect and manage customer data based on customer-defined SLAs	• Rubrik Secure Vault names, location, and capacity • Machine-legible data such as object names (fileset, name, etc.), host names, IP addresses, and unique identifiers (UUIDs) • SLAs, snapshot size and time • Audit and event log stream • 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 RSC-G as well as Rubrik Secure Vault. To realize the full benefits of all the features and functions provided by RSC-G and Rubrik Secure Vault, the 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 • IPMI events log • 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 • Rubrik Secure Vault information (UUID, ARP table, file system size and utilization, network routing, uptime reporting, memory and CPU usage, filesystem mounts, RAID/md devices, etc.) • Cloud data management operations success and failure, system logs, etc.

Customer Files and Backups

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.

SECURE HOSTING

RSC-G currently has multi-cloud, multi-region deployments on GCP across North America. Rubrik's publicly accessible Status Portal provides visibility into the operational status of the RSC-G service. Customers can sign up to be notified of updates to the status portal, including announcements related to scheduled maintenance.

LOGICAL DATA SEPARATION

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

DATA DURABILITY

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

SUBPROCESSORS

Rubrik works with leading service third-party providers to support the operations and delivery of RSC-G. 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 RSC-G based on the evolving threat landscape. We implement security controls aligned to security standards and frameworks including FISMA, FedRAMP, StateRAMP, CMMC (DoD Cyber Maturity Model Certification), CJIS (Criminal Justice Information Services), FERPA (Family Education Rights and Privacy Act), and the NIST Cybersecurity Framework.

OUR MULTI-LAYERED APPROACH INCLUDES:

- Continuous monitoring of critical security controls
- Annual comprehensive security assessments
- Twice-annual Incident Response Tests
- Annual Contingency Plan Tests, Penetration Tests, and Red Team Exercises

At least annually, RSC-G undergoes independent third party testing of implemented security and privacy controls to verify adherence to FedRAMP and relevant NIST standards.

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 RSC-G, 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 RSC-G, visit www.rubrik.com or contact us at inquiries@rubrik.com. For those who need specific details about the system's implemented FedRAMP controls or customer responsibility for FedRAMP controls, contact us at fedramp@rubrik.com.

rubrik

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

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

wp-rsc-government-architecture-and-security-implementation / 20241011