INFORMATION AND PRODUCT SECURITY

Cloud Data Management (CDM) Data Sheet

TABLE OF CONTENTS

1. CLOUD DATA MANAGEMENT (CDM) OVERVIEW

CDM is a single software fabric that manages all data in the cloud, at the edge or on-premises, for many use cases including backup, disaster recovery, archival, compliance, analytics, and copy data management. CDM is offered as software, or in combination (i.e. one can install it as a virtual appliance) with a hardware appliance and is installed and hosted at customer locations; therefore, managing and securing the deployment is the responsibility of the customer.

2. SECURE THE PLATFORM/APPLICATION

2.1. SECURITY OVERVIEW & ARCHITECTURE

Rubrik offers a comprehensive approach to security regardless of where data is located. To help facilitate the privacy and safety of enterprises' data, Rubrik deploys a multi-layered security framework that consists of the following components:

- **Data at rest encryption:** If enabled, Rubrik supports encryption of all data at rest to protect against physical breaches and this feature is offered for enablement during cluster bootstrap. With data at rest encryption, data is still secure even if a drive is stolen from a data center. Rubrik also offers both software (FIPS 140-2 Compliant AES-256) and hardware (FIPS 140-2 Level 2 HDD and SSD) encryption if the customer chooses to opt for it.
- **Data in-flight encryption:** The Rubik platform provides in-flight encryption leveraging TLS 1.2 with a SHA512 hash. Rubrik leverages client-side encryption libraries supported by public cloud providers and all archived data undergoes envelope encryption.
- **Flexible key management:** Rubrik offers the flexibility to manage keys with an internal key manager via the Trusted Platform Module (TPM) chip, or an external key manager via Key Management Interoperability Protocol. In both cases, Rubrik adopts security best practices by allowing users to easily perform a one-time key rotation. Rubrik key management also enables secure cluster erasure to provide government agencies and other entities with added security.
- **User authentication:** Rubrik reduces the risk of data breaches and cyber-attacks by assigning granular permissions for data access. The Rubrik platform integrates with Active Directory (AD) and supports granting authorization and groups from AD. With support for SAML 2.0, users can also securely access the cluster with single sign-on from their SAML 2.0 compatible IdP (Identify Provider). This enables users to access multiple applications with a single set of credentials without the interoperability issues associated with vendor-specific designs. Rubrik clusters use role-based access control (RBAC) to define the capabilities of authenticated users, and also to employ multi-factor authentication and API tokens for added layers of security.
- **Data integrity:** Rubrik provides data immutability against cyber-attacks such as ransomware. No external or internal operation can mutate the data since the underlying backups are read-only.
- **Centralized compliance reporting:** All user activity in the Rubrik platform is logged and made available to administrators through the Rubrik User Interface (UI) and Application programming interface (APIs). The activity logs centralize compliance reporting for system operations such as backup and recovery.
- **Data center security:** Rubrik hosts internal engineering and product development servers at a co-location service provider with state-of-the-art physical security measures. The co-location provider maintains high SLAs for availability, redundancy, and disaster recovery to support our business continuity plans. Rubrik uses 3rd party SaaS services and co-location data service providers to manage our IT operations. Our HR systems, email and calendaring, internal communications and requirements, and ticketing management systems use best-of-breed SaaS services. These services offer a very high SLA for availability, reliability, and security.
- **On-site security:** On-site security at our core sites (including HQ) includes a number of features such as security guards, badging, cameras, fencing, security feeds, intrusion detection technology, and other security measures.

2.2. AVAILABILITY & CONTINUITY

UPTIME

Rubrik is currently working on a publicly available system-status webpage for the SaaS product that includes system availability details, scheduled maintenance, service incident history, and relevant security events.

BUSINESS CONTINUITY AND DISASTER RECOVERY

Rubrik's business continuity and disaster recovery program is designed to address the risks when Rubrik services are unavailable. Business continuity and disaster recovery plans are reviewed annually and are periodically tested through tabletop tests, functional tests, or actual incidents.

MONITORING

Stats, log excerpts, and log bundles are used by our alerting system to generate internal Support and Engineering alerts to deliver proactive, context-aware support for Rubrik services. Diagnostic system data is securely transmitted to Rubrik, to determine the health of a cluster. Rubrik support teams monitor and analyze the data to proactively identify issues before they surface and monitor infrastructure health.

3. DATA MANAGEMENT

3.1. CDM PARTNERS

Rubrik works with multiple third parties to support our CDM product. Information about our sub-processors can be found at https://www.rubrik.com/en/legal/rubrik-subprocessors.

3.2. METADATA DEFINITION AND SECURITY LIFECYCLE

Rubrik collects "phoning home" type data from our clusters and nodes in order to provide our support and engineering teams with data that can be proactively used to detect possible system issues and improve the overall quality of our product. This data is sent to Rubrik in the form of both numeric statistics and logs. Metadata collected includes attributes such as Rubrik CDM cluster information (e.g., cluster health statistics, Excerpts of logs, log bundles etc.).

Overall, this data is used by our alerting system to generate internal support and engineering alerts to deliver proactive, context-aware support for Rubrik services. Diagnostic system data is securely transmitted to Rubrik to determine the health of a cluster. Rubrik support teams monitor and analyze the data to proactively identify issues to ensure that infrastructure health is not at risk.

For U.S. Federal and GDPR customers, generating a support bundle and downloading it locally is still the best solution. The downside with this approach is that it is time consuming and is dependent on customer availability. The support team may not be able to readily capture detailed system data, thus prolonging issue resolution times.

The benefits of enabling proactive support are as follows:

- With more frequent access to stats and logs, Rubrik support can speedily resolve any technical issues.
- Rubrik support teams can look into issues without waiting for direct access to CDM.
- With cluster configuration data being proactively captured, Rubrik support can identify and dispatch replacement parts expeditiously.

4. SECURE SDLC PRACTICES

Rubrik engineers follow secure code practices that span OWASP top ten security risks, common attack vectors, and Rubrik security controls. Rubrik leverages secure open-source frameworks with security controls to limit exposure to OWASP top ten security risks. These inherent controls reduce our product exposure to SQL injection (SQLi), cross-site scripting (XSS), and cross site request forgery (CSRF), among others.

Rubrik uses the following principles to guide the SDLC process:

- Quality in every step of the engineering process.
- Security by design, not as an afterthought.
- Continuous integration and release qualification.
- End-to-end test automation for velocity and repeatability.
- Phased product rollout with continuous customer feedback.
- Root Cause Analysis (RCA) process for continuous improvement.

Rubrik follows the release process outlined below when creating a new product:

1. **Definition:** In the definition phase, content and features are finalized for release. The engineering, product management, and support teams review and commit to requirements.
2. **Development:** During this stage, documentation is designed, tests are planned, and code is reviewed according to secure coding standards. For large projects, testing development and validation are ongoing.
3. **Hardening:** At this stage, features tests are automated and executed. There is an additional focus on system, scale, and stress tests, as well as scanning for security findings.
4. **General availability:** In the general availability phase, new features and functionality is made available for customer use.

5. VULNERABILITY MANAGEMENT

5.1. VULNERABILITY SCANNING

Rubrik employs security tooling to continuously and dynamically scan our 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). The source code repositories for our platform are also scanned for security issues.

5.2. THIRD-PARTY PENETRATION TESTING

In addition to our internal vulnerability management and security testing program, Rubrik employs independent third-party security experts to perform penetration tests prior to general availability (GA) of our major product releases.

6. ENCRYPTION/KEY MANAGEMENT

Rubrik CDM unifies backup, instant recovery, replication, and data archival in one scale-out platform. CDM enables easy and secure management of physical or virtualized data on-premises, at the edge, and in the cloud. Rubrik adds encryption at rest while maintaining web-scale performance and speed.

Rubrik's encryption offering is comprehensive, securing data in a cost-effective manner for all security conscious industries including government, financial, legal, and healthcare sectors. Many industries require compliance with rigid data protection policies in order to protect their classified, confidential, or personally identifiable information (PII). With Rubrik CDM, customers can ensure their data is protected even in the event of physical theft or a breach.

R528: FIPS 140-22 LEVEL 2 SELF-ENCRYPTING DRIVES

For hardware encrypted clusters, Rubrik encrypts user and application data at rest with FIPS 140-2 Level 2 certified self-encrypting drives (SED) as its HDDs and SSDs. Self-encrypting drives provide the additional functionality of automatic data protection without additional intervention. The data at rest encryption solution is turnkey, and all SEDs ship completely configured.

In order to boot up or power cycle, Rubrik retrieves the cryptographic keys protecting its SEDs via its TPMs. These keys are then used to unlock and mount the drives. Furthermore, these security keys can be used to instantly and securely delete data on a SED. Rubrik's encryption at-rest and in-flight helps safeguard your sensitive data in support of regulatory compliance.

SOFTWARE-BASED DATA AT REST ENCRYPTION

Rubrik's file system is protected with AES-256 encryption. Key management is done internally, providing an additional layer of security and enabling secure cluster erasure. Rubrik also supports detection of data tampering even when the system is powered off. Lastly, our software-based encryption solution is designed for scale to meet the needs of high data growth.

7. ACCESS MANAGEMENT

Access to Rubrik's production environment is restricted on an explicit need-to-know basis, utilizes least privilege, and is frequently audited and monitored. When employees are terminated or have changed job roles, there is a process in place to either remove or change/revoke their access and assets. Further, there is a process in place to review user access quarterly.

Authorization: CDM has multiple fine-grained privileges (additional details for privilege management can be found in the CDM user guide). CDM supports token based authentication policies via multi-factor authentication (MFA).

Remote access to CDM is only allowed whenever the customer requires Rubrik support to troubleshoot issues. Rubrik support personnel cannot access customer environments without explicit access enabled by the customer and once enabled, Rubrik support personnel access the environment via one of Rubrik's products, Support Tunnel. The default inactivity timeout is 4 days by default. The Rubrik cluster can be configured to disable the Support Tunnel automatically after a set period of inactivity. For more detail on this, refer section 12 Support Tunnel.

Authentication Options: CDM v5.1 and above support short message service (SMS or text), hardware tokens, software tokens via RSA, and password SAML/OAUTH/SSO. Prior to CDM v5.1, Rubrik supports passwords natively. SMS, hardware token, and software tokens are supported via RSA. Integration with Active Directory (AD) is available.

Hash Algorithm: For CDM, salted one-way hashes store passwords and other authentication credentials. All passwords are hashed using a one-way hash function (SHA256) with a 16-character salt, which means once passwords are hashed and written on disk, they are secure and no longer readable.

Password Management: CDM requires the password length to be a minimum of 8 characters. CDM v5.1 allows customers to configure both password length and password character composition (i.e., types of characters). Passwords are controlled by the customer. CDM can also be integrated with the customer's identity provider for password policy enforcement.

Account Lockout: On CDM v5.1 and above, authentication lockout can be configured by the customer. Prior versions do not support this feature. CDM v5.1 and above allows customers to configure lockout parameters. Further, administrators can reset passwords on CDM. CDM does not support authentication restriction to customer's IP addresses, although this can be configured by the customer by using their network security features. CDM does not currently prevent concurrent logins.

8. AUDITING (LOGGING AND MONITORING)

Rubrik activity log messages describe the current state of tasks on the local Rubrik cluster and furnish information about every task that was started on the local Rubrik cluster over the past 90 days, including tasks that result in a notification. User events are logged in the Rubrik activity log, along with all other cluster activities. A set of user activities can be reconstructed by filtering the activity log to display user events.

The Rubrik cluster supports transmission of system activities to an external syslog server. When syslog support is enabled, the Rubrik cluster sends messages to the syslog server that are based on the events that also appear in the Rubrik activity Log.

It is recommended that customers send logging information to a remote syslog server. By doing so, customers can correlate and audit security events across clusters effectively.

9. INCIDENT RESPONSE

Rubrik's Security Incident Response Team (SIRT) is responsible for responding to security incidents. They manage the receipt, investigation, public reporting and remediation of information about security vulnerabilities and issues related to our products and networks.

Reporting an incident or obtaining security support:
If customers identify a security issue or have a security concern related to Rubrik's products or services, contact Rubrik Support at support@rubrik.com.

Process:
Rubrik SIRT follows the following process for vulnerability management.

1. **Awareness:** SIRT receives notification of security incident.
2. **Active Management:** SIRT prioritizes and identifies resources.
3. **Determination of a fix:** SIRT coordinates fix and impact assessment.
4. **Mitigation plan:** SIRT engages experts and executives to mitigate the issue, and Customer Support to plan notifications to customers. If applicable, appropriate contacts with relevant authorities shall be maintained.
5. **Communications:** SIRT/Customer Support send out notifications to affected customers.
6. **Postmortem:** SIRT writes a postmortem on the issue.

10. POLICIES AND PROCEDURES

Rubrik has developed a set of security policies covering a broad range of topics relevant to Rubrik's operating environment. In addition to requiring users to acknowledge understanding of these policies through mandated annual training, they are made available on our intranet to all employees and contractors with access to Rubrik information assets.

11. TRAINING AND AWARENESS

All employees and contingent workers are required to complete privacy and security awareness training upon hire, and annually thereafter. Rubrik's security team also attends bi-monthly seminars to get trained on updates to products and related security topics. Additionally, Rubrik conducts regular phishing campaigns across the company and have an executive-sponsored campaign called #notonmywatch to actively instill good security behaviors and a strong security culture across Rubrik.

12. SUPPORT TUNNEL

The Rubrik cluster provides a built-in tunnel utility to permit authorized Rubrik support and engineering personnel to make a secure remote connection to the Rubrik cluster when access is enabled by the customer. The support tunnel functionality is enabled upon explicit authorization by the customer. Rubrik support uses the tunnel to examine the health of the Rubrik cluster and to troubleshoot and resolve issues.

12.1. SECURITY OVERVIEW & ARCHITECTURE

The MySQL database that stores the (encrypted) credentials is hosted by Amazon's relational database service (RDS). The database has a specific backup procedure. If the database itself is compromised, an attacker would see only the encrypted or strongly hashed and salted credentials.

For effective privilege separation, the generation of credentials occurs on a separate Security Operations VM that has restricted access to the Rubrik IT and the Rubrik Security teams. It is also backed up using the Rubrik IT Cluster. Administrative access to the VMs involved occurs via a separate username, and authorized users have their public keys added to authorized keys. No other accounts are granted administrative privileges.

All encryption keys used for the Support Tunnel are protected by HSM softcards, which require a passphrase. These passphrases are stored in encrypted form on the associated VMs, and the decryption key for these passphrases is stored on a physically present Yubikey assigned to each VM (by the ESX host). This protects the passphrase in case a Rubrik backup of the VM is accessed. In case the decryption keys and passphrases are lost, all encryption keys can be recovered using a quorum of the HSM Administrator Card Set (ACS).

12.2. ACCESS TO CUSTOMER ENVIRONMENT

Each node has a distinct SSH private key and password installed at the time of manufacture. The private key only exists in RDS, and the corresponding public key is added to the node's file for a new support user.

Access to the support tunnel is controlled using Rubrik's single sign-on (SSO). Thus an employee requesting access is added to the right group, and is automatically granted permissions on the servers. After logging onto the Support Portal, employees may access a customer node by running a script that accepts a Support Tunnel port number, looks up the private key of the corresponding customer node, and initiates an SSH connection to that cluster through the Support Tunnel (EC2). The script also logs the name of the user, the time of access, and the cluster UUID/node ID that was accessed.

When a customer opens a support tunnel, the Rubrik node creates a reverse SSH port forwarded to the Support Tunnel relay instance in EC2. This SSH traffic travels over a chisel layer, which uses an HTTPS Web Socket connection to route traffic over port 443. This layer is needed to traverse many customer firewalls, which permit egress traffic only on port 443. Traffic from Rubrik nodes first travels through the proxy.rubrik.com Elastic Load Balancer in EC2, and then to one of several Chisel instances. From there, Chisel forwards the SSH traffic to its ultimate destination: The Support Tunnel Relay instance.

By default, after manually enabling the Support Tunnel, The default inactivity timeout is 4 days. The Rubrik cluster can be configured to disable the Support Tunnel automatically after a set period of inactivity.

Rubrik CDM software can be upgraded via a support tunnel (the only recommendation is to not have Live Mounted restores running during the upgrade). Alternatively, customers can use the command-line interface (CLI) to download and upgrade Rubrik clusters on their end. This process does not require customers to enable support tunnel functionality.

12.3. AUDITING (LOGGING AND 24/7 MONITORING)

All systems are configured to export logs to an external logging server where they are monitored using automated alerts.

13. REFERENCE DOCUMENTS

- Rubrik CDM User Guide

14. REVISION HISTORY

Date	Version	Created By	Change Description
September 01, 2020	2020.01	Information Security team	

rubrik

Global HQ
1001 Page Mill Rd., Building 2
Palo Alto, CA 94304
United States

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

20200915_v1