Zero Trust Data Security™ Best Practices

Rubrik Zero Trust Data Security solutions protect data from cyber attacks and enable organizations to recover their applications and minimize business downtime. To ensure the best possible protection of data and to maintain eligibility for Rubrik's Ransomware Recovery Warranty, customers must adhere to the Data Security Best Practices in this document, as well as deployment requirements set forth in Rubrik's Security Hardening Best Practices Guide.

This document provides an overview of Rubrik Data Security Best Practices, and is divided into five areas:


DATA HEALTH


USER ACCESS


DATA ENCRYPTION


APPLICATION ACCESS


API SECURITY

DATA HEALTH

1. **Backups Meet SLA Policies –** Your backups are the last line of defense against a cyber attack, and so it is vital that you are able to meet not only your recovery point objective (RPO), but also that you can hit your Recovery Time Objectives (RTO). As an example, the fact that you can recover to a point in time which sees you lose only seconds of data might mean nothing if it takes months to verify exactly when your systems were compromised, and then restore your systems to that point in time.

   Rubrik SLA policies must be properly defined and applied against target workloads and datasets. Once policies are in place, regular monitoring must verify the completion of data backups. This monitoring is critical, as backup failures can result from an application, infrastructure, or services outages, performance bottlenecks, or other factors—directly impacting recoverability from an attack.

   Alerts must also be configured and monitored through Rubrik or other systems integrated with Rubrik.

2. **Enable SLA Retention Lock –** Retention Lock ensures that data retention settings within an SLA policy cannot be reduced or removed. For example, a ransomware attacker might attempt to change the retention period from three years to just one day, which would cause the system to remove any data older than 24 hours. This malicious action would prevent any data older than 24 hours from being restored. To ensure recoverability, Retention Lock must be enabled for all workloads.

   Enabling Retention Lock requires contacting Rubrik Customer Support and designating at least two trusted employees to authorize retention modifications on SLA Domains with Retention Lock enabled. Both employees are needed to authorize the change, which Rubrik Customer Support can then implement. (Note: that lengthening the retention period does not require authorization)

3. **Consider Data Lifecycle –** While Rubrik provides immutability of data, this is no longer the case once data is moved to archive. Bear this in mind when selecting your archive platform. Both Microsoft Azure (Azure Immutable Blob) and AWS (S3 Object Lock) have options to extend this immutability out to archives, and have integration points for Rubrik. Rubrik also offers Rubrik Cloud Vault as a managed service with an immutability option, offering even greater protection by virtue of being stored in a different Azure AD tenant.

USER ACCESS

1. **Multi-factor authentication for all user accounts –** Multi-factor authentication (MFA) is key to preventing an attacker with compromised credentials from getting access to Rubrik. Rubrik offers both a native, time-based one-time password (TOTP) solution, as well as integration with third-party authentication providers through SAML 2.0. A Rubrik Administrator will be prompted on login to enable this TOTP integration to safeguard access to the Rubrik web and command-line interfaces. MFA for all users (local, LDAP, & SSO) must be configured as a best practice.

2. **SSH key-based with passphrase-protected keys for CLI authentication –** The Rubrik Command-line interface (CLI) is an alternative way to manage the Rubrik system outside the web-based graphical user interface (GUI). The CLI can be used to automate tasks or to have a minimalist approach to administration. Nonetheless, the Rubrik CLI is just as powerful as the GUI and, therefore, steps must be taken to secure this access.

   Using SSH keys to authenticate provides better security than a basic username and password, which an adversary could sniff in a man-in-the-middle (MITM) attack. The SSH keys must be protected using passphrases to ensure that a rogue actor cannot simply steal those keys and use them to infiltrate the system. SSH with key-based authentication can be enforced by the Admin user in Rubrik 6.0.1 onwards.

3. **User roles are assigned with least privilege access –** Rubrik provides fine-grained role-based access control (RBAC). Administrators can assign the least privilege level that a user needs to perform their role. Rubrik ships with RBAC role templates and allows custom role templates to be created to meet your business needs. This limits exposure were a rogue actor to gain access to the system.

   Users must have roles that are defined with the least privilege, in line with the CISA[1] definition. For example, an application owner should be able to assign one of their component databases to an SLA domain. Still, they must not be able to overwrite files in a VM for which they are not responsible from an old snapshot.

DATA ENCRYPTION

1. **Data-at-rest and data-in-transit are always encrypted –** Rubrik clusters have the option to use software-based encryption or self-encrypting disks for data-at-rest. One of these options must be enabled to ensure that data within the system is safe and encrypted. Data must also be encrypted during transmission via TLS certificates. Rubrik supports the import and export of TLS certificates signed by a Certificate Signing Request (CSR) or a key phrase, as well as wildcard certificates. Encrypting data-in-transit ensures that data cannot be copied or stolen during transmission.

1 https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege

2. **Secure protocols for third-party systems –** Rubrik has powerful integrations with many other platforms. Those integrations must communicate with Rubrik only via secure channels such as HTTPS, SSH, or API. Where applicable, signed TLS certificates must be used.

APPLICATION ACCESS

1. **Create IP allow lists that limit connections to customer-owned networks –** Rubrik allows customers to restrict which IP networks can access the Rubrik SaaS interface. This ensures that users and devices outside the customer's environment cannot log in to the Rubrik instance. Only specific trusted networks must be populated in the allow list. Access to Rubrik must be restricted using a protected management network, limiting access only to those authorized to manage the environment.

2. **SSL-certificate security for User Interface (UI) and APIs –** As mentioned earlier, Rubrik supports TLS certificates to secure access to the system. Signed TLS certificates must be used to secure web-based interfaces over HTTPS to protect against attacks.

API SECURITY

1. **Secure service accounts –** Rubrik allows for creating and managing service accounts to represent services and client applications that need to invoke Rubrik APIs. Using service accounts eliminates the need to rely on user accounts to access the Rubrik APIs and reduces the lateral movement capabilities of an attacker. Service accounts must be used for automation tools and integrations that only require API access, and each different application or use case must have a unique account.

2. **Scoped API roles with least privilege –** Much like User roles, access via Rubrik APIs must be scoped to grant access only as necessary and implemented in the least privileged manner. In this way, risks are minimized if a role were to be compromised, either directly or via a software supply chain attack.

ADDITIONAL RESOURCES

Additional information and the latest guidance can be found in the Security Hardening Best Practices Technical White Paper. Visit rubrik.com/warranty to learn more about the Rubrik Ransomware Recovery Warranty.

rubrik

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

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

brf-ztds-best-practices / 20230913