rubrik

WHITE PAPER

Rubrik Cloud Vault for Microsoft Azure: Technical Deepdive

Brian Mislavsky
October 2025
RWP-0625

Table of Contents

INTRODUCTION

The purpose of this document is to help readers familiarize themselves with the concepts, features, and architecture essential for effectively using Rubrik Cloud Vault on Microsoft Azure.

AUDIENCE

This guide is for anyone seeking a deeper technical understanding of Rubrik Cloud Vault's capabilities on Microsoft Azure. This includes architects, engineers, and administrators responsible for cloud infrastructure, data protection operations, as well as individuals with a vested interest in the security, compliance, or governance of data.

OBJECTIVES

After reading this document, the reader should be able to answer the following questions regarding Rubrik Cloud Vault:

- *What is Rubrik Cloud Vault?*
- *What problem(s) does Rubrik Cloud Vault solve?*
- *How is Rubrik Cloud Vault architected (and why)?*
- *How does Rubrik Cloud Vault protect against Ransomware and assist with Incident Response?*

CHALLENGES

The New Perimeter

Organizations leverage secondary data centers or public cloud storage to maintain off-site copies of their data, which can be used as part of their business continuity planning. While useful in the event of scenarios such as a natural disaster, cybersecurity events such as a Ransomware attack require additional levels of protection.

While customer data may be stored off-site, administrative and security controls for the data remain the customer's responsibility. This means that the customer not only has to manage storage off-site for enhanced security, they also have to manage the security and operational processes and tooling needed to operate and secure it. For some organizations, this could mean upskilling staff to support public cloud, acquiring additional software licenses, and integrating their existing Identity Provider for authentication.

In the event of a cybersecurity incident, the blast radius should no longer be considered or limited to a physical data center. It should include any other locations—whether physical, virtual, or cloud-based—that fall under the customer's administrative control.

For example, in the event of a compromise of an identity provider or an administrative user, data stored off-site may either no longer be considered safe or may even be modified or deleted by a malicious actor, making it unreliable for cyber resilience.

Figure 1 - The New Perimeter

Cloud Cost Management
The actual cost of leveraging cloud storage extends beyond just calculating the utility-based pricing of consumed resources. It's essential to also consider additional soft costs, such as the training and upskilling of staff, licensing fees for third-party security tools, and the need for extra monitoring and operational processes related to integration.[1]

Moreover, budget planning can be complex for organizations due to the rapid deployment and consumption of cloud resources.

THE RUBRIK APPROACH: RUBRIK CLOUD VAULT

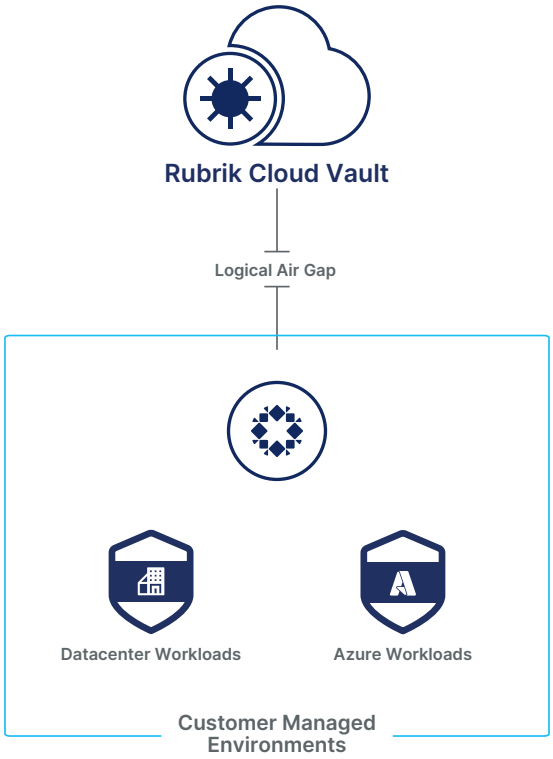


Figure 2 - Rubrik Cloud Vault

Rubrik Cloud Vault (RCV) is a fully managed cloud service that enables customers to securely store isolated copies of their data, enhancing their cyber resilience posture and helping them achieve regulatory compliance. This off-site layer of protection features air-gapped, isolated, and immutable data copies, which help customers safeguard their on-premises and cloud environments against threats and ensure they meet regulatory requirements.

KEY FEATURES

The key features of Rubrik Cloud Vault include:

- Logically Air Gapped
- Unified Data Management with Rubrik Security Cloud
- Zero Trust Data Security
- Fully Managed Service
- Predictable Cost

1. https://www.gartner.com/en/documents/3982411

Logically Air Gapped
Rubrik Cloud Vault protects data by ensuring a copy is logically air gapped from the source environment. This ensures that a clean copy of data is always available, even in the event of account and identity compromise.

Unified Data Management with Rubrik Security Cloud
Single Point of Management and Automation via Rubrik Security Cloud – Rubrik Cloud Vault is configured and managed using Rubrik Security Cloud - Rubrik's SaaS management platform, enabling a unified user experience.

Zero Trust Data Security
- **Architecture** – Zero Trust Architecture ensures that data is available, immutable, and logically air-gapped, making it impossible for ransomware to modify, encrypt, or delete it
- **RBAC** – Fine-Grained Role-Based Control following the concept of least privilege permissions, giving users access to only what they require, thereby decreasing the risk of bad actors or compromised accounts accessing things they shouldn't
- **Retention Lock** – Retention lock prohibits a person from clearing or shortening retention policies governing archived data
- **Immutability** - Rubrik Cloud Vault stores data immutably, ensuring that data cannot be modified or deleted until it is set to expire

Fully Managed Service
Simplified onboarding of cloud resources – As a fully managed service, Rubrik Cloud Vault reduces operational complexity, time to delivery, and the staff upskilling required to operate cloud storage for secure data protection.

Predictable Cost
Unified billing - Rubrik Cloud Vault is offered at a fixed price that covers direct cloud storage costs, including storage capacity, API interactions, and egress charges. Additionally, indirect costs such as security, staffing, and operations are included in the price, helping organizations stay within budget by making budget planning a simple task.

HIGH-LEVEL ARCHITECTURE

This section provides a high-level overview of how Rubrik Cloud Vault protects various workloads. The configuration of Rubrik Products is outside the scope of this document. For the most up-to-date step-by-step instructions, please refer to the *Rubrik Security Cloud User Guide*.

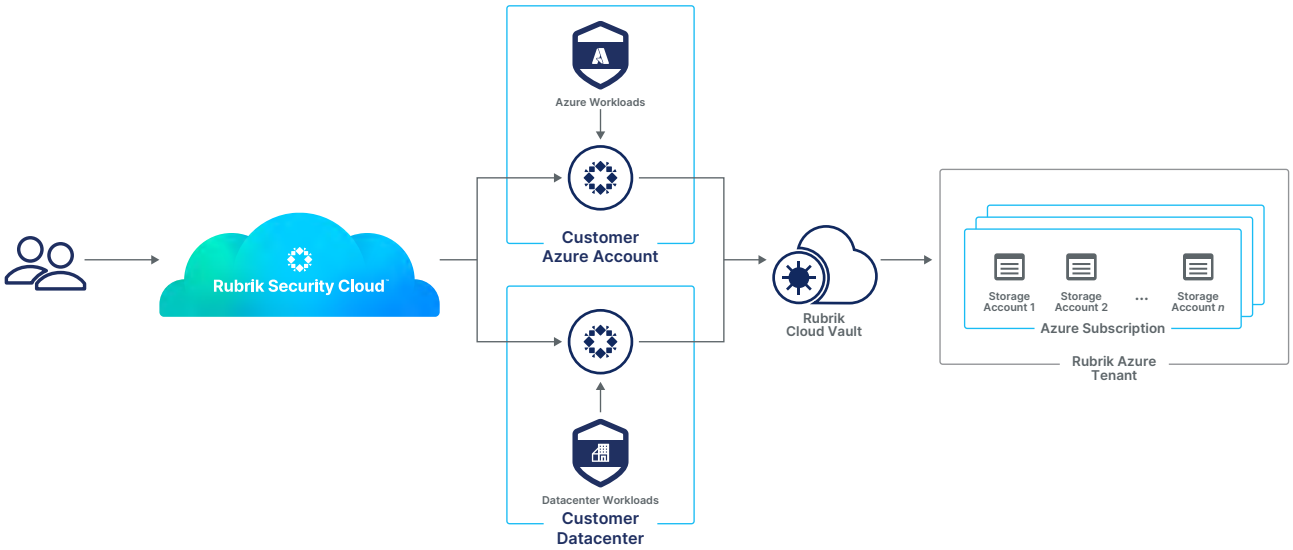


Figure 3 - Rubrik Cloud Vault - High-Level Overview

Customers manage Rubrik Cloud Vault using Rubrik Security Cloud, which serves as its control plane. Data is transmitted to/from Rubrik Cloud Vault by Rubrik's data plane, which can be one or more of the following: Rubrik Secure Vault, NAS Cloud Direct, Rubrik Exocompute.

HOW IT WORKS

This section provides an in-depth explanation of how Rubrik Cloud Vault works. For specific instructions on configuring Rubrik Cloud Vault, customers should refer to the *Rubrik Security Cloud User Guide*.

RESOURCE PROVISIONING

Customer Onboarding

When a customer is onboarded to Rubrik Cloud Vault, a customer-specific Entra ID Service Principal is created in an Entra ID directory managed by Rubrik. This Service Principal is used for controlling a customer's Rubrik Cloud Vault operations.

Location Creation

This section provides details on the backend provisioning process that takes place when a customer creates a Rubrik Cloud Vault location. For the most up-to-date steps involved in creating a Rubrik Cloud Vault location for protecting workloads, please refer to the *Rubrik Security Cloud User Guide*.

When a customer provisions a Rubrik Cloud Vault location, the following occurs:

- An Azure Subscription in the Rubrik Azure Tenant is identified for resource placement
- The following resources are provisioned:
  - Resource Group within the identified Subscription
  - An Entra ID Service Principal, with permissions scoped to the Resource Group
  - A Storage Account with a customer-specific 10-character name prefix is created in the Resource Group
  - A Storage Container is created in the Storage Account[2]

RESOURCE ISOLATION

Rubrik Cloud Vault locations are entirely isolated from one another. This isolation also exists between multiple locations belonging to the same customer or Rubrik Data Plane.

Storage Isolation

Rubrik Cloud Vault locations are entirely isolated from one another. Each Rubrik Cloud Vault location consists of a dedicated storage container within a dedicated Azure Storage Account, which is placed within a dedicated Resource Group assigned to the customer. While each Resource Group can only be assigned to a single customer, a customer may have multiple Resource Groups assigned to it when more than one RCV location is provisioned.

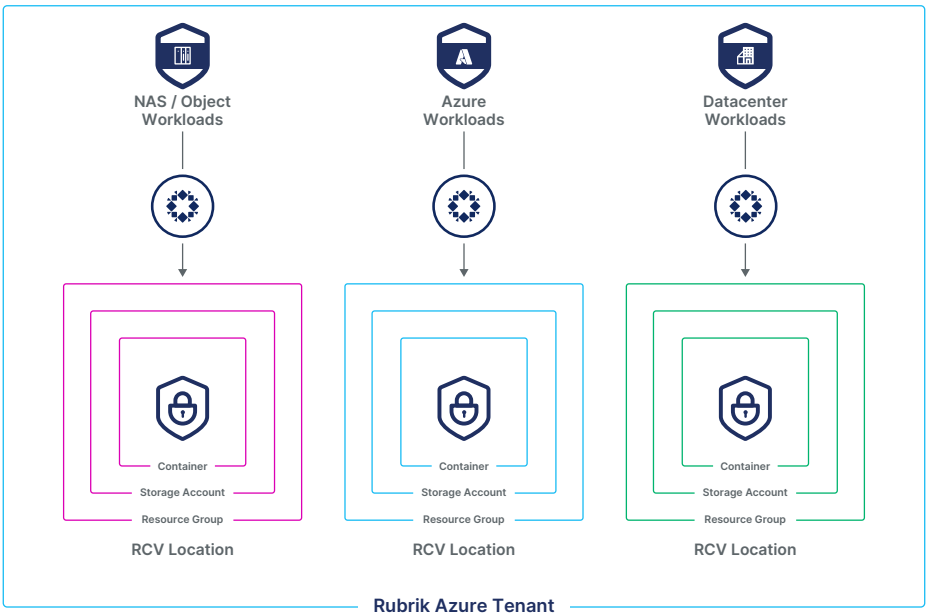


Figure 4 - Rubrik Cloud Vault - Storage Isolation

2. When used with Rubrik Secure Vault or Cloud Cluster, some metadata is automatically uploaded to the location. This metadata is immutable and is governed by the location's retention policy.

Permission Isolation
When a Rubrik Cloud Vault location is provisioned, Rubrik creates a dedicated Entra ID Service Principal as part of the process. This Service Principal exists in the Rubrik-managed Entra ID directory and has permissions scoped specifically to its assigned Resource Group. When interacting with an RCV location, Rubrik uses the Service Principal associated with the location to perform any actions.

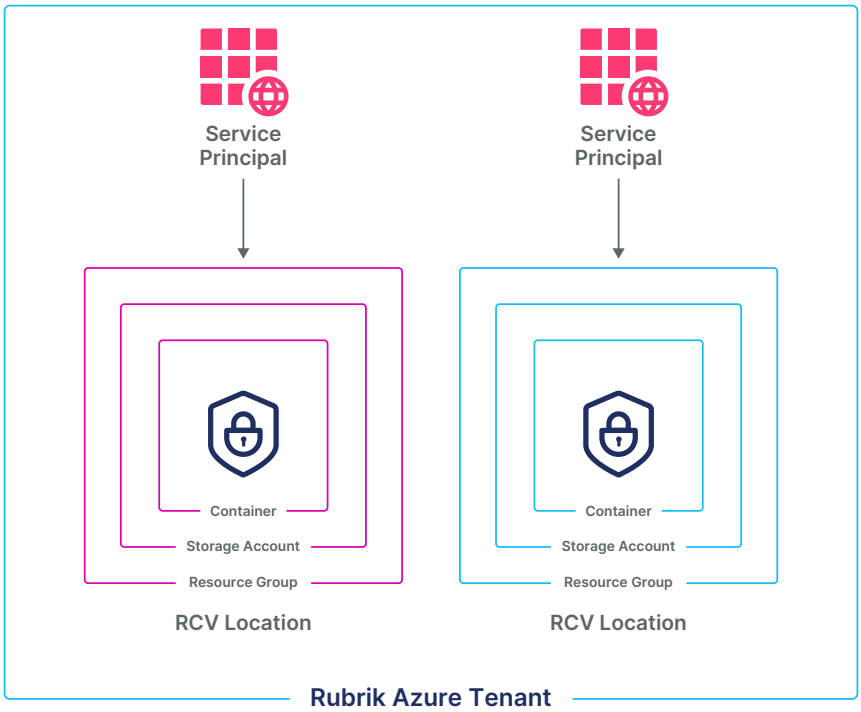


Figure 5 - Rubrik Cloud Vault - Permission Isolation

Additionally, Rubrik restricts access to Rubrik Cloud Vault locations within a customer environment to only the mapped resources. An example of this is as follows:

NETWORK ISOLATION

Rubrik provides various mechanisms for the network isolation of Rubrik Cloud Vault.

Tenant Isolation
Rubrik-managed Azure Tenants are configured to prevent unauthorized external access.

Once configured, only Rubrik Cloud Vault related traffic is allowed between the Rubrik data plane (Rubrik Secure Vault, NAS Cloud Direct, Rubrik Exocompute) and the Azure Storage Service endpoints.

Service Endpoints
When Service Endpoints are enabled in Microsoft Azure, communication between a cloud-based Rubrik data plane (Cloud Cluster, NAS Cloud Direct, Rubrik Exocompute) and Rubrik Cloud Vault stays within the Microsoft Azure backbone.

Private Endpoints
For customers seeking an additional layer of network security, Rubrik supports the use of Azure Private Endpoints, allowing existing Azure connectivity to be leveraged for transferring data to the Rubrik Cloud Vault, rather than relying on public Azure Storage service endpoints. For detailed steps on how to configure Azure Private Endpoints with Rubrik Cloud Vault, please refer to the *Rubrik Security Cloud User Guide*.

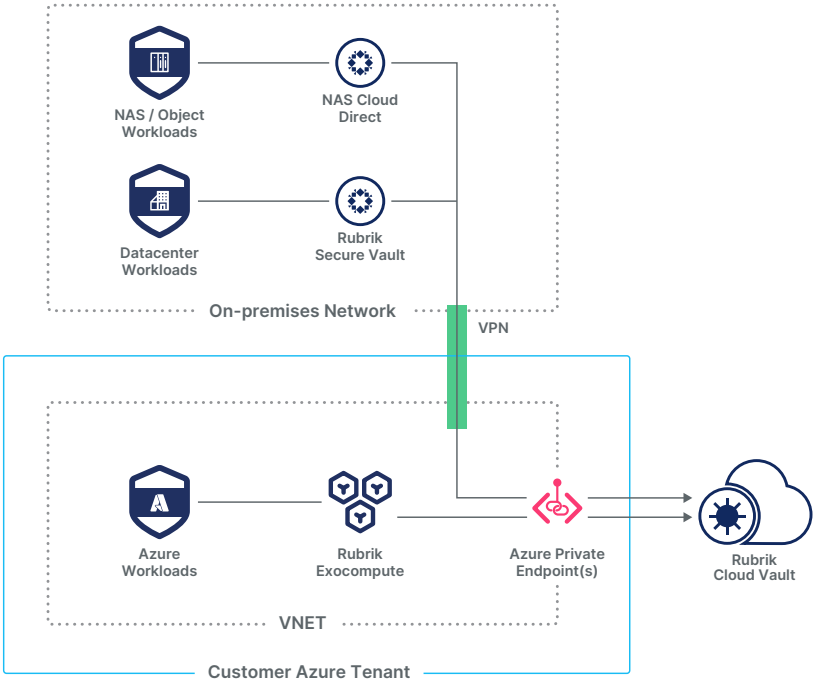


Figure 6: Private connectivity using Azure Private Endpoints

IP Allow Lists
For additional network isolation, customers can further restrict access to their Rubrik Cloud Vault locations by configuring an IP Allow List. When enabled and configured, Rubrik leverages Microsoft Azure APIs to configure the Azure Storage Firewall directly from within Rubrik Security Cloud.

Additionally, for locations created after April 2025, Rubrik provides an endpoint URL with a unique 10-character customer prefix that customers can use to restrict traffic to their Rubrik Cloud Vault locations. The syntax of the customer-specific endpoint is:

<10-character-customer-prefix>.blob.core.windows.net*

QUORUM AUTHORIZATION

Rubrik Cloud Vault locations are further protected against unauthorized actions when Quorum Authorization is enabled in Rubrik Security Cloud. When enabled, specific actions on Rubrik Cloud Vault locations and associated SLAs will require approval from multiple administrators to be performed.

For an up-to-date list of protected actions as well as implementation steps for Quorum Authorization, please refer to the Rubrik Security Cloud User's Guide.

REDUNDANCY & AVAILABILITY

Rubrik Cloud Vault Service Tiers
Rubrik Cloud Vault is offered in two service tiers: Backup Tier & Archive Tier. The Backup tier is built on Microsoft Azure Blob Cool Tier, and the Archive Tier is backed by Microsoft Azure Blob Archive Tier.

The Backup tier is ideal for use cases such as Cyber Resilience, where customers require immediate access to their data, while the Archive tier is better suited for long-term compliance and retention purposes. Because data retrieved from the Microsoft Azure Blob Archive Tier requires a lengthy rehydration time, the Archive Tier is not recommended for use cases requiring low RTOs.

Note:
To prevent early deletion penalties, Rubrik enforces minimum retentions for SLAs configured with Rubrik Cloud Vault as the target archival location.

Redundancy Offerings
Rubrik Cloud Vault Backup Tier is available in three different redundancy levels: Single Zone, Multi-Zone, and Multi-Region. Assuming they are entitled to all three, a Rubrik Cloud Vault customer could leverage various RCV Archival Locations using different combinations of service tiers and redundancy to maximize their Cyber Resilience while minimizing costs.

This section provides a brief description of each offering and explains how Rubrik Cloud Vault uses various Microsoft Azure storage offerings.

For additional information about Microsoft Azure Blob Storage redundancy, please refer to the Microsoft Azure website here.

Single-Zone Redundancy
Rubrik Cloud Vault with Single-Zone redundancy is built on Microsoft Azure Blob Locally redundant storage (LRS). LRS replicates your storage account three times within a single data center in the primary region. LRS provides at least 99.999999999% (11 nines) durability of objects over a given year.[3]

Redundancy Scenario:
If a localized event, such as a hardware failure were to occur within the Microsoft Azure datacenter, data would still be available via the other 2 copies.

Use Case(s):
- High availability/redundancy across multiple locations is not required
- Low cost

Limitation:
If the entire primary location is damaged or destroyed, data could be lost.

Multi-Zone Redundancy
Rubrik Cloud Vault with Multi-Zone Redundancy is built on Microsoft Azure Blob Zone-redundant storage (ZRS). ZRS replicates your storage account synchronously across three Azure availability zones in the primary region. Each availability zone is a separate physical location with independent power, cooling, and networking. ZRS offers durability of at least 99.9999999999% (12 9s) over a given year.[4]

Redundancy Scenario:
If an Azure Availability Zone (or entire data center) became unavailable, data would still be available via the two other Availability Zones.

Use Case(s):
- Applications that require high availability and minimal downtime.

Note:
Microsoft recommends using ZRS in the primary region for scenarios that require high availability.[5]

3. https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#locally-redundant-storage
4. https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#zone-redundant-storage
5. https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#redundancy-in-the-primary-region

Multi-Region Redundancy
Rubrik Cloud Vault with Multi-Region Redundancy is built on Microsoft Azure Geo-redundant storage (GRS). GRS copies your data *synchronously* three times within a single physical location in the primary region using LRS. It then copies your data *asynchronously* to a single physical location in a secondary paired region. GRS offers durability for storage resources of at least 99.99999999999999% (16 9s) over a given year.

A write operation is first committed to the primary location and replicated using LRS. The update is then replicated asynchronously to the paired region. When data is written to the secondary location, it also replicates within that location using LRS.[5]

Redundancy Scenario:
If a catastrophic event were to occur, rendering an entire Microsoft Azure region unavailable, data would be available via its Azure paired region.

Use Case(s):
- Disaster Recovery and business continuity when your data must survive regional outages.

Limitation:
- Additional steps are required for managing GRS backed RCV locations.
- When failed over to the paired region, the RCV Location is only available for recovering data. The RCV location needs to be failed back to the Primary region with GRS Redundancy re-established to resume backup operations.

GRS Failover Process
While this section describes how the GRS Failover & Failback process works, step-by-step instructions can be found in the Rubrik Security Cloud User Guide.

GRS Failover can only be initiated when certain conditions are met to prevent data loss or inconsistency. As mentioned previously, data is copied between primary and secondary regions asynchronously, which could lead to data not always being available in both regions. A safe failover requires that the following criteria be met:

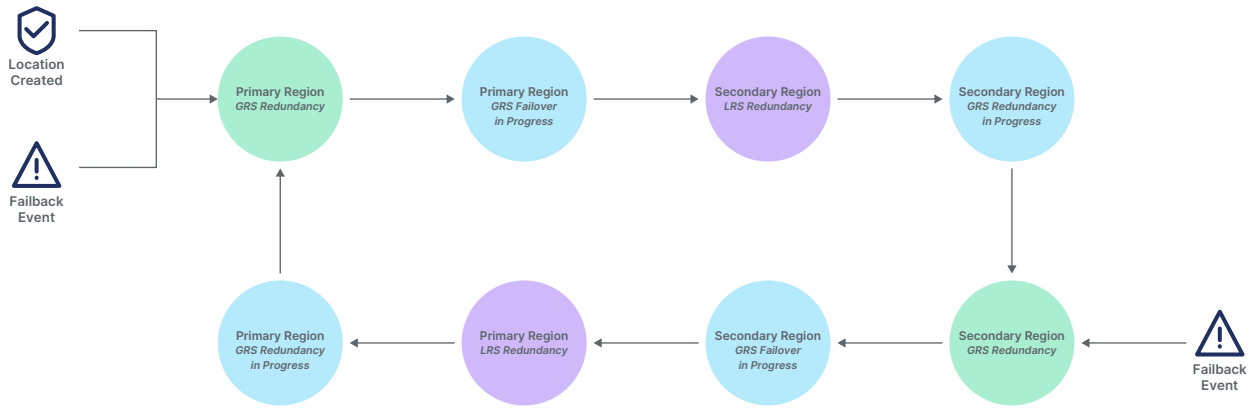
- No ongoing data activity or location state changes: Confirming that no data or state change activity is occurring on the RCV location in the primary region is crucial. This prevents the loss of data that has not been copied to the secondary location when the failover process is initiated
- Last redundancy sync time: Indicating the most recent point at which data is guaranteed to have been replicated, the last sync time helps assess potential data loss during failover. Any new data uploaded to the primary region after the last redundancy sync time is not copied to the secondary region and is lost once a failover begins

Managing Failover State
To manage GRS backed locations, Rubrik Security Cloud queries Microsoft Azure and derives the following information for a GRS RCV Location on an hourly basis to determine its state:
- Current redundancy level (LRS or GRS)
- Is a failover in progress? (True or False)
- Is the location active in its assigned primary region? (True or False)

Rubrik stores the location's state information for use during the failover process.

6. https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy#geo-redundant-storage

To manage the process, Rubrik tracks the status of a GRS backed RCV Location as being in one of several states. If eligible, the periodic job advances the location to the next available state. The criteria for each state is as follows:



State	State Criteria
Primary Region - GRS Redundancy	Current Redundancy = GRS and Primary Region = True
Primary Region - Failover in Progress	Primary Region = True and Failover In Progress = True
Secondary Region - LRS Enabled	Current Redundancy = LRS and Primary Region = False and Establish Geo-Redundancy = fail
Secondary Region - GRS Redundancy in Progress	Primary Region = false and Establish Geo-Redundancy = success
Secondary Region - GRS Redundancy	Current Redundancy = GRS and Primary Region = false
Secondary Region - Failover in Progress	Primary Region = true and Failover In Progress = true
Primary Region - LRS Redundancy	Current Redundancy = LRS and Primary Region = true and Establish Geo-Redundancy = fail
Primary Region - GRS Redundancy in Progress	Primary Region = true And Establish Geo-Redundancy = fail

DATA RESILIENCE

This section outlines the various ways in which customers can leverage Rubrik Cloud Vault to protect their data. Configuration and management steps for Rubrik Solutions are outside the scope of this document. For detailed configuration steps, please refer to the product documentation.

IMMUTABILITY

Data stored in Rubrik Cloud Vault is made immutable by default.

Rubrik uses a *rolling lock window* process that leverages Azure native blob-level versioning. Blob version metadata is tracked to ensure that the correct blob versions are made available when a customer downloads data from an Archival Location.

When snapshot data is uploaded to Rubrik Cloud Vault, Rubrik assigns an immutability lock of 4 weeks. To prevent immutability from expiring and putting data at risk of being tampered with, Rubrik clusters perform a daily background job that periodically extends the immutability lock back to 4 weeks if it is detected to be below a minimum threshold of 3 weeks. This background job continues until a snapshot becomes eligible to expire, per the archival retention defined in its SLA.

If a customer decides to expire a snapshot before its SLA-defined expiration date, the snapshot will be marked for expiration. However, deletion cannot occur until any existing immutability locks have expired, which may take up to 4 weeks.

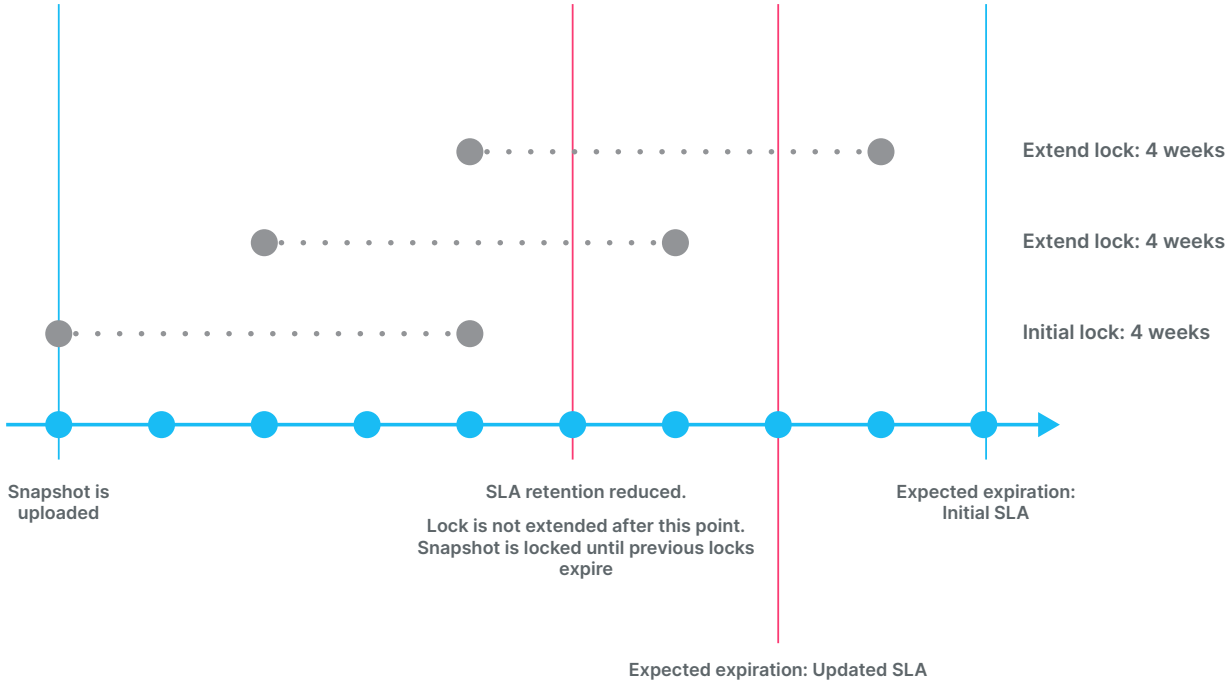


Figure 7: Rolling Lock Window

Should a customer choose to *reduce* the retention of an SLA, Rubrik simply does not extend the immutability policy past the updated retention length. This will result in a snapshot remaining immutable for the duration of time between the new expected snapshot expiration and the most recent lock expiration.

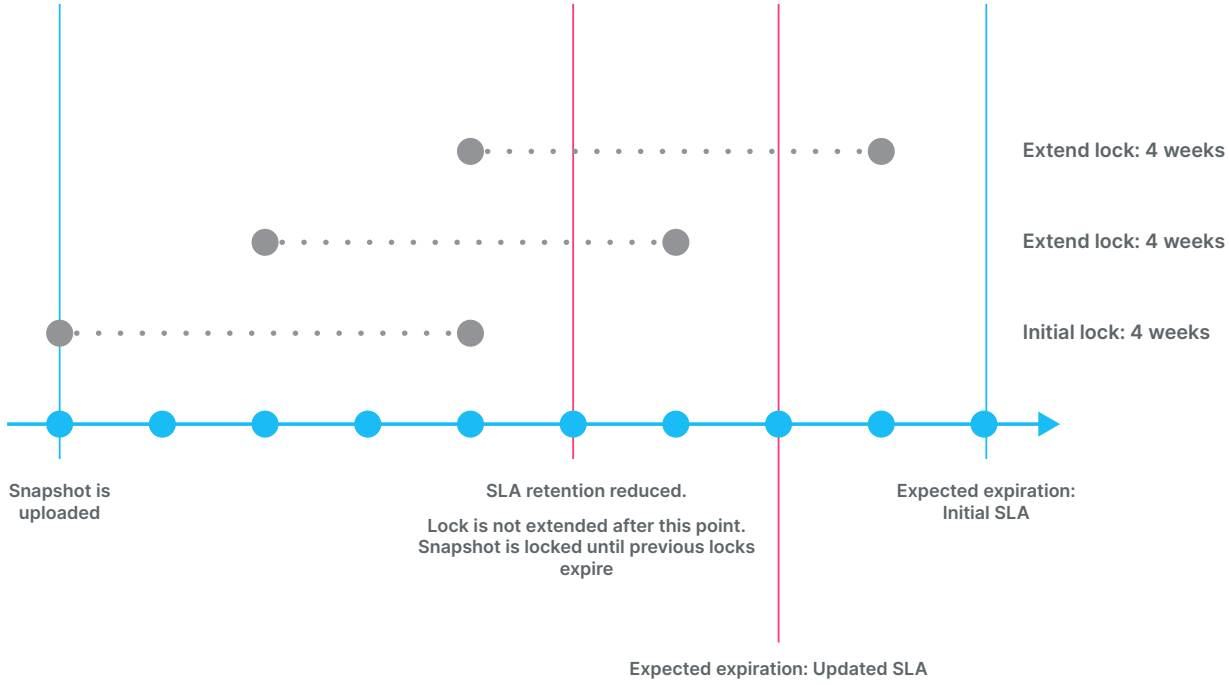


Figure 8: Reducing SLA retention

ENCRYPTION

Data sent to Rubrik Cloud Vault is encrypted in transit and at rest. The type of data-at-rest encryption may differ depending on the Rubrik data plane used.

Rubrik Secure Vault
Rubrik Secure Vault uses client-side encryption to protect data at rest within a Rubrik Cloud Vault location. This means customer data is encrypted before being sent to Rubrik Cloud Vault. This is achieved through a multi-layered key hierarchy that enables critical key management operations, such as rekeying and rotation.

Rubrik Encryption Service
Rubrik Secure Vault uses a Rubrik-native encryption mechanism called the Rubrik Encryption Service. This service allows Rubrik to perform data encryption and decryption (via the Storage Account Manager), as well as manage encryption keys as detailed in the next section.

Key Hierarchy
Instead of using a single encryption key to encrypt data, Rubrik Secure Vault employs a multi-layered key hierarchy, where keys are used to encrypt other keys, thereby creating multiple layers of security.

The key hierarchy is stored in the Rubrik Cloud Vault Archival Location, enabling recovery in disaster recovery scenarios. However, the key hierarchy is not stored in plaintext, since having access to it is equivalent to having access to the data for decryption. Instead, the key hierarchy is wrapped by the master key.

The primary benefit is that the keys used to directly encrypt the data (the Data Encryption Keys (DEKs)) are themselves encrypted. A malicious actor would need to compromise multiple levels of the hierarchy to access the actual data.

The key hierarchy consists of four levels:

- **Master Key (The "Key Vault")**: The highest-level key in the hierarchy. This key is customer-managed and can be either an RSA key or managed by Azure Key Vault. This key's sole purpose is to encrypt and decrypt the Root Key
- **Root Key (Root KEK):** This is the first key in the Rubrik-managed part of the hierarchy. It is wrapped (encrypted) by the customer-provided Master Key. The Root KEK, in turn, wraps the next level of keys
- **Level 2 Key Encryption Keys (KEKs):** These are keys that the Root KEK wraps. They are transparent to the customer and are used to wrap the Data Encryption Keys. Rubrik automatically rotates these keys periodically (every 30 days) for enhanced security
- **Data Encryption Keys (DEKs):** These are the keys that perform the actual encryption of the data blobs in the archive. Each DEK is used to encrypt a specific piece of data and is then wrapped by an Intermediate KEK

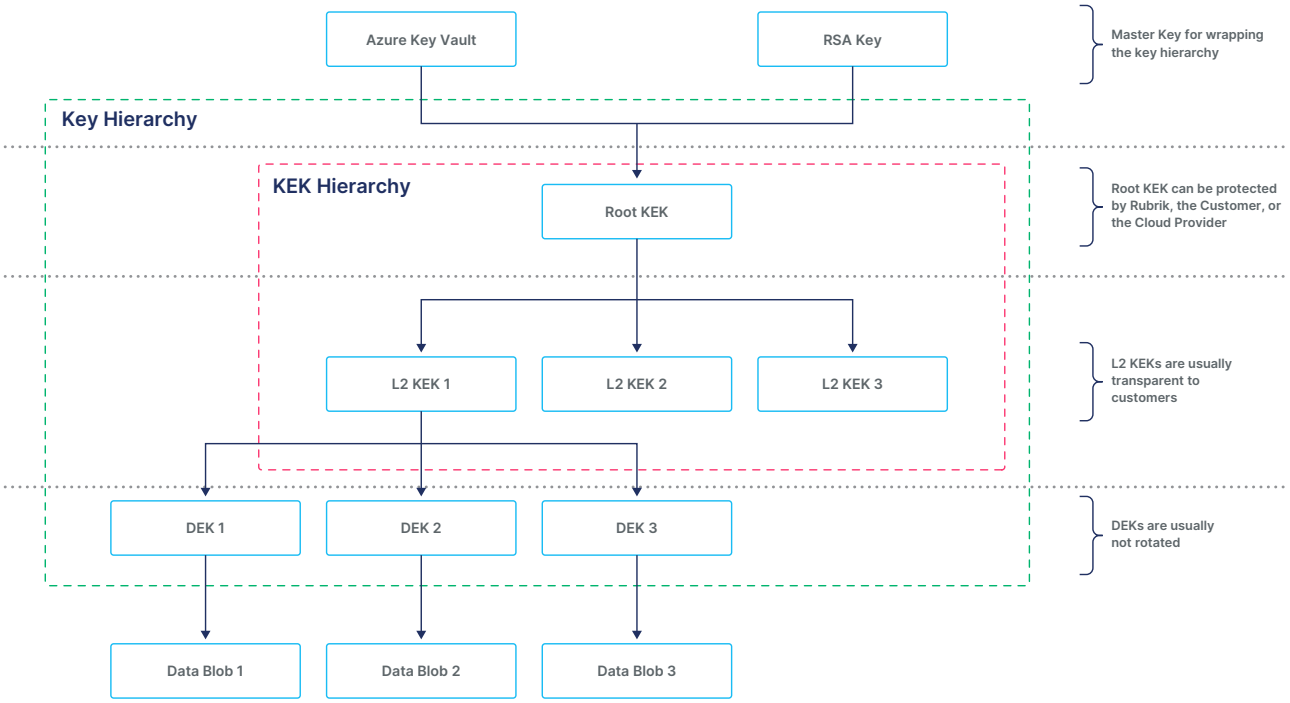


Figure 9: Encryption Key Hierarchy

Uploading Data

When Rubrik Secure Vault writes data to Rubrik Cloud Vault, the process ensures it is securely encrypted before it leaves the customer's environment.

The following describes the process of encrypting and uploading a file to Rubrik Cloud Vault:

- The Archival Storage Handler requests the Rubrik Encryption Service's Storage Account Manager to upload data
- The Storage Account Manager requests that the Rubrik Encryption Service generate a DEK. A randomly generated plaintext DEK and its respective wrapped DEK are returned
- The wrapped DEK is uploaded to the RCV location as a file with a __rnem suffix
- The data is first broken into chunks. Each data chunk is encrypted using the plaintext DEK and the GCM-AES-256 algorithm, then uploaded by the Archival Storage Account Manager

Downloading Data
When Rubrik Secure Vault reads data from Rubrik Cloud Vault for recovery, the process is essentially reversed. The steps are as follows:

- The Archival Storage Handler requests the Rubrik Encryption Service's Storage Account Manager to download the data
- The __rnem file is downloaded and is unwrapped by the Rubrik Encryption Service to get the plaintext DEK
- The data file input stream is converted to a decrypted chunk stream. Each chunk is downloaded, then decrypted using the plaintext DEK and GCM-AES-256 algorithm

Key Rotation & Re-Keying
Rubrik Secure Vault automatically rotates L2 KEKs every 30 days. The new key is used to encrypt DEKs after the rotation. Old/rotated L2 KEKs are retained for unwrapping DEKs they previously wrapped.

To enhance encryption security, customers can manually rekey the master key of a key hierarchy for an RCV location. When re-keying the master key, only the Root KEK needs to be re-encrypted using the new key. DEKs used to encrypt data are not affected by this operation. Additionally, when a rekeyed RCV location is connected as a reader location, its key master key can also be updated to ensure that data can continue to be accessed.

Rubrik Cloud Native Protection & NAS Cloud Direct
When storing data in Rubrik Cloud Vault, Rubrik Cloud Native Protection & NAS Cloud Direct leverage Server Side Encryption (SSE) using Platform Managed keys for encrypting data at rest.

DATA EFFICIENCY FOR CLOUD NATIVE WORKLOADS

Rubrik Cloud Native Protection stores data in Rubrik Cloud Vault using its Optimized Snapshot approach. This approach to snapshot retention offers maximum flexibility and cost-effectiveness for managing large amounts of data.

Instead of storing snapshots as a single "chain", Rubrik stores snapshots at different levels of a hierarchy. This ensures smaller snapshot chains for more efficient recoveries and improved space management.

EXAMPLE SLA

To explain the benefits of Rubrik Optimized Snapshots, the following scenario will be used. For the SLA, assume that a single Rubrik Cloud Vault location is used for the archival location.

Example SLA	
Snapshot Frequency	Retention
Daily	7 Days
Weekly	1 Month
Monthly	1 Year

After six days, the snapshots archived to Rubrik Cloud Vault look like this:

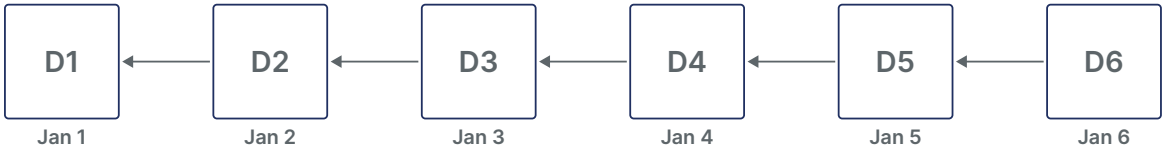


Figure 10 - First week of daily snapshots

The first seven daily snapshots function as a traditional linear snapshot chain. The first daily snapshot, taken on January 1st, is a full snapshot, with subsequent snapshots being incremental.

On January 7th, instead of taking an incremental snapshot over the January 6th snapshot as the first weekly snapshot, a new snapshot level is started, with the weekly snapshot based on the initial full snapshot.

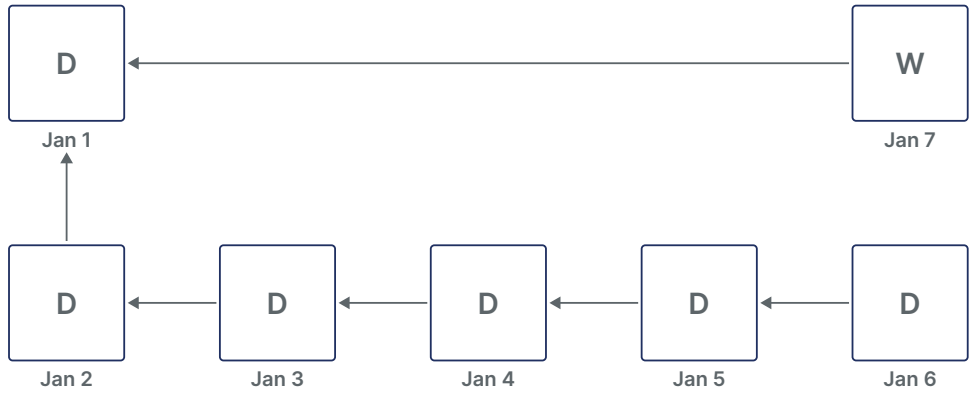


Figure 11 - First weekly snapshot

Once a new snapshot level is started, the previous snapshot chain/lower level is fully expired per the SLA and deleted. Subsequent lower-level snapshots will be based on the higher level.

In our example, the snapshots from January 2nd to 6th have now expired and will be deleted. The new chain of daily snapshots, beginning January 8th, will be based on the January 7th weekly snapshot, and so on. This is illustrated below.

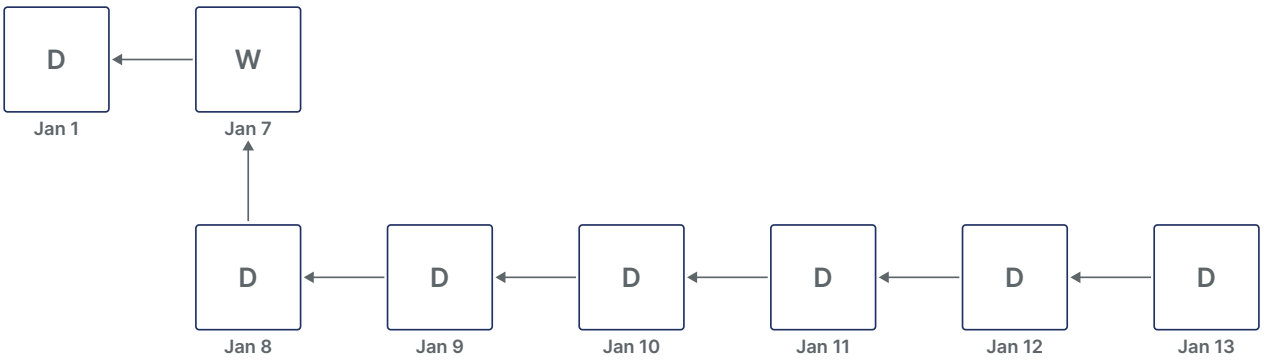
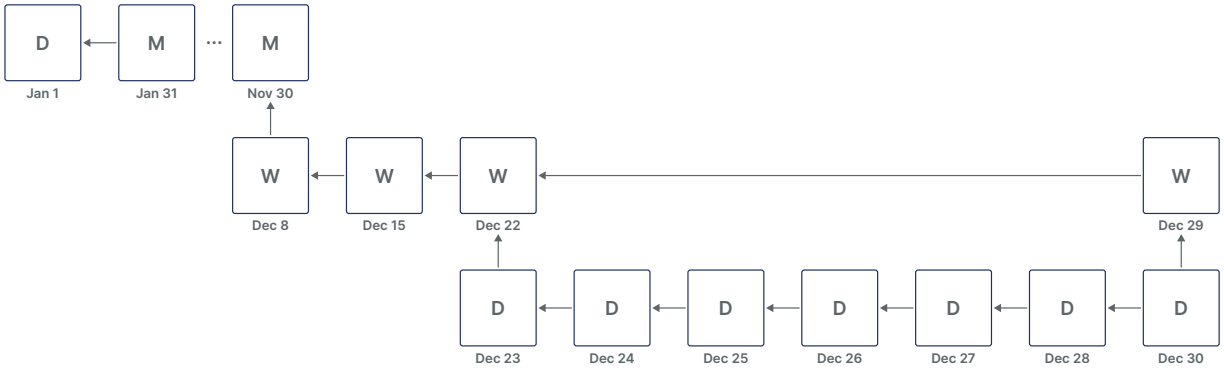


Figure 12 - Starting a new snapshot level

Putting this all together, according to the SLA defined in our example, a year's worth of snapshots will resemble a hierarchical tree, with various branches formed from a base snapshot.



SUMMARY

This concludes Technical White Paper RWP-0625: Rubrik Cloud Vault for Microsoft Azure - Technical Deepdive.

This document went over technical details on the architecture, value proposition, and key differentiators unique to Rubrik Cloud Vault. Readers were also provided with technical information about how different Rubrik solutions further secure their data using Rubrik Cloud Vault.

For additional information on Rubrik Cloud Vault or any of the Rubrik solutions mentioned in this document, please visit https://www.rubrik.com or reach out to your local Rubrik Account Team.

VERSION HISTORY

Version	Date	Summary of Changes	Author
1.0	September 2023	Initial Release	Brian Mislavsky
2.0	April 2024	- Add Object Level Immutability - Add Azure Secure Access	
3.0	September 2025	- Added Service Tiers - Updated Data Plane-specific information - Updated Encryption - Added Rubrik Optimized Snapshots	

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

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

Rubrik (NYSE: RBRK) 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.

Rubrik-Cloud-Vault-for-Microsoft-Azure_Technical-Deepdive / 20251031