rubrik + Microsoft

Azure Blob Storage Protection

Keep your Blob data safe and available

TODAY'S DATA MANAGEMENT AND SECURITY CHALLENGES

Azure Blob Storage is one of Azure's oldest and most reliable services, relied upon by companies around the world to store exabytes of unstructured, business-critical data. Far from being merely a repository for low-priority information, Blob Storage has evolved into a cornerstone for enterprise applications, powering critical workloads – from backup to AI and real-time analytics.

The reality is that companies are struggling to keep their cloud data safe. And it's no wonder - protecting the cloud perimeter comes with inherent challenges.

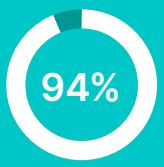
Inconsistent Data Protection: The sheer volume and sprawl of Blob data makes it difficult for an organization to set consistent protection policies across (potentially) hundreds of accounts. This often results in users maintaining backup plans in every Azure account where Blob accounts exist.

Lack of Visibility into Sensitive Data: About half of organizations surveyed say they lost sensitive data in 2023.[3] IT and security teams don't have the tools to understand where sensitive data lives in their Blob data and whether it is properly secured.

Slow Recovery: Organizations need the ability to quickly search for and restore specific Blobs, rather than depending on full storage account restores. This is essential because restoring an entire storage account can be a time-intensive process, particularly with large datasets or when recovering data from multiple accounts.

Expensive Backups: With Azure Backup, Blob data is backed up into either Hot or Cool Tier. Azure Backup does not currently support archiving Blob backups to the cheaper tiers such as Cold or Archive to help lower the cost.

AS DATA VOLUMES IN CLOUD ENVIRONMENTS LIKE AZURE BLOB GROW, SO DO ATTACKS.



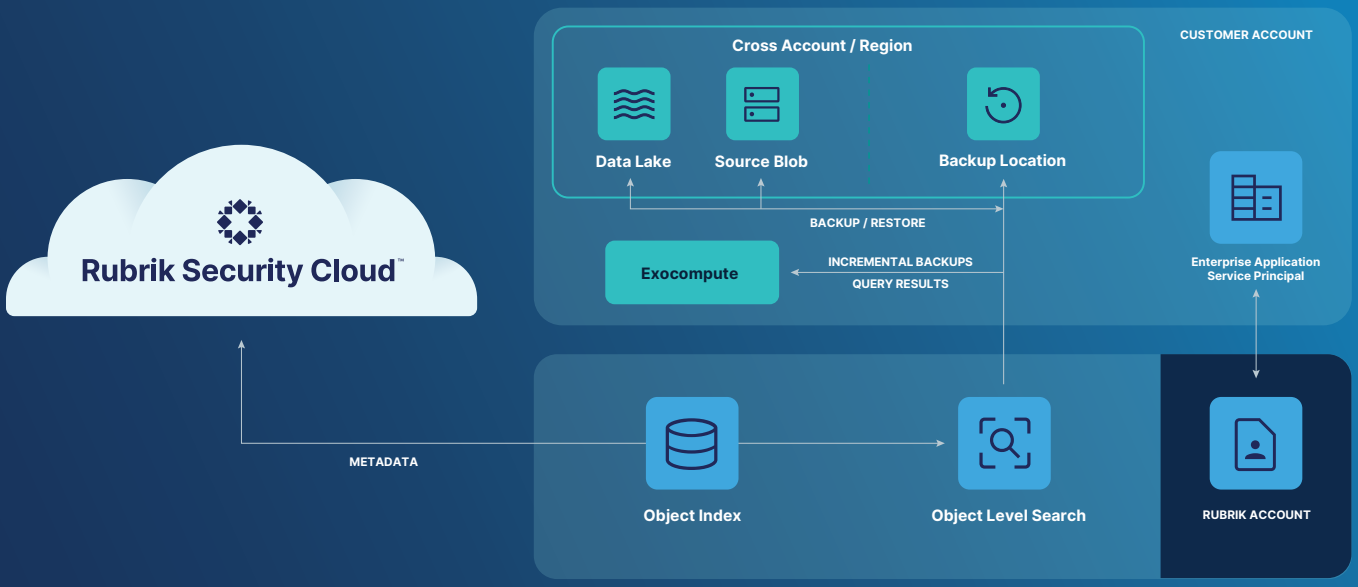
94% of IT and security leaders reported their organizations experienced a significant cyberattack last year.[1]

94% of cloud tenants were taergeted every month in 2023.[2]

62% were successfully compromised.[3]

[1] https://www.rubrik.com/zero-labs/2023-winter
[2] https://www.rubrik.com/content/dam/rubrik/en/resources/report-review/rpt-zero-labs-4.pdf
[3] https://www.rubrik.com/company/newsroom/press-releases/23/rubrik-zero-labs-fall-2023

AZURE BLOB PROTECTION FROM RUBRIK: YOUR SINGLE PANE OF GLASS



IT leaders responsible for managing and securing Azure Blob data can use Rubrik's Azure Blob Protection to safeguard their data from cyberattacks and loss. This solution offers a unified interface for managing data across all Azure accounts, regions, and workloads. It automatically discovers and inventories Blob containers, while providing policy-based protection that delivers global protection and complete cyber resilience. Key features include immutable, air-gapped backups, access control, and Blob and container level search and restore capabilities.

VERSIONING & REPLICATION DOESN'T PROTECT AGAINST CYBERATTACKS

While versioning and replication protect against accidental data loss or corruption, they cannot guard against malicious activities from compromised accounts. Since all data copies reside within the same account, an attacker can still encrypt, delete, or steal them. To truly safeguard data in Blob storage, you need comprehensive cyber protection. This includes implementing air-gapped, immutable backups with robust access controls and visibility into sensitive or overexposed data.

COMPREHENSIVE CYBER RESILIENCE FOR AZURE BLOB DATA

- Single-pane-of-glass visibility and management across all accounts and regions
- Immutable, logically air-gapped, access-controlled backups that are fully encrypted
- Object scanning to identify sensitive, overexposed, or unprotected Blob data
- Global security policies across on-prem and cloud workloads
- Locate and restore specific objects with granular search, or prioritize recovery of critical data using date ranges and prefixes
- Lower TCO with data archival to Azure Blob Cold and Archive tiers
- Azure Data Lake Storage (ADLS) Gen2 protection

KEY FEATURES OF AZURE BLOB PROTECTION FROM RUBRIK

Automatic Discovery and Onboarding: Once customers log in with a one-time, global administrator credential and are authenticated, Rubrik automatically deploys resources that enable backup and recovery processes. Rubrik's read-only permissions at the subscription level eliminate the need for extensive permissions for daily operations like backup, indexing, replication, and archiving. Permissions can be temporarily elevated when a restore is required, reverting to the least privilege model upon completion. During onboarding, Rubrik automatically configures resources such as Exocompute, a scalable Azure Kubernetes Service cluster that handles data movement and indexing, and an Enterprise Application/Service Principal for subsequent Azure subscription authorization.

After onboarding, customer credentials are immediately deleted from memory and never saved within the Rubrik platform. Rubrik Security Cloud then automatically discovers and inventories all storage accounts across the customer's Azure tenants, providing a single interface to manage data protection for all tenants and subscriptions.

Global Policy-Driven Protection: Rubrik's global "SLA Domains" protect Azure Blob and Data Lake Gen 2 storage accounts. SLA Domains replace the legacy "jobs" concept with a single policy assigned at the subscription, resource group, or storage account level. It supports all Azure Block Blob storage accounts, including Hot, Cool, Cold, and Archive tiers.

Ready to experience better management and protection for all of your Azure Blob data?

Contact us today to get started.

Superior Visibility and Control Over Sensitive Data: Continuously and autonomously discover, classify, and catalog all known and shadow data across all Azure Blob accounts in order to ensure comprehensive data governance, enhance security measures, and facilitate efficient data recovery strategies. Cut data exposure risk by contextualizing threats, identifying over privileged users, and monitoring for suspicious activity

Automatic, Immutable Backups: With Rubrik's "Incremental Forever" approach, the first backup is a full backup of the entire data set, while subsequent backups only process changed data since the last backup. Backups are stored in Azure storage accounts, using Hot, Cold, Cool, or Archive storage tiers. Rubrik enables logical air gaps by allowing customers to store backups in different regions or Azure subscriptions than the source data. For complete cyber resiliency, Rubrik uses Azure WORM (Write Once Read Many) technology to make backups immutable, protecting them from accidental or malicious deletion or encryption.

Rapid Restore: Rubrik allows you to restore entire storage accounts or individual blobs. To restore a storage account, select the account and specify the restoration point, which can be a different account. For blob-level restoration, search for a blob's name at a specific point-in-time, select the blob(s) to recover, and restore them to the original location or a different account. You can restore storage accounts and blobs to any region within any onboarded Azure tenant, regardless of where the original backups reside.

Lower TCO: Azure Blob Protection from Rubrik helps customers reduce cloud storage costs relative to Azure Backup, lowering the TCO. Data is compressed when archived, and users have the flexibility to instantly archive data to a variety of destinations, including lower-cost Azure Blob tiers and on-premises storage.