rubrik

Amazon S3 Protection

Manage and protect all Amazon S3 data.

DATA MANAGEMENT AND SECURITY CHALLENGES

Today, more than a million organizations[1] around the world rely on Amazon Simple Storage Service (S3) to store billions of unstructured, business-critical files. As data volumes grow and cybercrime increases, it's never been more important to manage and protect that data. But protecting Amazon S3 data is challenging.

- **Inconsistent Data Protection**
  The sheer scale of data can make it difficult for a customer to have consistent protection policies set up across (potentially) hundreds of accounts. This can result in IT maintaining separate backup plans in every Amazon Web Services (AWS) account where Amazon S3 buckets exist.
- **Shadow Amazon S3 Buckets**
  With hundreds of buckets deployed across hundreds of accounts, organizations can lack visibility and awareness of data residing within Amazon S3, resulting in unprotected critical organizational data.
- **Slow Recovery**
  If recovery becomes necessary, many organizations need the ability to quickly search for and restore specific objects, rather than depending on full bucket restores. This is essential because restoring an entire bucket can be time-intensive, particularly with large datasets or when recovering data from multiple buckets.
- **Expensive Backup**
  Backup solutions need to be able to leverage tiered storage within AWS such as Amazon S3 Glacier to keep costs low.

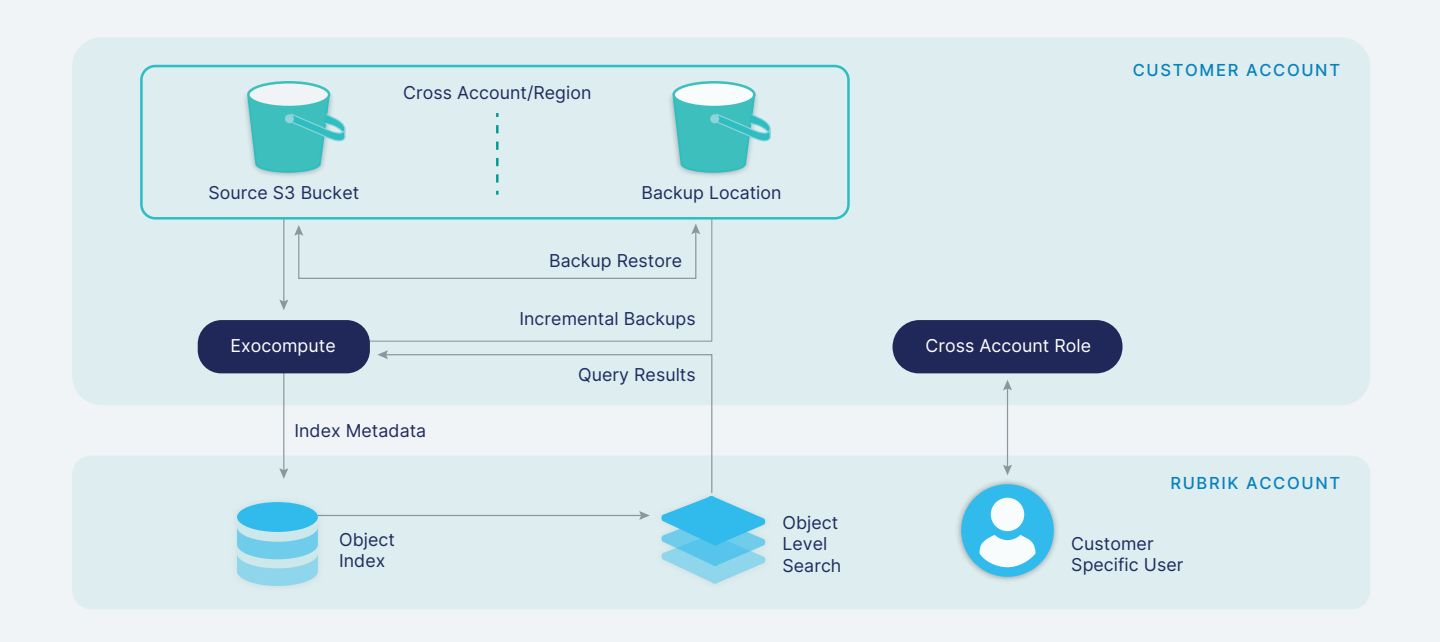
SUPERIOR MANAGEMENT AND PROTECTION FOR AMAZON S3 DATA

- Single pane of glass for protecting all Amazon S3 buckets across all accounts and regions for rapid recovery
- Object-level search and object- and folder-level restore
- Lower total cost of ownership (TCO) with data compression and instant archival to lower-cost Amazon S3 tiers
- Zero Trust architecture with air-gapped, immutable, access-controlled backups that never leave the environment

1 Enlyft.com, Companies using Amazon S3

aws PARTNER

AMAZON S3 PROTECTION FROM RUBRIK: YOUR SINGLE PANE OF GLASS



IT leaders tasked with managing and securing Amazon S3 data from cyberattacks and data loss can turn to Amazon S3 Protection from Rubrik for a complete solution for all data. Using Rubrik Security Cloud's unified interface, Amazon S3 Protection from Rubrik features automated discovery and inventory of Amazon S3 buckets across all related AWS accounts. From there, Rubrik's powerful and intelligent Service Level Agreement (SLA) Domain policy-based protection delivers cyber resilience for Amazon S3 objects, providing key table-stakes security features, such as immutable, air-gapped backups, role-based access control, and fast, efficient object-level search and object- and folder-level restore.

KEY FEATURES OF AMAZON S3 PROTECTION FROM RUBRIK

Automatic Discovery and Onboarding: Once authenticated into an AWS account, Rubrik will deploy an AWS CloudFormation stack to provision everything needed for Amazon S3 backup and recovery. Subsequent authentication is handled by a cross-account role, allowing customers to securely grant Rubrik access to their account while maintaining the ability to control and audit activity within their organization. Rubrik Exocompute is also configured to index Amazon S3 buckets and objects. For customers with multiple accounts, a CSV file with account details can be uploaded to Rubrik Security Cloud, enabling configuration of multiple AWS accounts at once. After Amazon S3 has been onboarded, Rubrik Security Cloud automatically discovers and inventories all Amazon S3 buckets within the AWS account, delivering a single interface to manage data protection needs.

Global Policy-Driven Protection: Amazon S3 buckets are protected with Rubrik's Global SLA Domains, which provide a unified approach to manage data protection across all Amazon S3 buckets as well as other workloads and environments protected by Rubrik. Once configured, SLAs are assigned to our Amazon S3 buckets, either on the account level, the bucket level, or assigned to buckets based ono AWS tag key-value pairs. Any bucket running within Amazon S3 Standard or Amazon S3 Infrequently Accessed can be protected by Rubrik Security Cloud through global SLA Domains.

Lower TCO: Amazon S3 Protection from Rubrik helps customers reduce cloud storage costs, 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 Amazon S3 tiers and on-premises storage.

Rapid Restore: Amazon S3 Protection from Rubrik enables restoration on both the bucket- and object-level hierarchy. For bucket-level restore, customers simply select the bucket they would like to recover within the Rubrik Security Cloud UI and specify the restore target. For object-level restore, customers can search for objects based on names on the snapshot level, select the desired objects to recover, and restore to either the original bucket (in-place) or a different bucket (export). Both buckets and individual objects can be restored to any region within any account, no matter where the original backups exist.

Ready to experience better management and protection for all your Amazon S3 data? Contact us today to get started.