rubrik

WHITE PAPER

Rubrik Zero Trust for Microsoft Environments

Table of Contents

RUBRIK ZERO TRUST FOR MICROSOFT ENVIRONMENTS

The proliferation of ransomware continues and organizations are faced with a paradigm shift in how they plan for an attack. This has also resulted in a new wave of technologies and tools to aid in the shift to Zero Trust. The National Institute of Standards and Technology (NIST) defines Zero Trust as "a set of cybersecurity principles used when planning and implementing an enterprise architecture." Rubrik Zero Trust Data Security is a data protection and cyber resilience platform that is based upon the principles of NIST's Zero Trust Architecture to protect application and user data against unauthorized access, and to provide a reliable recovery point from cyber attacks, such as ransomware.

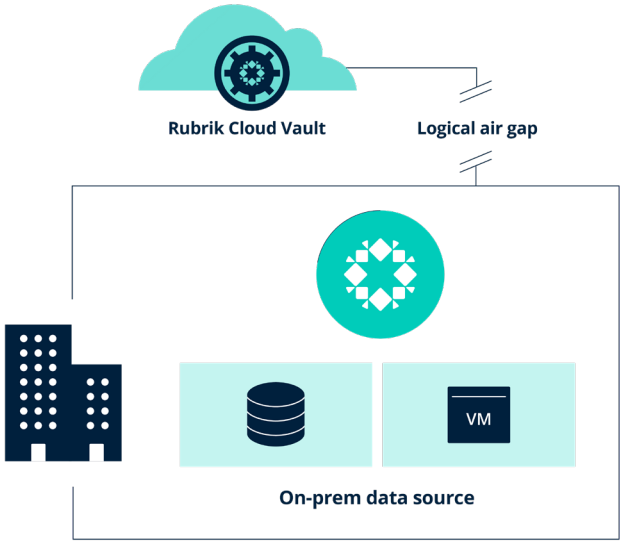
Underlying the Rubrik Zero Trust Architecture is Rubrik Security Cloud, a core set of technologies that set Rubrik apart from legacy backup solutions.

- **Immutable data platform –** Once ingested, no external or internal operation can modify the data. Data managed by Rubrik is never available in a Read/Write state to the client. This is true even during a restore or Live Mount operation. Since data is written as incrementals, infected data later ingested by Rubrik does not overwrite existing files or folders.
- **Declarative policy engine –** Rubrik allows administrators to abstract away much of the low-end fuss required to build and maintain data protection, so they can focus on adding value at a more strategic level across the organization. The Rubrik policy engine is elegantly simple because all of the imperative details are abstracted away and handled by an incredibly smart, scale-out system. The resulting input fields are reduced to Recovery Point Objective (RPO), retention period, archive target, and replication target.
- **Anomaly Detection –** As each backup snapshot's metadata is collected by Rubrik, we leverage machine learning to build out a perspective of what is going on with the workload. The model is trained to identify trends that exist across all samples and classify new data by their similarities without requiring human input. The result is that Rubrik detects anomalies, analyzes the threat, and helps accelerate recovery with a few clicks.
- **Sensitive Data Monitoring –** Reduce sensitive data exposure and manage exfiltration by discovering what types of sensitive data you have, where it lives and who has access to it.
- **Secure API-first architecture –** Having an API-Driven Architecture means that every action within the Rubrik UI can be accomplished by consuming an underlying API endpoint. Or in other words, if you can do it through the Rubrik UI, you can programmatically do the same through the API that's secured by role-based access and OAuth 2.0 Bearer tokens.

Simply put, Rubrik Zero Trust Data Security's enforces stringent controls around users, hosts, and applications that attempt to access it. **Trust nothing. Verify everything.**

EXTEND ZERO TRUST TO AZURE

Protecting data and workloads in hybrid cloud environments requires Zero Trust protection that is seamless between on-premises data center environments and public cloud infrastructures. Microsoft and Rubrik each bring best-in-class offerings and capabilities that unify management and offer a holistic approach to Zero Trust Data Security for your hybrid cloud.



Rubrik protects your Microsoft environments with full data protection for VMs running in Azure, as well as for storage volumes via Azure Managed Disks. API-driven integration between Rubrik and Azure storage services offer secure, immutable archival for long-term retention. Additionally, protection for Microsoft 365 creates a logical air gap for Microsoft data. Finally Rubrik has worked closely with Microsoft to offer an off sight data storage service built on Azure Blob Storage, called Rubrik Cloud Vault.

With Rubrik Cloud Vault, we deliver a new data security and ransomware recovery solution, to expand Rubrik Zero Trust Data Security capabilities to the cloud for account-isolated backup copy of customers' data.

With Rubrik Cloud Vault customers can build a comprehensive and multi-layered data protection strategy. The offering allows customers to maintain both immutable and instantly recoverable copies of their most-critical data in a secured cloud location, fully-managed by Rubrik. The offering reduces the risk that data is modified, deleted, or encrypted, and is logically air-gapped from customers' production environments for enhanced security against ransomware attacks.

Rubrik Cloud Vault adds an additional layer of Zero Trust to Azure by removing the chance for archived data to be destroyed by compromised administrator credentials. This is accomplished by placing data in an immutable Blob container that only Rubrik services can access.

Being offered as a service will additionally allow customers still on their cloud adoption journey to have a secured immutable storage location in the cloud with just a few clicks.

This technical note explains how the Rubrik Zero Trust Architecture extends into Microsoft Azure and Microsoft 365 environments so that enterprise data, backed up by Rubrik, is protected from ransomware attacks and other cyber threats.

SECURE ACCESS

All data access starts with authentication. Authentication verifies who a user or service is. In the current age, simple authentication with just a username and password is unacceptable. Multi-Factor Authentication (MFA) is a requirement. MFA is defined as requiring two or more authentication factors. An authentication factor can be something a user knows (a password), something the user has (a trusted device that is not easily duplicated, like a phone or hardware key), or something inherent to the user (fingerprint, voice, or face).

Rubrik offers a native MFA solution that is not dependent on any external systems. This provides a simple, yet effective MFA solution using Time-based One Time Passwords (TOTP). However, for many organizations, MFA needs to be centralized to make it easy on users and for IT to manage and enforce. Rubrik has adopted SAML 2.0 which means it seamlessly integrates with Azure Active Directory (Azure AD) to provide a robust MFA solution for data protection operations across Azure and Microsoft 365. Azure AD provides the following MFA options including SMS, Voice, Authenticator App, and more.

Bad: Password	**Good:** Password and...	**Better:** Password and...	**Best:** Passwordless
123456	**SMS**	**Authenticator** (Push Notifications)	**Windows Hello**
qwerty	**Voice**	**Software Tokens OTP**	**Authenticator** (Phone Sign-In)
password		**Hardware Tokens OTP** (Preview)	**FIDO2 Security Key**
iloveyou			
Password1			

After authentication, the process known as authorization determines what access rights an authenticated user or service has within the system. For example, authorization is what separates an administrative user, who can do anything within the system, from a service account that may only have read-only access to a specific portion of the system. Rubrik uses fine grained Role Based Access Control (RBAC) to make managing authorization simpler and more secure. Accounts can be given predefined or custom roles within the system and those roles determine a user's access rights.

To take this a step further, fine grained RBAC allows an administrator to provide the least privileges required for a task. Least privilege ensures authorized users have the absolute minimum amount of access rights that they need to perform their work. Since both Rubrik and Azure provide predefined roles, administrators have a good starting place to configure RBAC and least privilege across their Rubrik systems and into Azure.

EXTEND DATA IMMUTABILITY INTO AZURE

The proliferation and increased sophistication of ransomware has shown that backup data is a major target of cyber criminals. Many ransomware deployments delay execution of ransom notes until they have mitigated any protections a victim might have in place. Specifically the criminals target backup with encryption and destruction to maximize their chances of receiving the ransom. The best protection against this is to store backups in a purpose-built immutable location.

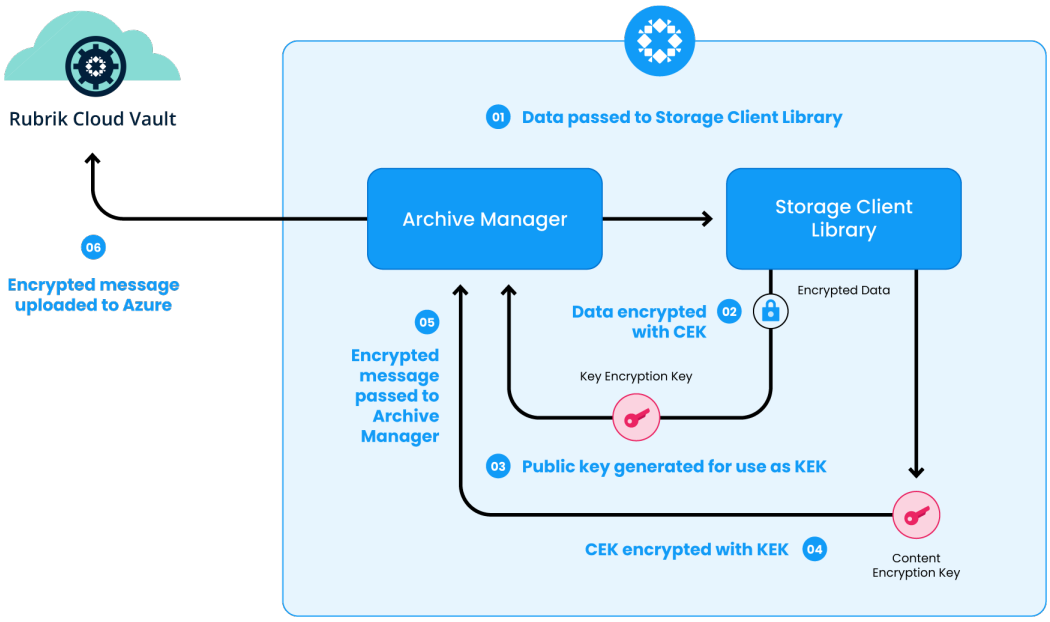
To provide immutability, Rubrik uses a purpose-built, append-only file system that stores data in a secure, proprietary format. As data is ingested, it is broken into chunks of data called patch files. A checksum algorithm is used to create a data fingerprint that is then permanently associated with each patch file. Those fingerprints are verified any time data is read from the system to ensure it hasn't been altered. The result is data that is secure, immutable, and ready for recovery. Given that many organizations are already utilizing the public cloud or plan to soon, it is crucial that their data maintain its immutability as that data is migrated.

For cloud archival operations, Rubrik integrates directly with the native immutability features of Azure Blob storage. This archive can live in the customer's Azure account or can be provided by the Rubrik Cloud Vault service. Rubrik securely transfers data to Azure Blob storage creating an immutable, readily available offsite copy of your data. In addition, businesses can protect their cloud-native workloads running on Azure using Rubrik Cloud-native Protection (CNP). Rubrik CNP utilizes Azure's native VM and Managed Disk snapshots which are also immune to being altered. The result is a seamless, automated, and immutable backup and archive for both traditional, on-premises workloads and those that are running on Azure.

ENCRYPT EVERYWHERE

Encryption is a requirement to secure modern enterprise applications. Rubrik offers data encryption at rest and in flight. Data at rest encryption uses AES-256 via a 256-bit Data Encryption Key (DEK). Additionally the DEK is encrypted with a 256-bit Key Encryption Key (KEK). These encryption keys are securely managed by a hardware TPM by default. Alternatively, using a KMIP-compliant Key Management Server (KMS) such as Azure Key Vault provides a centralized, scalable, and secure KMS that can manage keys across Rubrik clusters and other solutions.

In order to archive data from Rubrik cluster to Rubrik Cloud Vault or Microsoft 365, similar processes are followed. Prior to transferring data via a secure channel, Rubrik encrypts data with a Content Encryption Key (CEK). Then, to ensure the CEK stays safe, a KEK is generated which is used to encrypt the CEK. Data can then be transferred over the secure channel to a Rubrik Cloud Vault or Azure Blob Storage location where it will land in its encrypted format.



If a bad actor or attacker is able to gain access to administrator or compromised credentials, they would have no direct access to the data stored in Rubrik Cloud Vault or Microsoft 365 protection. Additionally, if Retention Locked SLAs are used they would be unable to delete or decrease the retention period of data locally on Rubrik appliances or stored in archive locations. This makes it very difficult for data to be affected by an attack. The protection and security of Rubrik cluster along with the flexibility and scalability of Rubrik Cloud Vault and Microsoft 365 protection make a formidable data defense.

ESTABLISH A LOGICAL AIR GAP

The legacy approach of securing data was to store a copy of data offline, usually on tape, so that there was no access to it. This was referred to as a physical air gap. Our always on and connected world, along with the pace at which data continues to grow, has dictated that a more modern approach be created. Rubrik creates a logical air gap for protected data that achieves the same objectives as a physical air gap by enforcing the following:

- **Authentication –** Both GUI and API are secured via MFA ensuring that attackers cannot gain access to the system even with compromised credentials.
- **Authorization –** Fine grained role-based access control enables the principle of least privilege to prevent users from moving laterally within the system to gain unauthorized access to resources.
- **Audit logging –** Operations are logged and can be monitored locally or shipped to a log analysis tool so there is an audit trail when changes are made within the system.
- **SLA compliance –** Attackers and rogue admins target backup data to remove an organization's ability to recover. With Rubrik SLA Retention Lock, organizations can prevent unauthorized reduction in data retention which ensures their SLAs can not be reduced to cause data to expire too soon.

The logical air gap not only applies to data protected by Rubrik on-premises but also extends into Rubrik Cloud Vault, Azure, and Microsoft 365. Rubrik ensures that data archived to Rubrik Cloud Vault is also logically air gapped by applying the same enforcement mechanisms through its integration with Azure. Additionally, by

storing the protected data in a separate, secure account managed by Rubrik, rogue or compromised Cloud Administrators cannot delete or alter the archive locations ensuring the data is intact and readily available when it is needed for recovery.

ENRICH MICROSOFT SENTINEL WITH RUBRIK INSIGHTS

Microsoft Sentinel users can accelerate and enrich threat investigations with more data risk insights and speed up recovery time with automated responses.

When Rubrik detects an anomaly, in addition to IT Operations receiving an alert, an incident also gets created in Microsoft Sentinel, so the Security team gets notified about anomalous activity. Furthermore, this gets enriched with detail about what types of sensitive information are compromised, such as credit card information, patient health care records - so Security teams can appropriately assess and triage. They can identify and block indicators of compromise in your historical data so that they can identify the last known clean copy.

When it comes to recovery Rubrik has a full set of capabilities available to the responder in terms of how they want to recover - whether it be a livemount, export or recover files. Recovery playbooks are included and can be customized to drive the behavior and automation they want to in the Rubrik Security Cloud platform.

With Rubrik for Microsoft Sentinel, Security and IT Operations understand the time of the attack, what data was affected and are able to confidently restore the last known clean copy to prevent malware reinfection.

CONCLUSION

It is clear that cyber criminals and their attacks are evolving to circumvent layers of protection. Attacks are becoming more targeted and ransom demands are increasing at an alarming rate. Organizations are looking for vendors to aid them in ensuring a fast and effective recovery. Rubrik and Microsoft have joined forces to give customers an easy onramp to a robust Zero Trust strategy that extends from the datacenter to the cloud.

Rubrik Cloud Vault utilizes Rubrik's Zero Trust Data Security with fundamental security and reliability features of Azure Blob Storage to provide customers with a valuable solution for addressing ransomware threats, as well as a secure platform to protect, and deliver accelerated recovery to their most important digital assets.

By combining Rubrik with Azure's native security features, customers can be confident that their data is safe across their hybrid cloud. Rubrik integrates directly with Azure Blob storage, Azure VM snapshots, and Azure Managed Disk snapshots to provide a seamless management experience for cloud archival, cloud-native, and Microsoft 365 data. Coupled with Azure's native security and access features such as MFA, RBAC, network controls, and Azure immutable Blob storage, a logical air gap is extended from on-premises to the cloud giving customers a single, united Zero Trust data protection solution.

For more information, please visit rubrik.com/products

rubrik

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

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

wp-rubrik-zero-trust-for-microsoft-environments / 20230913