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 Management is a data management and cyber resilience platform that incorporates NIST Zero Trust cybersecurity principles 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 DataGuardian, 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 cannot be overwritten, even infected data later ingested by Rubrik cannot infect other 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 RPO, retention period, archive target, and replication target.

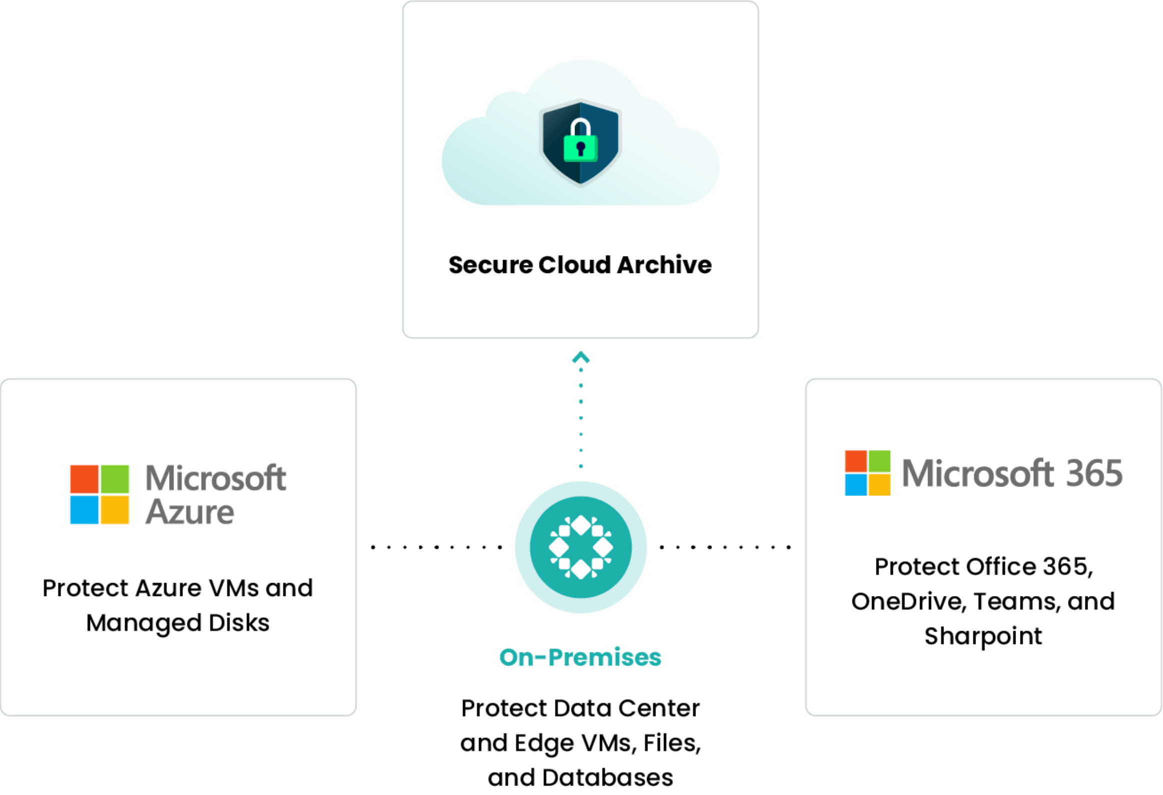
- **Threat engine –** As each backup snapshot's metadata is collected by Rubrik, we leverage machine learning to build out a full perspective of what is going on with the workload. The deep neural network (DNN) is trained to identify trends that exist across all samples and classify new data by their similarities without requiring human input. The result is that Rubrik detects anomalies, analyzes the threat, and helps accelerate recovery with a few clicks.

- **Secure API-first architecture –** Having an API-Driven Architecture means that every action in the Rubrik UI has a corresponding API that is documented and available for use. 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 Management only presents one path to access data, allowing the enforcement of 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 Management for your hybrid cloud.


Secure Cloud Archive
Microsoft Azure
Protect Azure VMs and Managed Disks
Microsoft 365
Protect Office 365, OneDrive, Teams, and Sharpoint
On-Premises
Protect Data Center and Edge VMs, Files, and Databases

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 Office 365, OneDrive, SharePoint, and Teams creates a logical air gap for Microsoft data.

This technical note explains how the Rubrik Zero Trust Architecture extends into Microsoft Azure and Microsoft 365 environments so that enterprise data, no matter where it resides, is always 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 qwerty password iloveyou Password1	**SMS** **Voice**	**Authenticator** (Push Notifications) **Software Tokens OTP** **Hardware Tokens OTP** (Preview)	**Windows Hello** **Authenticator** (Phone Sign-In) **FIDO2 Security Key**

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, it is easy for administrators 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.

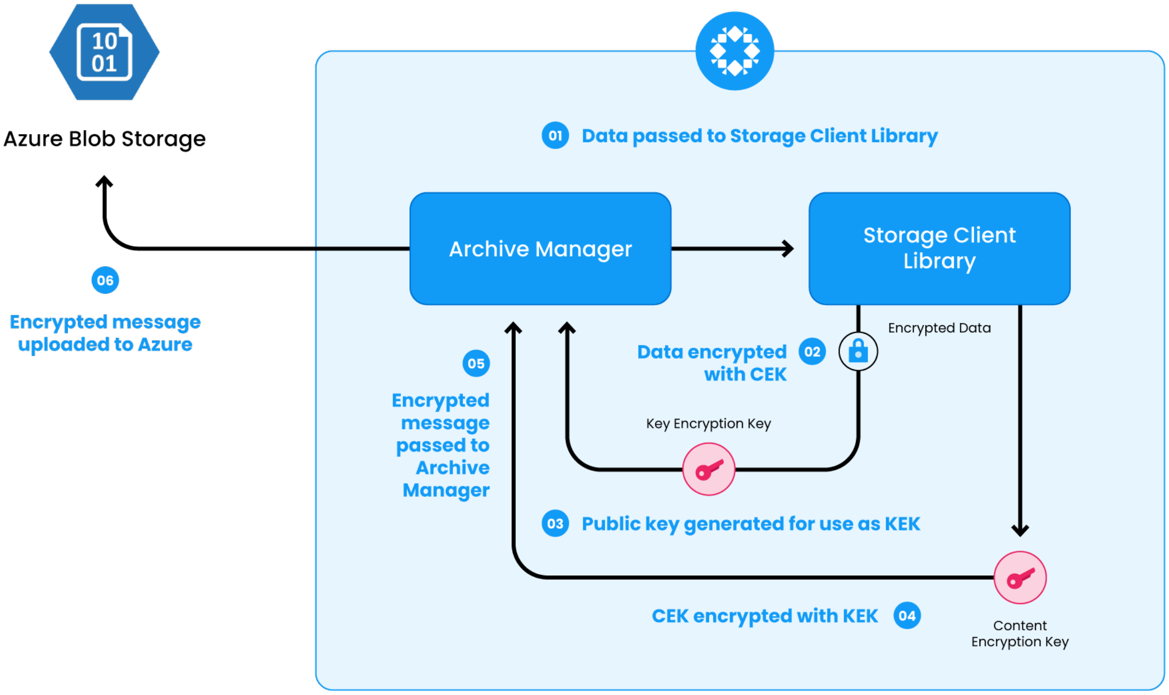
To provide immutability, DataGuardian uses a purpose-built, append-only file system that stores data in a secure, proprietary format. As data is ingested, it is broken into chunks of data called patch files. A checksum algorithm is used to create a data fingerprint that is then permanently associated 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 always 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 Cloud Data Management (CDM) integrates directly with the native immutability features of Azure Blob storage. Rubrik CDM 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 encrypts all data 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). KEK rotation can be automated via the Rubrik API and is a best practice to do regularly. 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 to Azure, 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 an Azure Blob store where it will land in its encrypted format.


10
01
Azure Blob Storage
01 Data passed to Storage Client Library
Archive Manager
Storage Client Library
06
Encrypted message uploaded to Azure
Encrypted Data
05
Encrypted message passed to Archive Manager
Data encrypted with CEK 02
Key Encryption Key
03 Public key generated for use as KEK
CEK encrypted with KEK 04
Content Encryption Key

If a rogue admin or attacker is able to gain access to the Azure Blob store, they would still need to get access to the KEK and CEK in order to decrypt any data. Additionally, Rubrik stores data in a proprietary format that only DataGuardian knows how to read.This makes it very difficult for data archived to Azure to be exfiltrated during an attack. The protection and security of Rubrik CDM along with the flexibility and scalability of Azure Blob storage 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. DataGuardian 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 CLI 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 any unauthorized reduction in data retention which ensures their data is always ready to be recovered.

The logical air gap not only applies to data protected by Rubrik on-premises but also extends into Azure and Microsoft 365. DataGuardian ensures that data archived to Azure Blob storage is also logically air gapped by applying the same enforcement mechanisms through Rubrik's integration with Azure. Additionally, by storing the protected Azure or Microsoft 365 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 exactly when it is needed for recovery.

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 public cloud.

By combining DataGuardian 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 own 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/zerotrust

rubrik

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

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

Rubrik, the Zero Trust Data Management™ Company, enables cyber and operational resilience for enterprises; including ransomware protection, risk compliance, automated data recovery, and a fast track to the cloud. For more information please visit www.rubrik.com and follow @rubrikInc on Twitter and Rubrik, Inc. on LinkedIn.

20211004_v1