TECHNICAL WHITE PAPER

Microsoft 365 Architecture and Security

August 2022
RWP-0582

TABLE OF CONTENTS

INTRODUCTION

Security has been a hallmark of Rubrik's products since the release of our initial product, CDM, in 2015. As Rubrik's software has extended into Software-as-a-Service (SaaS), security has remained a top priority and concern.

Rubrik is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services.

In this white paper Rubrik will discuss all elements of Rubrik's Microsoft 365 (M365) Backup and Recovery product line including infrastructure, encryption and key management, where data is stored and how Rubrik keeps the data integrous and available.

ARCHITECTURE

HYBRID SAAS INFRASTRUCTURE

Rubrik's hosted backup and recovery solution for Microsoft 365 (M365) has evolved over the years. The original Rubrik's M365 Backup and Recovery offering is a Hybrid SaaS model where Rubrik deploys software in the customer's Azure subscription.

Inside this architecture are three main layers of software that make up the hybrid SaaS model:

1. **The Control and Management Plane**
   The "brains" behind Rubrik's M365 offering. M365 protection is orchestrated by a data management engine. It runs as SaaS and is responsible for control and management of the Rubrik M365 software stack. Examples of control and management include access control, audit, backup/recovery tasks and reporting.

2. **The Data Plane (Exocompute)**
   Exocompute is the software that runs in a customer's Azure environment and is responsible for moving data from M365 to Azure Blob Storage (also in the customer's environment). This software is also known as the "data plane."

3. **The Source Data (M365)**
   The source data for M365 of course resides in M365 which includes Exchange, OneDrive, Sharepoint, Teams, etc. This data is pulled by the Exocompute layer into the customer's Azure environment.

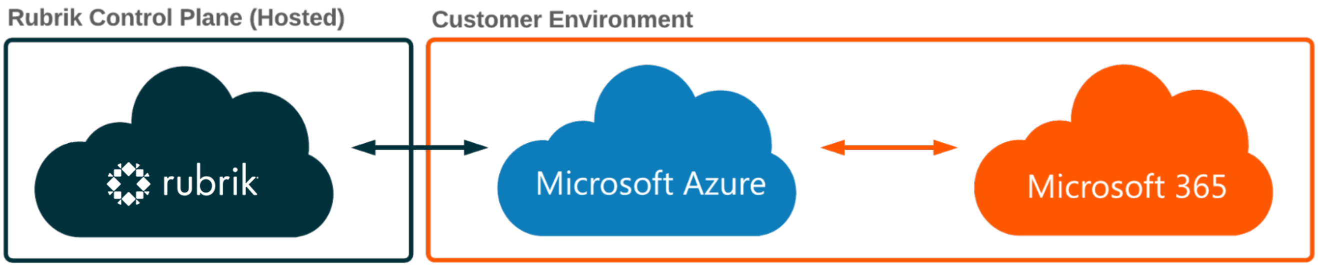

Figure 1. Hybrid architecture

PURE SAAS (HOSTED) INFRASTRUCTURE

Rubrik has also extended its M365 backup and recovery offering to include a "Pure SaaS" or hosted model.

In this architecture, customers do not need to manage Rubrik software components (e.g. Exocompute) in their own Azure environment. Instead the solution is delivered as a fully managed SaaS service. The control and management plane, as well as the customer's M365 source data, remain the same as with Hybrid SaaS. The only difference is Rubrik will manage the data plane and its associated software, and customers no longer need to pay for the Azure infrastructure costs to run the data plane. This model also provides customers with recovery capabilities that are resilient to ransomware attacks against the source tenant. This is due to the fact that the backed up data sets are air gapped away from the source tenant and stored inside the Rubrik owned tenant.

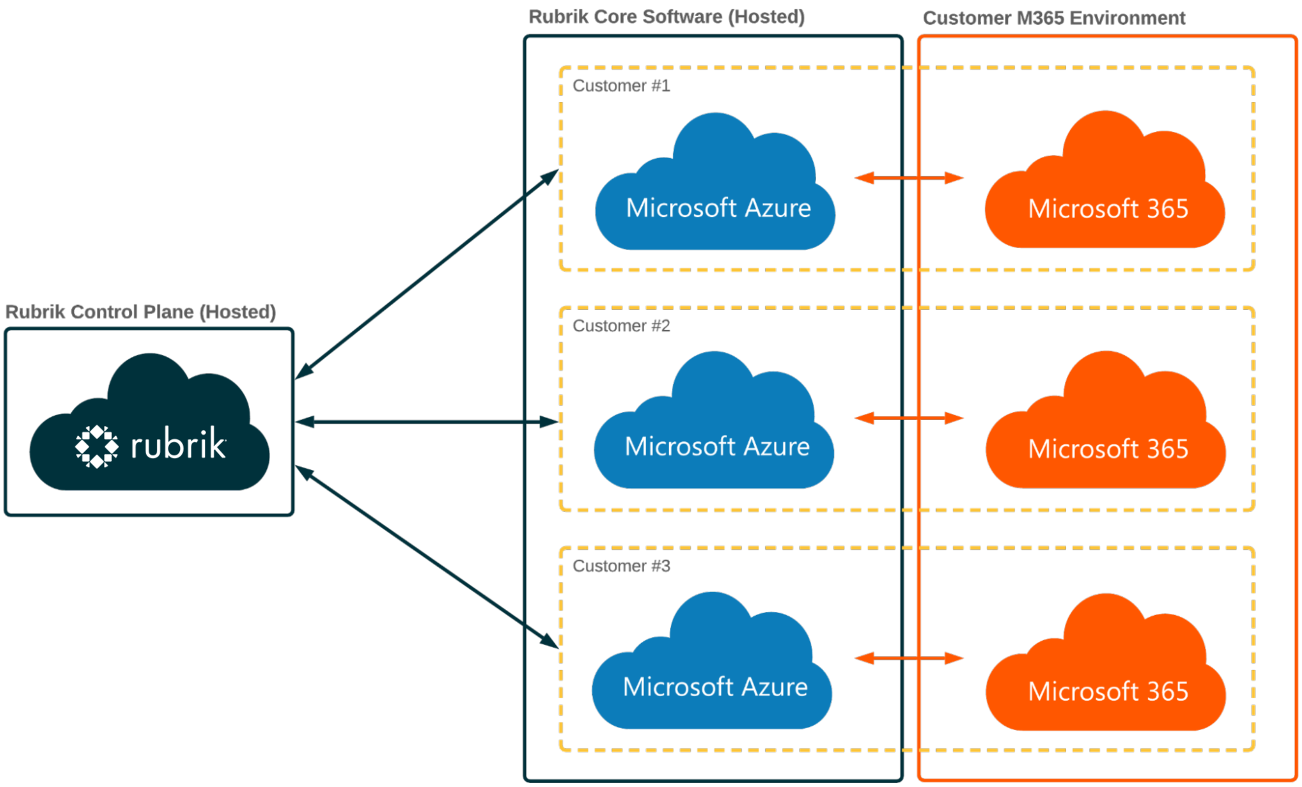

Figure 2. Hosted SaaS architecture

PURE SAAS (HOSTED) REGION DEPLOYMENTS

Rubrik's hosted (pure SaaS) M365 Backup and Recovery product can be deployed in multiple regions and data centers in North America, Europe, and Asia. The product is designed with high-availability and disaster recovery in mind, and regions are chosen that can support this.

M365 CORE SOFTWARE ARCHITECTURE AND COMPONENTS

Rubrik's core M365 software architecture consists of the following:

EXOCOMPUTE

Rubrik excompute runs inside of Azure environments and at its core is responsible for the data plane - that layer of software that pulls data from M365 and pulls it into the Azure (and ultimately Blob Storage).

The components that make up Rubrik's Exocompute layers include:

CONTAINERS

Rubrik's software for M365 is run in as a set of containerized applications. Container definitions are stored in an Azure Container Registry and updates are pushed via secure and automated deployment pipelines.

All containers are scanned for vulnerabilities as part of the deployment pipeline and then checksummed to ensure data integrity before being promoted to production. This ensures only authorized containers are ever run and that they have passed through appropriate validation checks.

KUBERNETES

Azure Kubernetes Service (AKS) is a managed container orchestration service based on the open source Kubernetes system and available on Microsoft's Azure public cloud.

AKS resides in a private Azure Virtual Network (VNet) allowing only inbound access from Rubrik. The connection between AKS and Rubrik is also secure using TLS 1.2 for transport.

Nodes in the Kubernetes cluster are managed by Microsoft and are running stripped down, hardened Linux operating systems. Security patches are applied regularly by Microsoft.

Lastly, AKS is managed by Rubrik - upgrades and scale are all handled automatically.

STORAGE

Rubrik's Exocompute data plane writes data to both Azure table and Blob Storage to store metadata and data respectively. Data is only ever stored encrypted-at-rest using both master and data encryption keys (KeK, DeK). Keys are stored securely in an Azure Key Vault KMS and accessed via secured credentials.

Storage accounts in Azure are set up to accept only TLS 1.2 connections with stringent firewall rules to allow only connections from trusted sources (e.g. Rubrik). Storage accounts use zone-redundant storage (ZRS) where data is replicated across multiple independent Azure data centers in the chosen region.

AZURE ACTIVE DIRECTORY (AD) AND ENTERPRISE APPS

Rubrik creates an Azure AD Enterprise Application (and associated Service Principal) for each customer who enables Rubrik's M365 Backup and Recovery software. The app is controlled by Rubrik but authorized by the customer through Modern Authentication (OAuth 2.0) to provide Rubrik access to their M365 subscription. Because Modern Authentication is used to perform this authentication, Rubrik never receives (and therefore, never stores) the customers credentials for their M365 subscription, as its access is revoked once Service Principals are created.

Rubrik's Enterprise Application architecture for M365 also provides scalable performance while performing backup and recovery tasks. By default, Microsoft rate limits the amount of calls an entity can make against the M365 APIs. This rate limiting is done per Enterprise Application and can bottleneck performance when using a single Enterprise Application. By increasing the number of Enterprise Applications, the amount of performance for ingest and restores also increases. Rubrik examines the workloads it is protecting within an M365 tenant, and dynamically recommends the appropriate Enterprise Application footprint to support the environment.

SECURITY AND ZERO TRUST ELEMENTS

AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING (AAA) IN RUBRIK

Rubrik Zero Trust Data Management approach of trust nothing, always verify, incorporates the "Triple A" (AAA) framework.

AUTHENTICATION

Authentication restricts access to Rubrik to a specified set of users.

Rubrik requires and enforces the use of strong passwords for all user authentication. This helps detect brute-force attacks and to block credentials identified in security breaches. Customer data is protected from certain common SaaS security issues, such as session hijacking, script insertion, and cross-site-request-forgery. Beyond this, IP whitelisting also enables Rubrik to restrict login access to a specified list of IP addresses, address ranges, or subnets.

SINGLE-SIGN ON (SSO)

Rubrik supports single sign-on (SSO) using the Security Assertion Markup Language (SAML) 2.0 standard. SSO allows login to Rubrik using credentials associated with an identity provider configured by the customer.

SAML 2.0 uses metadata files to exchange information between an identity provider (IdP) and a Service Provider (SP), such as Rubrik. The information in these files establishes a trust relationship between the two entities. The files also specify where authentication requests and responses should be sent, along with formatting details.

Rubrik can be integrated with any SAML 2.0-enabled IdP that supports SP-initiated SSO, such as ADFS, Azure, Okta, and OneLogin.

TWO-FACTOR AUTHENTICATION (2FA)

Time-based one-time passwords (TOTP) enable Rubrik Two-step Verification for Rubrik.

Rubrik Two-step Verification is an implementation of two-factor authentication (2FA) for Rubrik clusters. Users can enable Rubrik Two-step Verification to use TOTP-mediated 2FA, which provides an additional layer of authentication security. In addition to the username and password, TOTP uses an app to provide a single-use numeric code that serves as the second authentication factor. Administrators can enforce Rubrik Two-step Verification for users. When enforced, each user must configure Rubrik Two-step Verification on an individual basis.

Rubrik Two-step Verification supports authenticator apps from Microsoft, Google, and Okta.

AUTHORIZATION

Rubrik offers role-based access control (RBAC) that restricts access based on the roles of individuals within an organization. Depending on the assigned role, access rights are restricted to the relevant associated operations and resources. Access rights are also based on the least privilege principle, a key tenant of the Zero Trust framework with regard to M365.

For access to the Microsoft 365 APIs, Rubrik requests the minimum set of permissions needed to achieve the task for each Enterprise Application. Rubrik also uses multiple Enterprise Applications, each one scoped to a specific Microsoft 365 Application (i.e. Exchange Mailbox, OneDrive, etc.).

ACCOUNTING

The Rubrik Events feature identifies, isolates, and prioritizes incidents with a unified view of global Rubrik events.

The Events feature makes it possible to find point-in-time events (by event and object type) with easy-to-use filters and real-time search. M365 Events in Rubrik can also be forwarded to SIEMs or log management systems.

Audit log functionality shows log messages for Rubrik domain system events.

ENCRYPTION

All data in transit between Rubrik, Excompute (Azure), and M365 uses TLS 1.2 to communicate. No unencrypted communication is allowed. Communication internal to Rubrik or Exocompute is also encrypted with TLS 1.2 enforced.

Rubrik stores customers' backup data in Azure Blob Storage. To ensure strict isolation, each customer has their own Azure Storage Account. Data at rest is encrypted using the AES 256-bit cipher. Keys for data encryption are stored in Azure Key Vault with features like purge protection to prevent accidental key deletion enabled.. Key rotation is supported upon customer request.

NETWORK SECURITY

Rubrik's Exocompute data plane along with Azure Storage reside in a private VNet which has very restricted firewall rules, only allowing inbound access from trusted sources (e.g. Rubrik All connectivity into the data plane occurs through secure tunnels. Each tunnel is authenticated when established and secured using TLS 1.2 with mutual authentication by digital certificates. The certificates used for the tunnel are rotated periodically.

DATA INTEGRITY AND AVAILABILITY

WHERE IS DATA STORED?

M365 backup data and the indexes over it are stored in Azure Blob and table stores and encrypted using the AES 256-bit cipher. In order to maintain isolation between customers, each customer is assigned their own dedicated Azure Storage account. Customers may select the region that matches their data location requirements.

Master encryption keys are stored in Azure Key Vault. Access credentials to storage and Key Vaults are unique per customer.

HOW IS DATA STORED?

Customer M365 backup data is stored in Azure Blob and table storage. Metadata (e.g. object, job information) is stored in Rubrik in a multi-tenant relational database architecture. Data is de-duplicated across a customer's entire M365 subscription and also compressed.

HOW DOES RUBRIK ENSURE DATA DURABILITY?

Backup data is replicated via zone-redundant storage (ZRS)[1] which copies data synchronously three times to physically separated data centers in the same geographic region.

OPERATIONAL SECURITY

Rubrik keeps audit logs of all actions against production. No engineer has standing access to production, must request it with justification, and access is time limited.

Rubrik also conducts both internal and 3rd party reviews of security policies and access to production resources.

COMPLIANCE - 3RD PARTY VALIDATION AND CERTIFICATIONS

Rubrik's security policies are reviewed regularly by internal and 3rd party companies to ensure they are to best practices. Continual security scans and penetration testing is also part of Rubrik's security practice.

In late 2021 Rubrik completed a SOC 2 Type 1 audit.

[1] Data redundancy - Azure Storage | Microsoft Docs

MICROSOFT 365 API PERMISSIONS

EXCHANGE WEB SERVICE

- Calendars.ReadWrite.All
- Contacts.ReadWrite
- full_access_as_app
- Mail.ReadWrite
- Tasks.ReadWrite
- User.Read.All
- Tasks.ReadWrite

MICROSOFT GRAPH - GENERAL

- User.Read.All
- Group.Read.All
- Reports.Read.All

MICROSOFT GRAPH - EXCHANGE

- Calendars.ReadWrite
- Contacts.ReadWrite
- Mail.ReadWrite
- Group.Read.All
- User.Read.All
- Reports.Read.All

MICROSOFT GRAPH - ONEDRIVE

- User.Read.All
- Sites.Read.All
- Files.ReadWrite.All

MICROSOFT GRAPH - TEAMS

- Group.ReadWrite.All
- Channel.Create
- Teamwork.Migrate.All
- ChannelMessage.Send
- Chat.ReadWrite
- Chat.ReadWrite.All
- ChannelMessage.Read.All
- Sites.Read.All
- Files.ReadWrite.All
- User.Read.All
- ChannelMessage.Read.All
- Sites.FullControl.All

MICROSOFT GRAPH - SHAREPOINT

- Sites.Read.All
- Files.ReadWrite.All
- User.Read.All
- Sites.FullControl.All

OFFICE 365 SHAREPOINT ONLINE

- Sites.FullControl.All

MICROSOFT GRAPH - MANAGEMENT

- ServiceHealth.Read.All
- Group.Read.All
- User.Read.All
- Sites.Read.All
- Reports.Read.All

MICROSOFT GRAPH - AZURE APP

- Directory.AccessAsUser.All
- User.Read
- user_impersonation

CONCLUSION

The goal of this white paper is to educate our customers on how Rubrik secures data with regard to its M365 backup and recovery solution. Security is paramount in today's computing world - hopefully this paper shows how seriously Rubrik takes securing data under its management.

VERSION HISTORY

Version	Date	Summary of Changes
1.0	September 2021	Initial Release
2.0	October 2021	Grammar Updates, Add M365 API Permissions
3.0	August 2022	Additional permissions

rubrik

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

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

rwp0582-m365-architecture-and-security / 20220822