

Rubrik for Microsoft 365

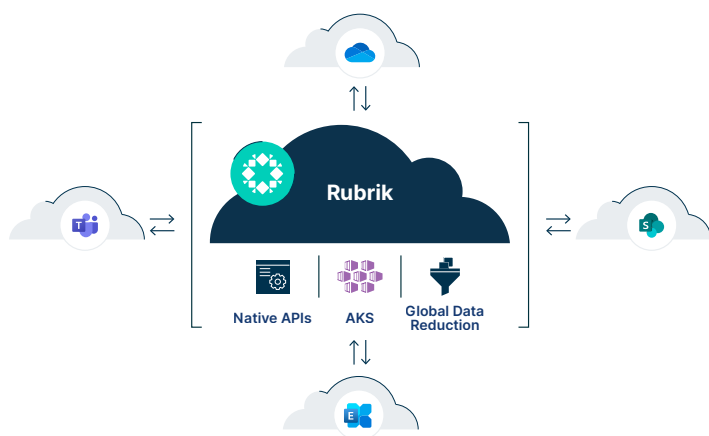
Cyber Resilience and Rapid Recovery at Scale

The modern IT Architect understands the technical requirements and constraints when selecting a solution to protect Microsoft 365 data. In addition to reducing operational costs, enabling employees, and leveraging the agility of cloud, they also take the appropriate steps to secure company data while minimizing recovery times from security incidents or operational mishaps.

These determining factors are underscored by the shared responsibility model of the cloud, which emphasizes the responsibility of the customer to protect data stored within a cloud provider's services. This, and due to the rise of ransomware, make it critical that Microsoft 365 (M365) data remains recoverable in the inevitable event of a ransomware attack or operational error.

RUBRIK SECURITY CLOUD FOR MICROSOFT 365

With Rubrik Security Cloud (RSC), you can keep your data secure, monitor data risk, and quickly recover your data, wherever it lives. Built on a zero-trust architecture, assuming all users, devices, and applications are untrustworthy and can be compromised; the solution offers data protection, data threat analytics, and data security posture and cyber recovery for M365 services such as Exchange Online, OneDrive, SharePoint, and Teams through:



Simplified data resilience with access-controlled, air-gapped, and immutable backup options in Rubrik Cloud Vault (RCV) and Rubrik M365 hosted offering.

Insightful data observability features such as Anomaly Detection and Sensitive Data Monitoring for M365 OneDrive and SharePoint.

Optimized data resilience and data remediation features that leverage elastic resources such as Azure Kubernetes Service (AKS) and Zone-Redundant Storage—managed and automated by Rubrik.

Reduce operational overhead and business risks with a simplified data security solution for Microsoft 365.

CYBER RESILIENCE FOR MICROSOFT 365

Microsoft provides world-class perimeter defenses to keep attackers out of customer environments. From strict access controls and a layered defense-in-depth approach to security, many customers today rely upon the trusted security of the Microsoft Cloud. However, when it comes to cyber disasters, Microsoft states in the M365 documentation that the first step is to verify your backups¹. This is where Rubrik becomes a *critical component* of a robust data security strategy.

Upon deployment of the Rubrik M365 hosted model, Rubrik automates the provisioning of AKS infrastructure and zone-redundant storage to protect and store M365 data—all which is separately stored and supported by Rubrik. This provides a separation of duty, and mitigates the security incident where a customer's credentials are compromised by an adversary.

Additionally, Data Threat Analytics and Data Security Features such as Anomaly Detection and Sensitive Data Monitoring for SharePoint and OneDrive are extended by Rubrik Security Cloud—providing data insights to prepare, and recover, from a cyber attack. Rubrik Anomaly Detection helps determine the scope of a ransomware attack, using machine learning to detect deletion, modification and encryption of data. Rubrik Sensitive Data Monitoring helps customers reduce sensitive data exposure and manage exfiltration risk by discovering sensitive data you have, and more importantly, where it lives.

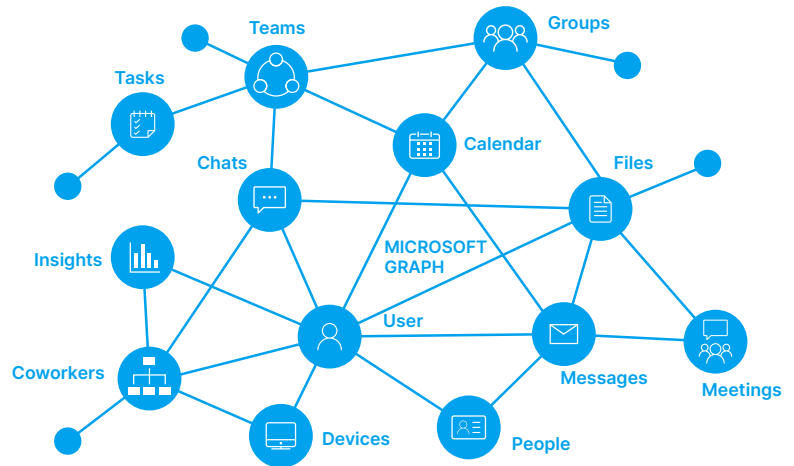
¹ <https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recover-from-ransomware?view=o365-worldwide>

THE RUBRIK SOLUTION AT SCALE

Providing scale to optimize data protection operations in software-as-a-service (SaaS) is a continually moving target that requires a strong foundation in cloud-centric architectures. At the center of these architectures is the ability to leverage the elasticity of cloud, reducing or eliminating bottlenecks, and providing redundancy. This allows the solution to effectively scale up on-demand as needed for large operations, such as recovery.

Even though the compute scaling capabilities are critical to a performant architecture, it is not the only potential bottleneck. In order to interface with the Microsoft environment, Rubrik communicates with M365, via AKS, through multiple Microsoft APIs. The recommended M365 API is known as Microsoft Graph, which provides a single endpoint that allows Rubrik to connect to each of the underlying M365 applications.

Also available are the traditional APIs that are specific to each M365 product—some of which carry advantages over the Microsoft Graph counterpart. Thus, in order to provide both performance and reliability, Rubrik takes a “hybrid” approach in consuming APIs with the ultimate goal of creating the most reliable and performant experience possible. For example, if Microsoft Graph fails during an operation for M365 Exchange, Rubrik can switch to the traditional Exchange Web Services API to complete the task with minimal interruptions in the data protection process.



UNDER THE HOOD OF RAPID RECOVERY

Although mitigating the risk of data loss is paramount, providing the ability to recover quickly is of near-equal importance. For data recovery in SaaS, it means scaling up infrastructure resources to meet demand and efficiently leveraging APIs.

Microsoft provides globally available resources with their cloud infrastructure; as such, they work to ensure each API is consistently available to each of their customers. One way to ensure this is through throttling, and after a certain number of concurrent calls, Microsoft will return an HTTP 429 status code (too many requests) and fail the request. In the context of M365 protection and recovery, this could potentially result in application wait times if too many requests are made.

To design for this, and optimize each round trip, Rubrik will batch multiple queries into a single API request to the Microsoft APIs. Rubrik will also dynamically load-balance API calls through multiple M365 service principles (also known as Enterprise Applications). Each of these Enterprise Applications is specific to individual M365 products (Exchange Mailbox, OneDrive, SharePoint, Teams, etc.) and are automatically provisioned as needed for optimal performance.

CONCLUSION

With the streamlined delivery of the applications, it is clear that the convenience and simplicity of M365 is a welcomed change to many organizations. However, it is still imperative for IT to recognize the need for cyber resiliency, and a well executed data security strategy. With the data services of Rubrik Security Cloud, customers can take advantage of the key benefits of M365, all while keeping their data secure by providing intelligent and accelerated recoveries of their data when ransomware strikes.



Global HQ

3495 Deer Creek Road
Palo Alto, CA 94304
United States

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

Rubrik is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit www.rubrik.com and follow @rubrikinc on X (formerly Twitter) and Rubrik on LinkedIn. Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.

brf-rubrik-for-microsoft-365-technical-brief / 20230913