

Rubrik-Hosted Data Protection for Microsoft 365

As a Tier 1 modern workplace tool, Microsoft 365 is a prime target for cyber attacks. Sixty percent of Microsoft 365 tenants have suffered an account takeover¹, and 81% of Microsoft 365 accounts have seen an email breach². While Microsoft offers world-class tools for data governance, hackers can manipulate retention policies to permanently delete data when global admin credentials are compromised. Litigation hold is designed for eDiscovery search for legal requests, not for restoring lost data at scale. For rapid restores from cyber attacks, organizations need a secure, air gapped solution to strengthen security posture, minimize sensitive data exfiltration risk and help ensure business continuity.

RUBRIK BENEFITS

Secure critical Microsoft 365 data. Help ensure data is resilient, discoverable, and readily accessible.



WITHSTAND CYBER ATTACK

Isolate backups from the Microsoft 365 tenant and solution with an air gap. Grant secure admin privileges and protect from hackers manipulating retention policies to delete production data. Discover and classify sensitive data in Microsoft 365 and beyond. Retain data encryption control with Bring Your Own Key (BYOK).



AUTOMATE PROTECTION AND MANAGE SENSITIVE DATA RISK

Eliminate manual job scheduling and protect new data automatically. Determine sensitive data exposure risk both pre and post-attack. Help ensure classified data exists only where it should, and facilitate compliance with GDPR and other regulations with delegated privileges and Role-Based Access Control (RBAC).



RECOVER RAPIDLY

Find and recover the data you need with fast search and restore. Help expedite remediation efforts by knowing whether files and folders impacted in an attack contain sensitive data. Select data for granular or bulk recovery.

WITHSTAND CYBER ATTACK

Make backups secure. Gain confidence in the ability to restore from a reliable backup copy with WORM-locked immutability, SLA Retention Lock, and Intelligent Data Lock.

- **Help Prevent Unwanted Access:** Multi-factor Authentication (MFA) helps keep attackers out, even if Microsoft 365 admin credentials are compromised.
- **Centralize Protection:** Unify protection and risk monitoring of Microsoft 365 data with other on-prem and cloud workloads. Help reduce data exposure and exfiltration risk by discovering the types of sensitive data in your environment and where it lives across SharePoint sites or OneDrive files and folders.
- **Establish a Secure Connection:** Authenticate with the global administrator role for the protected Microsoft 365 subscription. Industry-standard modern authentication establishes a secure connection.

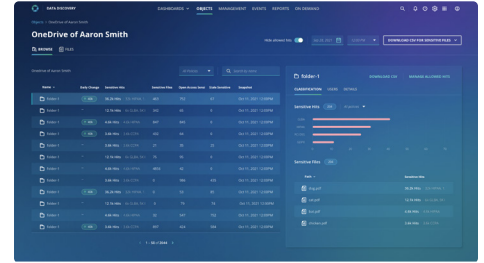
1 <https://www.proofpoint.com/us/blog/threat-insight/dangerous-functionalities-in-microsoft-teams-enable-phishing>

2 <https://pages.egress.com/whitepaper-m365-outbound-email-05-11-uslp.html>

AUTOMATE PROTECTION AND MANAGE SENSITIVE DATA RISK

Secure tens of thousands of users across Exchange Online, OneDrive, SharePoint, and Teams with SaaS-based and policy driven protection. Meet business SLAs with comprehensive Rubrik Security Cloud protection across enterprise, cloud, and SaaS. With Rubrik-hosted protection, a single license includes the software and storage, with fixed, predictable costs. **Enterprise Edition** licensing includes **Sensitive Data Monitoring** of backups for proactive risk mitigation – with minimal production impact.

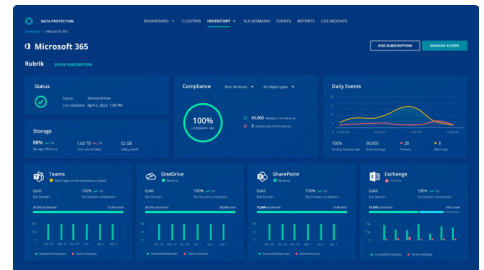
- **Assess Potential Data Exposure Risk:** Use pre-built or custom sensitive data analyzers to continuously monitor backups across categories like PCI, PII, and PHI. Gain insight into what regulatory bodies may need to be notified in an attack based on how sensitive data is classified and where it exists.
- **Easily Onboard New Users, Sites, or Mailboxes:** Meet the demands of a growing environment with automated protection. Automatically discover new users, sites, and teams. Assign protection policies at the application level or according to Microsoft Entra ID (Azure AD) Groups. Designate user permissions for self-service access. Override group SLAs for granular, individual user protection, with multiple daily backups.
- **Ensure Backups are Running:** Eliminate manual job-scheduling with a singular, intuitive dashboard. Check compliance, SLA audits, and recovery tasks. Rely on a fully-automated Rubrik retry mechanism and switching among multiple available Microsoft APIs to automatically handle API failures and errors. Export reports on demand on protection status and how sensitive data is classified and flagged, or set up recurring delivery.



RECOVER RAPIDLY

Avoid the headache of not knowing if files are still retrievable from the Microsoft 365 Recycle Bin—60, 90 days and beyond—or relying on versioning to revert changes and restore data.

- **Quickly Locate Data:** Search for files based on details like keywords, event titles, email subject, author, or date range. Browse point-in-time snapshots. Restore data from both inactive and active users. Find and recover individual files hosting sensitive data. Restore emails, folders, shared mailboxes or an entire OneDrive or site.
- **Perform Fast Backups and Restores:** Minimize RPOs. Boost performance with containers spun-up on demand using Azure Kubernetes Service (AKS) to orchestrate provisioning and deprovisioning. Nodes scale automatically based on workload demands.
- **Restore Data Where it's Needed:** Restore to the original user or another user. Easily recover accidentally-deleted SharePoint lists or recover Teams channel posts to the original Teams channel. Rubrik instances in Azure Blob Storage make API calls to recover to the preferred location.



WHAT OUR CUSTOMERS ARE SAYING

“We are always looking to protect against ransomware and constantly use our backups for file restores and email restores. The only place we can do it all is from Rubrik. Easy restores and they have their file in a matter of minutes.”

Ruddy Cordero, Senior Director of Infrastructure and Operations
Sesame Workshop



“We already had Rubrik for on-prem. It was easy to expand to Microsoft 365. Sensitive Data Monitoring helps us proactively secure where our sensitive data resides and who has access, and can help us identify if data was exposed in an exfiltration attack.”

Andy Powell, CTO
Canterbury Christ Church University



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.

dis-rubrik-hosted-protection-for-microsoft-365 / 20230918