rubrik

Data Security Posture Management (DSPM) for Microsoft 365 Copilot

Reduce the risk of sensitive data exposure for secure Copilot adoption

Organizations are increasingly turning to AI assistants like Microsoft 365 (M365) Copilot to enhance productivity. What makes Copilot such a powerful tool is its ability to leverage content from across an organization to provide accurate and relevant responses.

However, many organizations may not have the data security controls in place to ensure sensitive data remains secure. Common misconfigurations such as mislabeled sensitive files and overly broad access permissions could lead to leakage of your organization's most sensitive data.

To help mitigate this risk, Rubrik offers Data Security Posture Management (DSPM) for M365 Copilot. DSPM allows organizations to reduce the risk of sensitive data exposure by identifying overexposed, mislabeled, and misplaced sensitive data and offering easy, in-app remediation. With Rubrik, IT, Security, and Modern Workplace teams can more easily prepare M365 environments for secure Copilot adoption.

PREPARE YOUR DATA FOR SECURE COPILOT ADOPTION

Automate data discovery and classification so you can more easily find, manage, and secure your sensitive data.

CONTROL ACCESS TO SENSITIVE DATA

Detect and revoke risky permissions such as org-wide and public access to sensitive data with bulk remediation.

REDUCE THE RISK OF SENSITIVE DATA EXPOSURE

Identify missing or incorrect Purview MIP labels and easily remediate at scale, enabling you to restrict user access to sensitive data.

HOW IT WORKS

Discover and Classify Data
Rubrik continuously and autonomously discovers and classifies all known and unknown data—both structured and unstructured—at a very rapid rate.

By utilizing an independent classification engine, Rubrik provides a wide range of supported file types and extends to non-Microsoft systems across on-premises, cloud, and SaaS applications, thereby providing you with a single pane of glass for all of your assets and data.

Apply Purview MIP Labels
Using an independent data classification engine, Rubrik automatically audits and identifies where Microsoft Information Protection (MIP) data sensitivity labels are missing or inaccurate, allowing you to easily apply the correct label at scale from within the Rubrik platform.

This feature helps ensure that all your data is correctly labeled, which is critical for enforcing policies that protect and restrict access to sensitive information.

Revoke Public and Org-Wide Access

Rubrik alerts you to sensitive files that are accessible to anyone with a link (including external entities) or to the entire organization. It then provides an easy way for you to revoke public and org-wide access with one-click bulk remediation in Rubrik Security Cloud.

By reducing overshared access in near real-time, you can secure sensitive data and prevent unauthorized access.

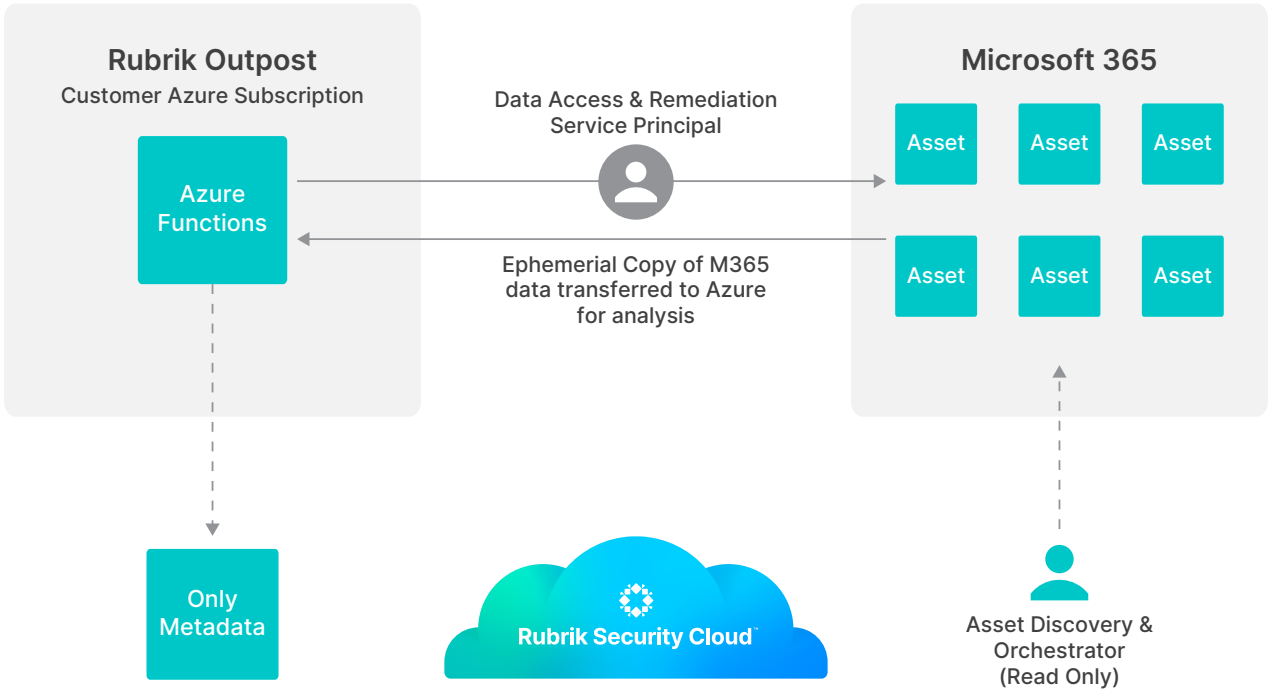
Create Segmentation Policies

With many companies dedicating SharePoint sites to specific purposes and managing access at the site level, Rubrik offers custom policies to help stop the right data from slipping into the wrong site.

Keeping sensitive data in the right site or drive prevents exposure to unauthorized users.

High Level Design (Customer Hosted)

30 minute installation. ~2 week scan time.



To learn more about our integration with Microsoft, visit our partnership page.

rubrik

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

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

ds-dspm-for-m365-copilot / 20250430