EBOOK

MICROSOFT 365 CYBER RESILIENCE

End-to-End Protection for Your Critical M365 Environment

rubrik

Contents

Microsoft 365 (M365) is a critical productivity application for the modern workplace, with more than 400 million[1] paid users worldwide using the platform to collaborate efficiently. However, M365's extensive adoption also subjects it to sophisticated cyber threats, data sprawl, and compliance challenges.

As organizations increasingly rely on M365, the attack surface expands and exposes sensitive data and critical operations to potential breaches. The urgent need for comprehensive protection is underscored by some alarming statistics:

Every day, Microsoft customers face 600 million cyber attacks, or 54 per second.

(source: Microsoft Digital Defense Report)

Identity-based attacks increased 10x in 2024 alone

(source: Microsoft Digital Defense Report)

40% of organizations have postponed implementing M365 Copilot by three months or more due to data security concerns.

(source: Gartner)

Average cost of a data breach $4.88 million

(source: IBM Cost of a Data Breach 2024)

Rubrik understands the importance of comprehensive M365 security. Rubrik Security Cloud is integrated with Data Security Posture Management (DSPM) capabilities that go beyond traditional backup solutions to include robust security, governance, and rapid recovery features. Rubrik delivers unparalleled visibility into your sensitive data—where it lives, who has access to it— and ensures swift recovery in the event of a cybersecurity incident.

With Rubrik,your organization can proactively address these challenges by enhancing your security posture before an attack, ensuring seamless recovery to quickly restore business operations.

With Rubrik, IT and Security leaders have confidence in their ability to safeguard their M365 environments against evolving cyber threats, ensuring continuous protection and resilience. This ebook will help you understand how Rubrik can help you protect your sensitive M365 data—before, during, and after an attack.

BEFORE AN ATTACK

Strengthen Your Security Posture

Right now, malicious actors could be scanning your environment— identifying publicly exposed sensitive data, targeting over-permissioned accounts, gaining access to data, and mapping your on-prem and Azure cloud applications for vulnerabilities.

Bad actors may be busy surveying your vulnerabilities, but they typically remain undetected in environments for weeks or months before launching an attack. They patiently gather intelligence and drop attack tools in strategic locations without your knowledge. This helps them establish persistence mechanisms and move laterally throughout your environment to maximize impact when they finally strike.

So what can you do about this?

Data Discovery and Classification

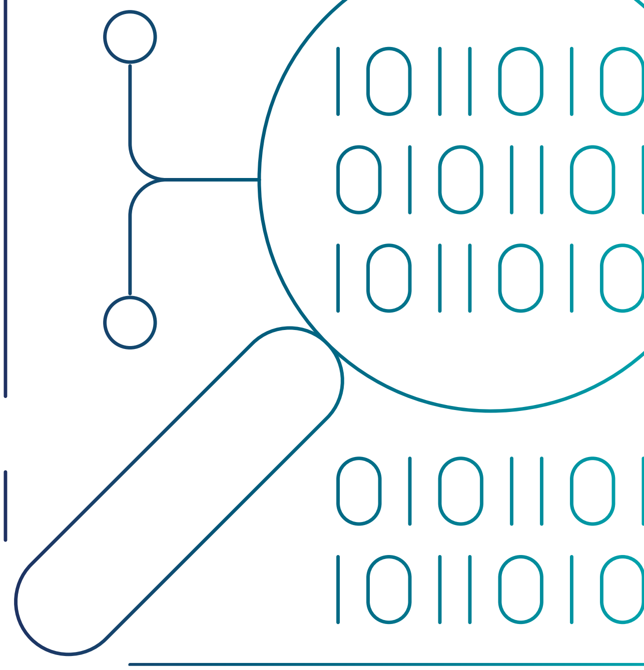
- Autonomously discovers and classifies sensitive data across SharePoint, and OneDrive without agents
- Provides in-app remediation of missing or incorrect labels to enforce proper data governance
- Validates M365 environment readiness for secure adoption of AI tools like Copilot by ensuring proper data controls

Data Risk Management

- Reduces exposure risk by identifying and enabling remediation of organization-wide and public share permissions that attackers frequently target first
- Automatically validates that sensitive data resides only in authorized M365 locations, preventing “shadow IT” vulnerabilities

Data Access Governance

- Provides comprehensive visibility into who has access to sensitive data across M365 services
- Detects over-permissioned accounts that attackers often target for credential harvesting
- Enables organizations to effectively manage corporate access policies and least privilege principles, reducing potential attack vectors



DURING AN ATTACK

Detecting & Responding to Threats

When an attack is under way, threat actors are likely to use all the tricks of the trade to make sure their incursion is successful. They'll be phishing your staff to gain access to sensitive data. They'll use compromised credentials to sneak into privileged networks undetected. They'll exploit software vulnerabilities to gain access, then quietly expand their footprint across your M365 environment—escalating privileges and preparing for data encryption or exfiltration.

So how should you respond during the heat of a cyber attack?

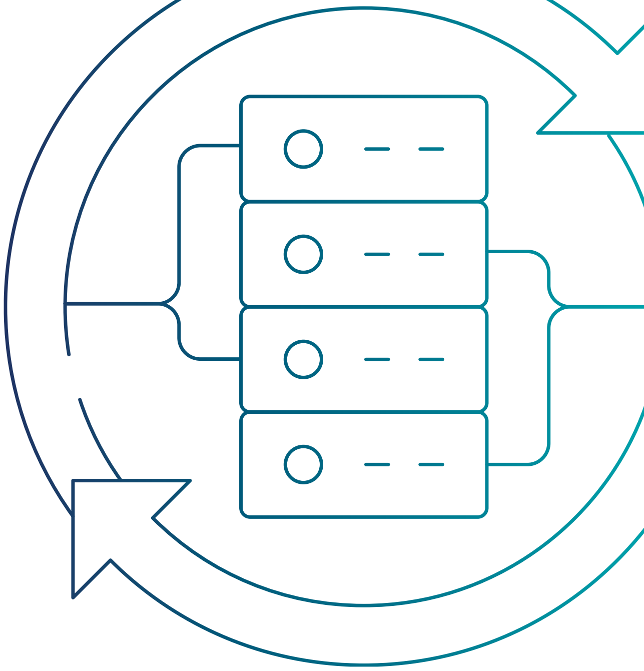
How Rubrik can help:

Threat Monitoring and Anomaly Detection

- Alerts security teams to traces of an attack while attackers are still in discovery mode, by automatically scanning for known exploits and attacker tools.
- Alerts security teams to abnormal data behavior (such as sudden file modifications or permission changes) through integration with SIEM and XDR platforms
- Utilizes AI/ML to establish behavioral baselines and detect unusual data access patterns to determine the blast radius of the attack.
- Monitors for unauthorized access, mass encryption attempts, and suspicious activity without production impact
- Creates a time-series view of data changes to pinpoint exactly when attackers first breached your environment

Threat Hunting and Clean Recovery

- Turbo Threat Hunting scans up to 75,000 backups in seconds to precisely identify when attackers first compromised your systems
- Provides full-context forensic investigation with timeline insights to map the attacker's movement through your environment
- Determines attack scope and point of infection without requiring production systems to be online
- Recovers clean backup copy
- Prevents reinfection by isolating and quarantining compromised files before recovery, breaking the attack chain



AFTER AN ATTACK

Recovering and Restoring Business Operations

Just because an active attack is over doesn't mean the threat disappears. Your perimeter may be restored, but bad actors may persist in your environment. They may deploy ransomware to encrypt critical files or exfiltrate sensitive data for extortion. They may attempt to delete or corrupt backups and make every effort to retain access even after initial discovery.

So what do you do once you thwart an active attack to return to a safe and stable environment?

How Rubrik can help:

Prioritized Recovery

- Orchestrates intelligent recovery based on business criticality and sensitive data classification
- Enables granular restore of specific users, files, or entire sites without requiring full restoration
- Supports flexible restoration to the same or alternate account in the same or alternate tenant, providing greater recovery options during compromise scenarios
- Reduces recovery time by up to 100x compared to traditional methods through automated workflows, minimizing business downtime and financial losses

Zero Trust Security and Immutable Backups

- Provides air-gapped, immutable backups that prevent attackers from encrypting or deleting your recovery resources
- Enforces strict role-based access control (RBAC) with separate control plane architecture to prevent attackers from compromising your recovery capabilities
- Maintains comprehensive audit logging of all access and recovery actions to detect any unauthorized attempts to manipulate backups
- Supports customizable retention policies that align with regulatory requirements and cannot be altered even by attackers who gain administrative access

Why You Must Secure Your M365 Environment Right Now

Cyber threats loom larger than ever, so protecting your Microsoft 365 environment is not just an option—it's a necessity. The urgency to safeguard M365 data arises from a complex threat landscape, characterized by advanced ransomware and wiper malware attacks. These malicious entities are not merely content with breaching surface-level defenses; they aim to penetrate backup systems, where they can inflict the most damage.

The reality is stark—Microsoft's shared responsibility model leaves a substantial burden on customers to protect their own data. This model presents significant data protection gaps, with native recovery options often being insufficient, possibly extending downtime from mere days to debilitating weeks.

Moreover, the compliance landscape for organizations is becoming increasingly stringent. Regulatory requirements around data protection, breach reporting, and recovery capabilities are intensifying, with potential fines for non-compliance reaching up to 4% of global revenue. This regulatory pressure compounds the need for a resilient data protection strategy.

Adding another layer of complexity is the rapid adoption of Artificial Intelligence (AI) tools, such as Microsoft Copilot. While these tools promise to elevate business processes, improper data visibility, labeling, and access controls could inadvertently increase the risk of sensitive data exposure, thereby amplifying the threat landscape both internally and externally.

How Rubrik Can Help

The best option is to address these challenges head-on, deploying an advanced data protection solution like Rubrik. With Rubrik, you get complete visibility across all M365 workloads, transforming the cumbersome task of data inventory from a weeks-long endeavor into a process that takes mere minutes. Furthermore, Rubrik arms organizations with cyber-resilient protection, through immutable backups, proactive risk reduction, early threat detection, and rapid recovery capabilities. Rubrik can significantly minimize the impact of a breach, reducing both downtime and data loss.

Rubrik can also help enterprises to navigate the intricate maze of regulatory requirements. By automating retention policies, minimizing sensitive data exposure, and facilitating audit processes through comprehensive reporting, organizations can confidently meet their compliance obligations.

Rubrik can also help with the secure adoption of AI technologies, including Microsoft Copilot. By   meticulously labeling sensitive data, Rubrik can help you mitigate the risks associated with AI getting access to the wrong data sets. Proper data labeling plays a significant role in the safe and effective deployment of AI.

In sum, Rubrik stands as an indispensable ally in an organization's quest to protect, manage, and leverage their M365 data amidst an increasingly perilous cyber threat landscape.

rubrik

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

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

Rubrik (NYSE: RBRK) 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.

microsoft-365-cyber-resilience / 20250624