



Rubrik Data Protection for M365

Proactive defense and resilience against cyberattacks

Attacker's Actions

Before an Attack

Rubrik's M365 Data Protection

Attack Preparation / Reconnaissance



Identity compromise initiates most attacks, letting adversaries persist undetected for months while exploiting vulnerabilities;

90% of organizations faced an identity-related incident last year.

- Scans your environment for vulnerabilities.
- Identifies publicly exposed sensitive data.
- Targets over-permissioned accounts.
- Gains access to data.
- Maps your on-prem and Azure cloud applications.
- Lurks undetected for weeks or months.
- Establishes persistence mechanisms.

Proactive Protection / Strengthening Security Posture



Rubrik's Data Access Governance (DAG) provides visibility into sensitive data and access, reducing attack surface by remediating over-permissioned accounts and enforcing least privilege.

- Autonomously discovers and classifies sensitive data across SharePoint and OneDrive without agents.
- Remediates missing or incorrect data labels to enforce proper data governance.
- Identifies and remediates targeted public and organization-wide share permissions.
- Provides M365 sensitive data access visibility.
- Ensures M365 data controls enable secure AI adoption (e.g., Copilot).
- Validates M365 environment readiness for secure adoption of AI tools like Copilot by ensuring proper data controls.

Attacker's Actions

During an Attack

Rubrik's M365 Data Protection

Attack Execution / Exploitation



Attackers exploit vulnerabilities to gain initial access, then expand their footprint, escalate privileges, and prepare for data encryption or exfiltration. Microsoft has

reported a tenfold increase in identity-based attacks in early 2024 alone.

- Exploits access gained via phishing scams, compromised credentials, or vulnerable software.
- Escalates privileges and expands attack footprint across your M365 environment.
- Prepares for data encryption or exfiltration.

Threat Detection and Response



Rubrik integrates with SIEM/XDR to alert on abnormal data behavior, facilitating full-context forensic investigation with time-series insights to pinpoint breaches, and supporting OneDrive/SharePoint anomaly detection.

- Alerts security teams to any trace of an attack while attackers are still in discovery mode.
- Uses AI/ML to establish behavioral baselines and detect unusual data access patterns, determining the blast radius of the attack.
- Monitors for mass encryption attempts, unauthorized access, and suspicious activity without production impact.
- Scans thousands of backups (up to 75,000 in seconds) to precisely identify when attackers first compromised your systems.
- Recovers clean backup copy.
- Prevents reinfection by isolating and quarantining compromised files before recovery.

Attacker's Actions

After an Attack

Rubrik's M365 Data Protection

Post-Attack Persistence / Damage and Extortion



Attackers deploy ransomware, exfiltrate sensitive data, attempt to delete or corrupt backups, and maintain persistence. There has

been a 275% YoY increase in ransomware attacks on Microsoft customers. These attacks can lead to data loss and ransomware.

- Deploys ransomware to encrypt critical files.
- Exfiltrates sensitive data for extortion.
- Attempts to delete or corrupt backups.
- Maintains persistence mechanisms to lay the foundation for future attacks.

Recovery and Resilience / Restoring Business Operations



Rubrik enables rapid, prioritized recovery in hours, not days, offering a comprehensive RTO for data and identity to ensure M365 service availability post-incident.

- Provides air-gapped, immutable backups that prevent attackers from encrypting or deleting your recovery resources.
- Orchestrates intelligent recovery based on business criticality and sensitive data classification, beginning with the most critical functionality.
- Enables granular restoration of specific users, files, or entire sites without requiring full restoration.
- Orchestrates full recovery of Active Directory and Entra ID.
- Supports multiple restore options to provide flexibility during compromise scenarios, including restoration to the same or alternate account/tenant.
- Automated workflows cut recovery times by up to 100x, vastly minimizing business downtime. Maintains comprehensive audit logs of all access and recovery actions to detect any unauthorized attempts to manipulate backups.
- Rolls back to a clean, malware-free state to combat attacker persistence.

Rubrik Security Cloud is one platform to consolidate point products for Data Security Posture Management, Cyber Recovery, and Identity Recovery.

Key Benefits



Complete M365 Visibility

Get a comprehensive, continuously updated inventory of sensitive data across all M365 workloads.



Cyber Resilient Protection

Reduce breach impact with immutable backups, proactive risk reduction, early threat detection, and rapid recovery capabilities.



Enterprise-Scale Compliance

Automatically enable retention policies, reduce sensitive data exposure, and generate reports for audit and regulatory requirements.



Secure AI Adoption

Accelerate secure deployment of Microsoft Copilot and other AI tools by ensuring sensitive data is labeled with correct access controls. Rubrik minimizes sensitive data exposure risk.

Watch M365 Storylane Demo



"With Rubrik, you don't just recover data—you recover your business".