End-to-End M365 Cyber Resilience

Partner Marketing Playbook

Version 1.0
August 2025

rubrik

Why Now/Market Conditions

Microsoft 365 is a critical productivity engine and, unfortunately, a prime cyber attack target.
While Microsoft secures the infrastructure, your organization is responsible for protecting its M365 data and identities.

Identity Compromise

Attacks frequently start with identity compromise. **90%** of organizations have experienced an identity-related incident in the past 12 months.

Ransomware Increase

There has been a **275%** YoY increase in ransomware attacks on Microsoft customers, often ending with data loss and ransomware.

Severe Consequences of Data Loss

Losing M365 data or suffering identity compromise risks **operational paralysis**, data breaches, regulatory penalties, cyber insurance issues, and eroded board confidence.

Native Gaps & Limited Recovery

Microsoft's native tools lack the security, granularity, and orchestration required for rapid recovery, especially for identity. **Incident recovery can take weeks to months.**

Emerging Risks

AI tools like Copilot could inadvertently access **overexposed sensitive data** if posture isn't managed, turning productivity tools into liabilities.

End-to-End Cyber Resilience is required, unifying Cyber Posture (reducing attack surface) and Cyber Recovery (ensuring quick service restoration).

Core Messaging

Rubrik delivers complete M365 cyber resilience by unifying M365 Cyber Recovery, Automated Risk Mitigation, and Orchestrated Entra ID Recovery on a single platform.

- Discover, classify, and monitor sensitive data. Discover and remediate risky identities with sensitive data access.
- Restore AD/Entra ID across hybrid environments in mere hours—on one air-gapped platform.
- 100x faster clean recovery without re-infection. Air-gapped. Recover faster with prioritized recovery.

100-word option

With Rubrik, CISOs gain the resilience to maintain business continuity, reduce downtime, improve compliance readiness, and confidently adopt innovations like Microsoft Copilot—while demonstrating provable security posture to boards, regulators, and insurers. Rubrik addresses the full spectrum of M365 risks: ransomware, insider threats, accidental deletion, overexposed sensitive data, and identity compromise. Rubrik delivers complete M365 cyber resilience by unifying data and identity protection on a single platform. For CISOs, this means much more than backup—it's a comprehensive solution with immutable backups, advanced recovery orchestration, proactive data security posture management (DSPM), and orchestrated AD/Entra ID identity recovery.

Value Proposition

End-to-End Cyber Resilience unifies Cyber Posture (reducing attack surface) and Cyber Recovery (ensuring quick service restoration). This means that Cyber Resilience = Cyber Posture + Cyber Recovery.

Cyber Posture
+ Cyber Recovery
= Cyber Resilience

Introducing Rubrik for M365: End-to-End Cyber Resilience

Rubrik Security Cloud delivers End-to-End Cyber Resilience by providing a unified platform to consolidate point products and drive savings. With Rubrik, you gain:

- **Reduced Exfiltration Risk:** Detects and remediate sensitive data exposure and access.
- **M365 Service Availability:** Achieve fast, clean recovery of M365 and Entra ID to get back up and running quickly after a cyber incident.

This comprehensive solution integrates Data Security Posture Management, Cyber Recovery, Identity Recovery, and Data Protection capabilities.

The 3 Pillars of End-to-End Cyber Resilience for M365

Rubrik Security Cloud provides comprehensive end-to-end cyber resilience for M365 through three core pillars:

1

Automated Risk Mitigation for Cyber Posture

This pillar focuses on reducing your attack surface and protecting sensitive data within M365:

Data Security Policy Automation

Apply built-in or custom data policies to minimize unauthorized or accidental data exposure. This includes policies for overexposed data (e.g., company-wide accessible personal data, SSN, CC #, DOB) and misconfigured data (e.g., missing confidential MIP labels).

Data Classification

Classify sensitive data at scale, including historical data, and leverage AI to classify documents based on business context. This supports classifications like Confidential, General, and Public and integrates with Purview & MIP.

Data Access Governance

Discover risky identities with sensitive data access, visualize access graphs, and receive alerts on over-privileged identities to revoke permissions effectively.

Over-exposure Remediation

Automatically remove links to publicly shared and organization-wide shared sensitive data, and trigger Auto MIP labeling when violations are detected.

2

Orchestrated Identity Recovery for Service Availability

This pillar ensures the rapid and clean recovery of your critical identity infrastructure:

Comprehensive Identity Recovery

Recover essential Entra ID objects, including users, groups, roles, Enterprise Apps, App Registrations, and Conditional Access Policies.

Rapid Clean Forest Recovery

Quickly restore entire forests, trees, and domain controllers in a streamlined 5-step process.

Restitch Entra ID

Re-establish relationship mappings and updates to ensure Entra ID and M365 are aligned, and re-associate on-prem AD and Entra ID.

Hybrid Recovery

Recover both AD and Entra ID across hybrid environments to a clean state within minutes, including all interdependencies.

3

M365 Cyber Recovery for Service Availability

This pillar focuses on fast, clean recovery of your M365 data and proactive threat management:

M365 Prioritized Recovery

Recover in hours by prioritizing the most important users and data first.

Threat Monitoring/Anomaly Detection

Identify potential threats and anomalous behavior before they escalate.

Threat Hunting

Eliminate indicators of compromise (IOCs) by scanning for and identifying them, and quarantining infected data.

Unified Cyber Resilience Platform

Confidently navigate ransomware, mass deletion, and compliance challenges from a single, integrated platform.

Customer Challenges

Accidental Deletions & Human Error

Admin mistakes or bulk updates lead to lost/corrupted records.

Cyber Threats & Mass Deletion

Attackers gaining unauthorized access to perform widespread data deletion.

Identity Compromise

Primary AD/Entra ID attack vectors make data backups useless if users cannot authenticate.

Compliance Risks

Native retention policies fail to meet long-term regulatory requirements.

Data Exposure

Sensitive data overexposed via public links or organization-wide sharing leads to breaches.

Native Tool Gaps

Limited built-in recovery options lack immutability, air-gap security, and orchestration.

Key Personas & Pain Points

PERSONA	KEY GOALS	PAIN POINTS
CIO/CISO	• Ensure overall business continuity and minimize downtime for M365 in the face of catastrophic cyber events. • Establish a robust strategy for data governance, compliance, and cyber insurance readiness. • Proactively reduce the risk of data breaches, exfiltration, and regulatory penalties. • Confidently demonstrate a provable security posture to the board, regulators, and insurers. • Enable the secure adoption of emerging technologies like Microsoft Copilot. • Protect and rapidly recover critical identity infrastructure (Active Directory, Entra ID).	• Risk of complete business paralysis from Active Directory (AD) or Entra ID compromise (identity is the #1 attack vector). • Severe financial and reputational damage from sensitive data breaches and exfiltration. • Exposure to non-compliance penalties (e.g., GDPR, CCPA) due to inadequate data protection. • Inability to satisfy stringent cyber insurance prerequisites for M365 coverage. • Difficulty in providing clear, provable resilience assurance to executive boards. • Security concerns and lack of visibility hindering the secure deployment of AI tools like Copilot. • Managing the inherent complexity and heightened risk of hybrid identity infrastructure (on-prem AD and Entra ID).
Director	• (IT Manager, Director of Business Applications, Director of IT) • Ensure M365 service uptime and meet critical Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). • Manage operational risks related to M365 service availability. • Implement early threat detection and response mechanisms for M365. • Gain initial visibility into sensitive data exposure. • Efficiently scale data protection as the M365 footprint grows.	• Significant business downtime and operational paralysis after larger incidents. • Failure to meet stringent RTO/RPO mandates for M365 data. • Slow identification of ransomware, mass encryption, or malicious deletion events within the M365 environment. • Uncertainty about the blast radius and scope of sensitive data compromise during an attack. • Difficulty in scaling protection efficiently and cost-effectively as M365 usage expands.
M365 Admin	• Ensure reliable and efficient daily backups of M365 data. • Simplify recovery processes for common data loss scenarios. • Reduce manual effort and time spent on restore requests. • Maintain consistent data retention policies across M365 applications.	• Time-consuming manual checks for backup completion and integrity. • Limitations and recovery failures with native M365 tools (e.g., Recycle Bin). • High volume of user requests for file and email restores. • Difficulty in consistently applying and enforcing retention policies across diverse M365 workloads.

Rubrik's Differentiated Capabilities (Expanded & Layered)

M365 Immutable Backup (aka Foundation Edition)

- Immutable, logically air-gapped backups stored securely in Rubrik Cloud Vault or BYO storage.
- Policy-based automation (SLAs) with auto-discovery of new users/sites.
- Unified platform for M365 and other workloads.
- Flexible granular (file, email, object) and mass recovery capabilities.

Cyber Recovery (aka Enterprise Edition)

- **Prioritized Recovery:** Orchestrated workflow restores critical data first based on user priority or time sensitivity (e.g., last 14 days for exec mailboxes, most recent SPO/Teams data), enabling 1-3 day operational recovery vs. weeks/months for full restore.
- **Anomaly Detection:** ML algorithms analyze backup metadata patterns to identify potential ransomware activity, mass deletions, or unusual file modifications in OneDrive/SharePoint, providing early warnings.
- **Threat Monitoring and Threat Hunting:** Determine attack scope by analyzing backups for malicious changes (deletions, modifications, encryptions); identify IOCs using integrated threat feeds to pinpoint clean recovery points and prevent reinfection. Rubrik Turbo Threat Hunting is the first and only such solution in the market that can scan up to 75,000 backups in under 60 seconds, helping organizations – after an incident– know where malware is, when it matters most.
- **Data Discovery and Classification (in Backups):** Automated analysis of backup data to identify locations of sensitive information (PII, PCI, PHI, custom patterns) for risk assessment and incident response context.
- **Self-Service Recovery:** Securely delegate restore capabilities (in-place only) for Exchange and OneDrive to end-users via SSO, reducing IT helpdesk workload while maintaining control.

Data Security Posture Management

- Continuous discovery and classification of sensitive data in live M365 environments (SharePoint, OneDrive) using >65 built-in policies or custom analyzers.
- Identifies overexposed sensitive data via public or organization-wide sharing links.
- Automatically audits and facilitates correction of missing/incorrect Microsoft Information Protection (MIP) sensitivity labels at scale.
- Enforces user-defined data segmentation policies (e.g., prevent finance data in marketing sites).
- Identifies stale/redundant data.
- Provides visibility needed for secure Copilot/AI adoption.

Identity Recovery

- Secure, immutable, air-gapped backups for AD (Forests/Domains/Objects including GPOs/Attributes) & Entra ID (Users, Groups, Roles, Enterprise Apps, App Registrations, Conditional Access policies*).
- Orchestrated AD Forest Recovery simplifies the complex ~20+ step Microsoft process into a guided workflow, enabling faster recovery to a clean environment.
- Live AD Object Comparison identifies changed attributes for granular restore or posture analysis.
- Streamlined Hybrid Recovery provides a unified process for restoring intertwined AD/Entra environments.
- All protected by Zero Trust architecture (immutability, air gap, encryption, RBAC, optional Retention Lock/Quorum).

Campaign Messaging

Campaign	Achieve complete end-to-end M365 cyber resilience before, during, and after an attack through a single platform.
Perception	Perception: Native Microsoft 365 tools and legacy backup solutions are sufficient for protecting M365 data and ensuring business continuity.
Reality	M365 is a primary target for sophisticated attacks, including ransomware and identity compromise, with 275% year-over-year increase in ransomware attacks on Microsoft customers and 90% of organizations experiencing identity-related incidents. Native tools lack the immutability, granularity, and orchestration required for rapid recovery, especially for identity, and recovery after major incidents can take months. A layered defense is essential, encompassing secure backups, operational recovery intelligence, proactive data security, and identity resilience.
Value Prop	Rubrik delivers complete M365 cyber resilience by protecting both data and identity on a single platform. This comprehensive solution provides immutable backups, advanced recovery orchestration, proactive data security posture management (DSPM) to address overexposed sensitive data and compliance, and orchestrated AD/Entra ID identity recovery. Rubrik helps CISOs minimize risk, ensure business continuity, and confidently navigate ransomware, insider threats, accidental deletion, and compliance challenges, even enabling secure adoption of innovations like Microsoft Copilot.

Key Messages and Rally Cries

CYBER POSTURE

- **Sensitive Data Classification:** Discover, classify, and monitor sensitive data. Fills in Purview's blind spots.
- **Overexposed Data Access:** Ensure right users have the right access to the right data. Accelerate Copilot prep.

CYBER RECOVERY

- **M365 Prioritized Recovery:** Recover 100x Faster.
- **Entra ID Recovery:** Fast recovery of identity provider without reinfection. Ensure ability to log-in.

COMPLETE CYBER RESILIENCE

Cyber Posture + Cyber Recovery

Resources

The following content is available to help you and your customers learn about Rubrik End-to-End Cyber Resilience for M365.

Customer-Facing Assets:

Blog

Unlocking M365 Cyber Resilience: Rubrik's Data Threat Analytics and Advanced Recovery Options

Ebook

End-to-End Protection for Your Critical M365 Environment

Webinar

Achieving End-to-End Cyber Resilience with Microsoft 365 Webinar

Securing M365 Data and Identity Systems Against Modern Adversaries

Web Page

End-to-End Cyber Resilience for Microsoft 365

Partner-Facing Assets:

M365 – Partner FAQ

M365 – Battlecard

M365 – Pitch Deck

M365 Partner Email Templates

Buyer's Journey

Awareness/Education → **Consideration** → **Conversation**

Blog

M365 Under Siege: Why Your Business Needs End-to-End Cyber Resilience

Infographic

M365 Attacks vs Rubrik Infographic Landing Page

DSPM for M365 Infographic Landing Page

Ebook

Unlocking M365 Cyber Resilience: Rubrik's Data Threat Analytics and Advanced Recovery Options

Webinar

Securing M365 Data and Identity Systems Against Modern Adversaries

Achieving End-to-End Cyber Resilience with Microsoft 365 Webinar

Next-Gen SaaS Data Protection: M365

White Paper

End-to-End Protection for Your Critical M365 Environment

Bulletproof Your Microsoft 365 Data

DEMO

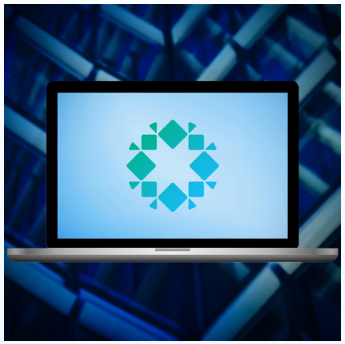
Storylane M365 with DSPM

Storylane M365 with E2E

Build an Integrated Marketing Campaign

Need ideas for how to structure your campaign? The following blueprint can be used to help you develop a multi-touch marketing program that moves prospects through the buyer's journey.

Sample Flow

Awareness	Interest	Consideration	Evaluation
Gartner Analyst Report	On-Demand Webinar	Camp Rubrik	Case Study
			
Gartner® Magic Quadrant™	Achieving End-to-End Cyber Resilience with Microsoft 365 Webinar	M365 with DSPM	St. Luke's University Health Network

Reach out to your CDM or Marketing Representative to customize an integrated campaign to deliver the best results with your accounts.

Discovery Questions & Personas

CISO/CIO

- How do you ensure overall M365 business continuity and minimize impact from catastrophic events like ransomware or identity compromise?
- What is your strategy for M365 data governance, compliance, and cyber insurance readiness?
- How confident are you in demonstrating a provable M365 security posture to your board, regulators, and insurers?
- How do you protect against and recover from Active Directory (AD) or Entra ID compromise, which is a primary attack vector?
- In the event of an M365 attack, how quickly can you definitively answer:
  - » Was identity breached, and where?
  - » Was sensitive data exfiltrated?
  - » Do we need to initiate a recovery, and if so, what's the prioritized recovery plan and estimated timeline?

Directors of Business Applications/IT

- How quickly can you restore critical M365 services after a major incident, and are you consistently meeting your RTOs/RPOs?
- What is your strategy for proactive threat detection, specifically for ransomware, within your M365 environment?
- What are your main challenges in ensuring M365 service availability and managing the initial stages of security response during an incident?
- How critical is Microsoft 365 to daily operations, and which M365 applications are most vital to your business?
- In the event of an M365 attack, what is your team's process to quickly determine:
  - » If identity was breached and which users were impacted?
  - » If sensitive data was exfiltrated?
  - » What was impacted, and what is the scope of recovery?
  - » The required recovery actions, including prioritization and estimated recovery time?

M365 Admins

- What critical business processes rely on M365?
- How quickly can you recover M365 services after a larger incident, and are you meeting your RTOs/RPOs?
- What is your strategy for detecting potential threats like ransomware early within your M365 environment?
- Do you have initial visibility into sensitive data exposure across your M365 data?
- How do you manage operational risks related to M365 service uptime and the initial stages of security response?
- What are your pain points regarding business downtime after incidents, or scaling protection efficiently as your M365 footprint grows?
- How critical is Microsoft 365 to your organization's daily operations and overall business strategy? Which specific M365 applications are most vital?
- What challenges, if any, do your IT teams face in managing and protecting the M365 environment?