



NEWS RELEASE

New Microsoft and Rubrik Integration Delivers Complete Identity Attack Response

2026-03-23

Microsoft Defender and Rubrik Identity Resilience create a unified detection-to-recovery offering; customers achieve trusted recovery in hours instead of days

SAN FRANCISCO--(BUSINESS WIRE)-- Rubrik (NYSE: RBRK), the security and AI operations company, today announced a new integration with Microsoft Defender at RSAC 2026, enabling organizations to move from identity threat detection to rapid remediation and trusted recovery. The integration connects Microsoft's real-time identity threat detection with Rubrik's automated identity rollback and recovery capabilities, helping organizations respond faster to identity-based attacks.

Identity has become the primary target for modern cyberattacks. According to Rubrik Zero Labs research, **90% of IT and security leaders** say identity-driven cyberattacks are their organization's top concern. Yet most security tools stop at detection, leaving organizations to manually investigate malicious changes and restore compromised identity systems.

"Detection is only half of the battle," said Anneka Gupta, Chief Product Officer at Rubrik. "Organizations need the ability to quickly and surgically reverse malicious identity changes and completely restore their infrastructure. By combining Microsoft Defender's threat detection with Rubrik Identity Resilience, we give security and IAM teams the power to move from a detected compromise to a trusted, recovered state in hours, instead of days."

With this integration, organizations can extend Microsoft Defender detections directly into Rubrik's identity recovery workflows, allowing teams to investigate incidents, reverse malicious identity changes, and restore trust

across hybrid environments.

Joint Rubrik and Microsoft Defender customers can now:

- Understand attack impact faster by correlating threat alerts with identity changes.
- Reverse malicious identity modifications without performing full domain restores.
- Restore trusted identity states using immutable recovery points.
- Maintain visibility across hybrid identity environments, including Active Directory and Entra ID.

The integration builds on Rubrik's continued investment and broader vision for Identity Resilience, focused on ensuring identity systems remain trusted, available, and recoverable in the face of cyberattacks, operational disruptions, and evolving compliance requirements.

Over the past 15 months, Rubrik has rapidly expanded its identity capabilities, introducing recovery for Active Directory and Entra ID, expanding protection to multi-identity provider environments including Okta, and launching Identity Resilience capabilities that help organizations investigate incidents and reverse malicious changes. The company has also expanded ecosystem integrations with leading security platforms including CrowdStrike Falcon Identity Protection and now Microsoft Defender, connecting threat detection with automated remediation and trusted recovery.

For more on how Rubrik is redefining identity security, read more [here](#).

About Rubrik

Rubrik (NYSE: RBRK) is the Security and AI Operations Company. The company's data security platform secures and recovers data from cyber threats and operational disruptions. Rubrik has been recognized as a Leader in the Gartner® Magic Quadrant™ for Enterprise Backup and Recovery Software Solutions for two consecutive years and is trusted by over 6,600+ customers across the globe, including world-renowned enterprises and government organizations. For more information, visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter).

Media Contact

Meghan Fintland
Head of Global PR
925.785.9192
press@rubrik.com

Source: Rubrik