

Rubrik for Microsoft Defender:

An Integrated End-to-End Identity Resilience Solution

Keep systems secure, operational, and recoverable by combining Microsoft Defender's proven identity threat detection with Rubrik's clean and current identity recovery



Identity is a primary attack vector. Rather than breaking in through technical exploits or file injections, attackers simply log in using valid credentials; for example, [97%](#) of identity attacks are password-based. Once inside, adversaries blend in and escalate privileges. Ultimately, attacks impact identity system integrity and users can't access critical resources. Despite [90%](#) of IT and security leaders citing these threats as their greatest risk, incident response is often crippled by legacy tools and fragmented, manual workflows. This siloed approach, in which detection, remediation, and recovery are managed in isolation, creates avoidable friction that slows organizational response, extends attacker dwell time, and increases the likelihood of long-term attacker persistence.

The unified Identity Resilience solution between Microsoft Defender and Rubrik Identity Resilience closes this gap.

A Better Way: A Streamlined Identity Attack Response

Together, Microsoft Defender and Rubrik Identity Resilience deliver an integrated approach to identity security, spanning detection, containment, investigation, remediation, and clean recovery.



Microsoft Defender

Detect and respond to advanced identity cyberthreats across your identity fabric.



Rubrik Identity Resilience

Get context and historical activity visibility into identity changes. Correlate activity across systems. Enable precise restore of affected identity objects or full recovery. Remove attacker persistence and roll forward sanctioned identity changes so that you don't lose months of work.

End-to-End Identity Attack Response



Detect

Behavioral anomalies, suspicious session activity



Contain

Enforce token revocation & policy implementation



Investigate

Correlate identity attack timelines



Remediate

Undo malicious changes



Recover

Restore IdPs to backdoor-free state, with zero data loss

Microsoft Defender + Rubrik Identity Resilience: Better Together

Value Drivers	Operational Levers
 Unified Visibility, Deep Context, & Faster Investigation Combine Microsoft's real-time detection with Rubrik's identity activity logs. Keep systems secure and easy to govern. Simplify compliance with an immutable system of record.	 Correlated Intelligence & Forensics Rubrik ingests Microsoft's alerts and maps them to time-sequenced identity activity logs. This allows teams to pinpoint malicious changes and map the blast radius.
 Operational Continuity & Trusted Restore Reduce downtime from days or weeks to just hours. Recover identity infrastructure to a trusted state without disrupting business operations.	 Real-Time Containment & Surgical Recovery Stop active threats by blocking anomalous identity behaviors and isolating compromised sessions in Defender. Use Rubrik to granularly undo unwanted changes like privilege escalations or policy modifications without disrupting healthy configurations.
 Recover Clean and Current Reduce the risk of attacker persistence by removing backdoors. Bring forward sanctioned identity changes without wiping months of work.	 Remove Persistence & Rebuild Clean Analyze identity drift, triage logged changes by risk, and surgically reapply safe changes to a clean baseline. Remove attacker persistence from the rebuilt environment.

Empowering Security & IT Teams to Keep Identity Systems Secure

Security and IT teams no longer have to choose between speed and confidence. By ensuring identity systems remain trusted, operational, and recoverable, you can enable organizations to maintain access and uptime, investigate incidents, and restore identity infrastructure across hybrid environments. With Rubrik and Microsoft, organizations gain a complete view of the attack timeline and a trusted path to recovering identity systems cleanly.

Visit rubrik.com/identity to learn more.

SAFE HARBOR

Any unreleased services or features referenced in this document are not currently available and may not be made generally available on time or at all, as may be determined in our sole discretion. Any such referenced services or features do not represent promises to deliver, commitments, or obligations of Rubrik, inc. and may not be incorporated into any contract. Customers should make their purchase decisions based upon services and features that are currently generally available.

NOTE

Please speak to Rubrik and/or Microsoft representatives to confirm the availability and functionality of Rubrik's and/or Microsoft's products and services before making any purchase or renewal decisions.