NEWS RELEASE

Rubrik Accelerates Cyber Recovery for Applications Running on Amazon Web Services (AWS)

2026-11-10

- Unveils advanced cyber investigation and recovery capabilities for critical AWS workloads
- Autonomous Business Recovery (ABR) for AWS Cloud Applications is now generally available, with expanded service support

PALO ALTO, Calif.--(BUSINESS WIRE)-- Rubrik (NYSE: RBRK), the Security and AI Operations Company, today announced expanded cyber recovery capabilities for critical Amazon Web Services (AWS) workloads, including near real-time deletion detection, impact investigation, sensitive data blast radius reporting, and surgical recovery. Rubrik also announced the general availability (GA) of Autonomous Business Recovery (ABR) for AWS Cloud Applications, now extended to cloud-native architectures.

Attackers increasingly use compromised identities and cloud APIs to disrupt business operations. Rubrik's new capabilities help organizations running on AWS quickly understand the impact of an attack and recover with precision. ABR enables organizations to recover entire AWS applications from an established clean point, so they can bring back their Minimum Viable Business (MVB): the minimum set of applications and business services that support revenue, customers, employees, and operations.

"As more cybercriminals compromise identities and use cloud APIs to bring business operations to a halt, it's vital for organizations to be able to quickly gain a comprehensive understanding of an attack's blast radius and restore their systems," said Anneka Gupta, Chief Product Officer at Rubrik. "The expansion of Rubrik's cyber recovery capabilities for AWS arms organizations with the detection and investigation tools required to confront modern threats. We are delivering continuous cyber resilience from initial detection through complete business recovery."

Recovering Cloud Services After an Attack

When an attack hits a cloud environment, security teams have to answer three questions at once: what happened, what sensitive data was exposed, and how to get back to clean without losing weeks of work. Traditionally, this requires days of investigation, building a picture of what happened by stitching together logs and multiple tools. With Rubrik's new cyber recovery capabilities, teams can detect, understand, and recover in a fraction of the time:

- Near Real-Time Deletion Detection: Flags the deletion of critical cloud resources within seconds, rather than at the next backup, and shows the latest clean recovery point so teams can act immediately.
- Impact Investigation: Brings every type of alert related to your cloud workloads into one centralized experience to see the full impact of an incident.
- Sensitive Data Blast Radius Reporting: Shows whether sensitive data was impacted to answer compliance questions quickly. LLM-powered classification improves how accurately sensitive data is identified.
- Surgical Recovery: Removes malicious files, such as those encrypted or infected with malware, from cloud VMs. It then rolls forward the clean changes, minimizing data loss compared to rolling back an entire VM to a prior snapshot.

Securing the Minimum Viable Business with Autonomous Business Recovery

Cloud applications are complex webs of compute, data, networking, and configurations. Traditional recovery methods require teams to manually stitch together native snapshots using obsolete runbooks. ABR eliminates the guesswork as it discovers, protects, and recovers complete AWS applications.

Previously **announced** at Rubrik Forward, the solution is now generally available. Key benefits now include:

- Expanded Service Coverage: In addition to Amazon Elastic Compute Cloud (Amazon EC2) instances and Amazon Relational Database Service (Amazon RDS) databases previewed earlier, the GA release includes support for containerized applications (Amazon Elastic Kubernetes Service (Amazon EKS)), Amazon Elastic Container Registry (Amazon ECR), AWS Lambda functions, and Amazon Simple Storage Service (S3).
- Preemptive Clean Point: Rubrik's Preemptive Recovery Engine™ continuously identifies and establishes a clean recovery point before an incident occurs, bypassing the need for manual, post-attack iterative infrastructure scanning.
- Application-Level Recovery: Restores the entire application, including both data and configurations, in the exact dependency order required for immediate functionality.

Expanded cyber recovery capabilities for critical AWS workloads are expected to be generally available in the coming months. For more information, read the **blog** and join the virtual **Cloud Resilience Summit** taking place on

Tuesday, November 10, 2026.

About Rubrik

Rubrik (NYSE: RBRK) is the Security and AI Operations Company, delivering one platform built at the intersection of data, identity, and AI. The platform enables agentic cyber resilience and trusted AI operations for enterprises worldwide, built to recover before disruption strikes and stay a step ahead, so security is never the reason ambition stalls. For more information, please visit **www.rubrik.com** and follow Rubrik on **LinkedIn** and **X**.

© 2026 Rubrik, Inc. All rights reserved. Rubrik and the Rubrik logo are trademarks of Rubrik, Inc. Other marks are the property of their respective owners.

SAFE HARBOR STATEMENT: 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.

Media Contact:

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

Source: Rubrik