Logo

NEWS RELEASE

# New Rubrik Agent Cloud Accelerates Trusted Enterprise AI Agent Deployments

2025-10-22

- Industry's first solution to enable organizations to adopt agents at scale with the ability to monitor, govern and remediate
- Discovers agents built on platforms such as OpenAI, Microsoft Copilot Studio, and Amazon Bedrock to provide a single pane of glass for AI operations
- Where most tools stop at observability, only Rubrik empowers organizations to rewind agent mistakes

PALO ALTO, Calif.--(BUSINESS WIRE)-- AI agents represent the biggest opportunity and the biggest threat to organizations everywhere. Rubrik, Inc. (NYSE: RBRK), the Security and AI Operations Company, today announced the launch of the Rubrik Agent Cloud to accelerate enterprise AI agent adoption while managing risk of AI deployments.

Rubrik Agent Cloud showing a finance agent’s current lifecycle—from observability and control to performance management and simulation.

AI transformation is now mandatory for most organizations. However, IT leaders are constrained because Agentic AI has significant risks including hallucination as well as compromise by threat actors. Rubrik Agent Cloud is designed to monitor and audit agentic actions, enforce real-time guardrails for agentic changes, fine-tune agents for accuracy and, finally, undo agent mistakes. Built on the Rubrik Platform that uniquely combines data, identity and application contexts, Rubrik Agent Cloud gives customers security, accuracy, and efficiency as they transform their organizations into AI enterprises.

"IT and security leaders often don’t know what their AI agents are doing or how to undo their mistakes. Rubrik wants to help them answer: ‘What agents do I have?’ ‘What are they capable of doing?’ ‘How are they performing?’ ‘What did they do?’ and ‘Can I undo that when they screw up?’" said Bipul Sinha, CEO, Chairman, and Co-Founder of Rubrik. "AI agents have the potential to cause 10x the damage in 1/10 of the time. With Rubrik Agent Cloud, we uniquely address this

challenge by leveraging our leadership in data, identity, and resilience to help our customers deploy AI agents with peace of mind."

## Accelerate Enterprise AI Deployment and Resilience

Rubrik Agent Cloud will offer comprehensive agent management capabilities that encompass the entire AI agent lifecycle – from observability and control to performance management and simulation.

- Agent Monitor:
  - Auto-discovers both infrastructure-as-a-service (Azure/AWS) agents as well as platform-as-a-service (M365/AgentForce) agents.
  - Automatically discovers and maps active agents across popular agent builders such as OpenAI, Microsoft Copilot Studio, Amazon Bedrock and other popular agent building tools.
  - Continuously monitors agent activity and data access, and maintains immutable audit trails capturing context from data, identity, and applications.
- Agent Govern:
  - Tracks agent usage, evaluates performance against prompts, and gives teams the tools to control destructive/undesired actions.
  - Defines and enforces agent behavior, access, and action policies in real-time.
  - A centralized tool to provide integration with enterprise identity systems—helping ensure secure, compliant, and controlled innovation.
- Agent Remediate:
  - **Announced in August 2025**, Agent Rewind integrates with Rubrik Security Cloud to provide the industry's only solution for precise time and blast radius rollback of undesirable or destructive actions.
  - Goes beyond observability to allow organizations to instantly undo unwanted or destructive actions, without any downtime or data loss.
  - Selective rollback of agent-driven changes ensures continuous protection for critical data and systems, and immutable recovery.

Rubrik Agent Cloud is now available through limited early access for select customers. Not all features of Rubrik Agent Cloud are currently available. Discover what's next in agent operations by exploring **Rubrik's blog** and reserving your spot at our **upcoming webinar**.

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.

## About Rubrik

Rubrik (RBRK), the Security and AI Operations Company, leads at the intersection of data protection, cyber resilience, and enterprise AI acceleration. Rubrik Security Cloud delivers complete cyber resilience by securing, monitoring, and recovering data, identities, and workloads across clouds. Rubrik Agent Cloud accelerates trusted AI agent deployments at scale by monitoring and auditing agentic actions, enforcing real-time guardrails, fine-tuning for accuracy and undoing agentic mistakes. For more information, please visit **www.rubrik.com** and follow **@rubrikInc** on X (formerly Twitter) and **Rubrik** on LinkedIn.

## Media Contact

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

Source: Rubrik