NEWS RELEASE

Rubrik Unveils Agent Rewind For When AI Agents Go Awry

2025-08-12

New offering becomes the first to enable organizations to safely and confidently undo unwanted actions from AI agents

PALO ALTO, Calif.--(BUSINESS WIRE)-- Rubrik, Inc. (NYSE: RBRK), the Security and AI company, today announced the launch of Agent Rewind, following the close of **Rubrik's acquisition of Predibase**. Agent Rewind, powered by Predibase AI infrastructure, will enable organizations to undo mistakes made by agentic AI by providing visibility into agents' actions and enabling enterprises to rewind those changes to applications and data.

“As companies consider investing in AI, they often don’t take into account the mistakes that AI agents can and will make,” said Johnny Yu, Research Manager at IDC. “Agentic AI introduces the concept of ‘non-human error,’ and as with its human counterpart, organizations should explore solutions that allow them to correct potentially catastrophic mistakes made by agentic AI.”

"As AI agents gain autonomy and optimize for outcomes, unintended errors can lead to business downtime," said Anneka Gupta, Chief Product Officer at Rubrik. "Agent Rewind integrates Predibase's advanced AI infrastructure with Rubrik's recovery capabilities to enable enterprises to embrace agentic AI confidently. Today's organizations will now have a clear process to trace, audit, and safely rewind undesired AI actions."

AI agents possess significant potential, yet, like humans, they are prone to mistakes that result in unintended business disruption. Recent incidents of AI agent errors highlight a spectrum of situations ranging from technical malfunctions and legal issues to even the deletion of entire production databases. **A recent study** found that AI

agents are frequently becoming disoriented, choosing incorrect shortcuts, and struggling to complete even simple multi-step tasks, revealing critical flaws that undermine their reliability and effectiveness.

Agent Rewind makes previously opaque AI actions visible, auditable, and reversible, creating an audit trail and immutable snapshots that facilitate safe rollback. Current observability tools only show what happened, but not why or how to reverse high-risk actions.

"Agent Rewind will close the loop on what happened, why it happened, and how to undo it," said Chad Pallett, Chief Information Security Officer at BioIVT, a global research partner and biospecimen solutions provider for drug and diagnostic development. "When using AI, there is a need for observability and secure rollback. Rubrik and Predibase will provide not just data safety and model speed, but also AI recoverability. In a market craving true observability and remediation, Agent Rewind is the answer I've been waiting for."

When AI goes awry, Agent Rewind offers:

- Context-Enriched Visibility: Surfaces agent behavior, tool use, and impact while contextualizing each action, mapping it back to its root cause – from prompts to plans to tools – to enable precise recovery when something goes wrong.
- Safe Rollback: Uses Rubrik Security Cloud to rewind what changed, whether that's files, databases, configurations, or repositories.
- Broad Compatibility: Will integrate seamlessly with a wide range of platforms, APIs, and agent builders, including Agentforce, Microsoft Copilot Studio, and Amazon Bedrock Agents, and will be compatible with any custom AI agent.

To gain further insight into Agent Rewind and Rubrik’s perspective on the challenges and opportunities of AI Agents, read more on Rubrik's **blog** or see a **demo** here.

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 company, operates at the intersection of data protection, cyber resilience and enterprise AI acceleration. The Rubrik Security Cloud platform is designed to deliver robust cyber resilience and

recovery including identity resilience to ensure continuous business operations, all on top of secure metadata and data lake. Rubrik's offerings also include Predibase to help further secure and deploy GenAI while delivering exceptional accuracy and efficiency for agentic applications. 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