NEWS RELEASE

Rubrik Launches Rubrik Agent Cloud for Anthropic's Claude Code

2026-06-09

Delivers Runtime Agent Security and Agent Rewind for Code Repository and Agentic Harness

LAS VEGAS--(BUSINESS WIRE)-- Rubrik FORWARD--Rubrik (NYSE: RBRK), the Security and AI Operations Company, today announced Rubrik Agent Cloud (RAC) for Anthropic's Claude Code and Claude Cowork. Organizations can now deploy Claude-powered agents at scale with observability, control, and the industry's only agent rewind to reverse unintended actions, and immutable codebase recovery when an incorrect action outruns version control. A new, additional layer of resilience for Claude agents backs up, monitors, and restores the configuration that governs how agents behave.

AI agents now write, push, and deploy code autonomously, but enterprise security infrastructure was built assuming humans are always in the loop. A gap could enable rogue commits, repo ransomware, prompt injection, and IP exfiltration at machine speed - with blast radius far beyond what traditional DevSecOps controls were designed to handle.

"Organizations are adopting Claude faster than any agentic technology we have seen, and every security leader asks the same question: how do we stay in control when an agent can act?" said Anneka Gupta, Chief Product Officer, Rubrik. "Rubrik Agent Cloud gives organizations a resilience layer for Claude, which allows them to see what agents can access, govern what they do, rewind their actions, and recover both the code and the agent's own configuration when something is destroyed or tampered with. Working with Anthropic, a leader in AI, lets us bring that control to customers from day one."

RAC for Claude Code and Cowork: Delivers enterprise control and resilience layers for organizations deploying Anthropic's Claude. The autonomous environment is secured with the following capabilities:

- Semantic AI Governance Engine (SAGE): The industry's first AI governance engine, designed to secure and control autonomous agents in real time. SAGE replaces static, manual oversight with intent-driven governance to safely scale the enterprise AI workforce.
- Agent Inventory: Delivers 360-degree visibility into risk, access permissions, and policy violations across all deployed agents.
- Agent Rewind: Provides the power to instantly and precisely reverse unintended actions from custom agents to agents developed in popular agentic tools, including agentic development environments like Claude Code and Cowork.
- Codebase Resilience: Enhanced rewind for code & developer pipelines maintains continuous, immutable snapshots of GitHub and Azure DevOps repositories, stored outside the repo and beyond the reach of compromised credentials. When an agent or an attacker exploiting one takes an action that version control cannot undo, such as force-pushing over commit history or deleting every branch, RAC restores a known-good state with one-click repository or org-level recovery, including ransomware rollback for code.
- Resilience for Claude Agents: Backs up, version-tracks, and restores the configuration that governs how Claude agents behave (system prompts, tool permissions, skills, and key files such as CLAUDE.md and settings) across organization, repository, and user levels. Rubrik continuously monitors for configuration drift and flags changes that appear malicious or unauthorized before they propagate. Rather than a blunt rollback, Rubrik's intelligent recovery is able to autonomously tie the detected drift to the healthy backup snapshots to enable fast, orchestrated recovery.

For more information, check out the Rubrik Agent Cloud for Claude Code and Cowork **here**.

Learn more breaking news at Rubrik FORWARD:

- **Rubrik Now Available as AI Agent**
- **Rubrik Unlocks Unstructured Data**
- **Rubrik Introduces Autonomous Business Recovery Solution for Cloud Applications**
- **Global Systems Integrators Partner with Rubrik to Deliver Rubrik Agent Cloud for Anthropic's Claude Code**
- **Rubrik Advances Identity Resilience Through Strata Acquisition and Identity Roll Forward Innovation**

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 Anthropic

Anthropic is an AI safety and research company dedicated to building reliable, interpretable, and steerable AI systems. Its Claude family of models enables advanced capabilities across a wide range of applications, including code understanding and security analysis.

About Rubrik

Rubrik (NYSE: 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, Rubrik
925.785.9192
press@rubrik.com

Source: Rubrik