Rubrik Agent Cloud

Monitor. Govern. Remediate.

EXECUTIVE SUMMARY

AI agents are transforming enterprise productivity by writing code, analyzing data, and making autonomous decisions that accelerate innovation. However, without a dedicated control layer, one unintended action, whether from hallucination or cyber compromise, can create **10 times the damage in 1/10th of the time**. Enterprises are "flying blind," unable to see, govern, or instantly recover from autonomous agent actions.

The **Rubrik Agent Cloud (RAC)** delivers the essential enterprise control layer for AI agents. Built on Rubrik's cyber resilience foundation, it allows organizations to **monitor agent actions, govern agent behavior, and remediate agent mistakes**, turning AI chaos into operational excellence.

THE AI OPERATIONS IMPERATIVE: CLOSING THE CONTROL GAP

AI transformation is mandatory, but IT leaders are paralyzed because the autonomous nature of Agentic AI dramatically amplifies the risk of technical error and cyber compromise. Organizations need a comprehensive platform to deploy agents and manage associated risks.

For these IT leaders, Rubrik answers the critical questions that enable confident action:

- **What agents do I have and what are they capable of doing?**
- **How are they performing?**
- **What did they do, and can I undo that when they screw up?**

Rubrik closes this control gap with the first enterprise-grade platform designed to **govern, monitor, and recover** from agent-driven actions at scale.

Common Challenges:

Blind Autonomy & Sprawl:
No unified view of agent activity, data access, or the identities they assume, leading to ungoverned deployment across the organization.

Instant Impact:
A single compromised or misconfigured agent can corrupt critical data or trigger systemwide changes in seconds.

WHAT IS RUBRIK AGENT CLOUD?

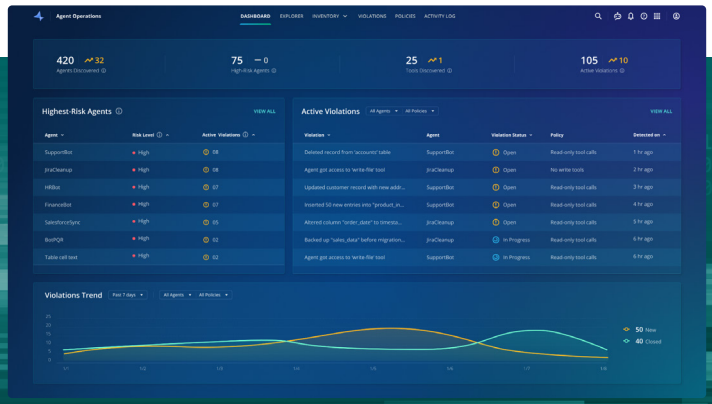
The Rubrik Agent Cloud is the unified control layer for enterprise AI, combining risk and operational management. It ingests agent telemetry from major systems like OpenAI, Microsoft Copilot Studio, and Amazon Bedrock, then enriches it with data and identity context from Rubrik's security foundation.

The platform is built around three core capabilities:

AGENT MONITOR
Gain comprehensive visibility into agent activity and risk.

AGENT GOVERN
Enforce real-time guardrails and ensure compliance with defined policies.

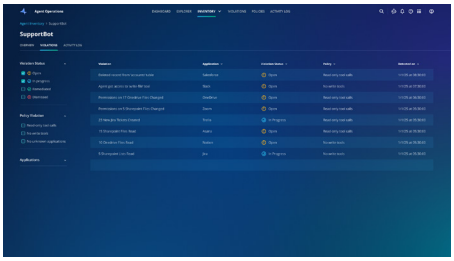
AGENT REMEDIATE
Reverse unintended or unauthorized actions with precision.



Gain holistic visibility across your entire agent estate, from policy violations to performance ROI.

HOW RUBRIK AGENT CLOUD ENABLES SUCCESS

Rubrik Agent Cloud delivers **Complete Agent Management**, serving as the first enterprise platform designed to monitor, govern, and remediate AI agents across data, identity, and applications.



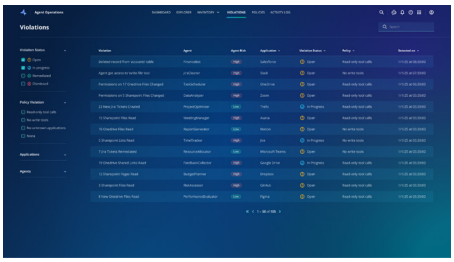
See issues early and respond with confidence.

Agent Monitor: See Agent Actions Clearly

RAC provides continuous visibility into active agents and their activity across the environment, mapping their behaviors, permissions, and data access patterns in a single unified view.

Key capabilities:

- **Auto-Discovery:** Automatically discover and monitor agents across your environment, including both **Infrastructure-as-a-Service (Azure/AWS)** agents and **Platform-as-a-Service (M365/AgentForce)** agents.
- **Continuous Monitoring:** Capture agent activity and data access in an immutable audit trail.
- **Risk Evaluation:** Identify agent capacity and operational risks early to respond with confidence.



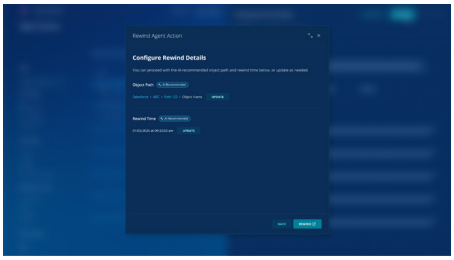
Keep innovation secure, compliant, and under control.

Agent Govern: Enforce Guardrails and Maintain Compliance

Define how agents behave, what they can access, and when. Rubrik enforces policy guardrails in real time, helping ensure responsible agent behavior and improving performance.

Key capabilities:

- **Centralized Policy:** Define and enforce policies to control destructive or undesired agent actions.
- **Performance Evaluation:** RAC tracks agent usage and **evaluates performance against prompts**, and gives teams the tools to control destructive/undesired actions.
- **Real-Time Guardrails:** Detect and block violations instantly, integrating with enterprise identity systems to enforce access controls.



Recover quickly and keep operations running.

Agent Remediate: Reverse Mistakes and Restore Trust

When AI agents make mistakes, Rubrik helps you recover fast. **Agent Remediate** integrates with Rubrik Security Cloud to provide the industry's only solution for precise recovery.

Key capabilities:

- **Selective Rollback:** Undo unwanted or destructive actions with **precise time and blast radius rollback**, without any downtime or data loss.
- **Immutable Recovery:** Continuous protection for critical data and systems built on Rubrik's cyber resilience foundation.
- **Fast Restoration:** Recover quickly and keep operations running confidently after an agent error or compromise.

THE RUBRIK STAKEHOLDER ADVANTAGE: CONFIDENT AI AT SCALE

Stakeholder	Key Challenge Solved	Primary Benefit
CIOs and AI Leaders	Risk of uncontrolled AI growth	Confident AI adoption at enterprise scale
Security and Risk Teams	Lack of visibility into agent actions	Continuous monitoring and targeted rollback
Platform Engineers	Managing agent sprawl and impact	Centralized control and simplified governance
ML and AI Teams	Risk of disruption during iteration	Safe experimentation with policy and recovery built in

ACCELERATE YOUR AI JOURNEY WITH RUBRIK

Rubrik Agent Cloud gives enterprises the visibility, guardrails, and recovery needed to deploy AI safely. Built on Rubrik's proven cyber resilience foundation, it unifies monitoring, governance, and recovery for every stage of AI adoption.

Unleash agents. Not risk.

Learn more at rubrik.com/agent-cloud. Not all features of Rubrik Agent Cloud are currently available.

SAFE HARBOR STATEMENT

Any unreleased services or features referenced in this brief 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.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

brf-rubrik-agent-cloud / 20251020