



NEWS RELEASE

Rubrik Unveils Agent Identity to Secure Agentic Actions in Real-Time

2026-08-04

Rubrik Agent Cloud now monitors every agent and MCP server, controls access per tool call, and remediates unwanted actions

LAS VEGAS--(BUSINESS WIRE)-- Today at the Black Hat Conference, Rubrik (NYSE: RBRK), the Security and AI Operations Company, announced Rubrik Agent Identity, a powerful new AI-based solution to manage and control AI agents' access and permissions, addressing a key obstacle in enterprise agent deployment.

AI agent deployments are rapidly evolving, with the potential to execute complex, automated workflows across SaaS applications, databases, and APIs at unprecedented speed and scale. Yet most organizations lack the capability to monitor and control agent access and actions at the necessary speed and scale. Rubrik Agent Identity is designed to reduce operational vulnerabilities that stem from agent identities by allowing customers to both monitor every agent and model context protocol (MCP) at runtime using AI, and to deliver just-in-time permissions per tool call.

"Agents are no longer just synthesizing information, they are acting on behalf of employees, and using the access models we built for humans. Static credentials were never designed for autonomous actors," said Dev Rishi, General Manager of AI at Rubrik. "Agent Identity lets enterprises decide who can do what with agents and enforces it at each tool call, at the moment of action, with scoped, short-lived access. With Rubrik Agent Cloud, enterprises can govern agent activity, enforce identity-aware policies, and apply semantic policy evaluation before sensitive actions execute."

Control AI Identity with AI

Modern AI creates an unmonitored "shadow workforce" that bypasses traditional security boundaries. Because these systems often rely on broad, static credentials, a single compromised agent can trigger destructive, system-wide actions with zero visibility.

According to recent data from Rubrik Zero Labs, 86% of global IT and security leaders expect AI agents to outpace their organization's security guardrails within the next year, while only 23% report full visibility into the agents operating in their environments.

Rubrik Agent Identity, delivered as an expansion of the Rubrik Agent Cloud platform, establishes a unified "Govern, Control, and Prove" model across the entire agent lifecycle. The new solution operates alongside Rubrik's established **SAGE** governance framework, and now provides four distinct Rubrik Agent Cloud pillars:

1. **Agent Observability:** Monitor every agent and MCP at runtime.
2. **Agent Identity:** Control access per tool call at speed and scale using fine-tuned AI.
3. **Agent Runtime Security:** SAGE intent-driven governance to enforce policies, and detect agent errors in real time.
4. **Agent Rewind:** Undo agentic mistakes.

Secure the Moment of Action: Rapid Posture Hardening in Three Steps

The architecture introduces key capabilities designed to help enterprises rapidly harden their agentic identity posture:

- **Build an Agent Identity Inventory:** Discover and catalog all active AI agents, MCP servers, skills, and plugins to immediately eliminate unmonitored shadow AI.
- **Delegate Least-Privilege Access:** Scope access to specific MCP servers and tools by user and group using On-Behalf-Of federation, extending existing enterprise identity structures rather than replacing them.
- **Enforce with Just-In-Time Tokens:** Eliminate standing permissions entirely by minting scoped, short-lived tokens per tool call, ensuring access is validated at runtime before execution.

Enforce Runtime Access Control at the MCP Gateway

To prevent malicious or erroneous actions before they occur, every MCP tool call must clear three distinct checkpoints before execution:

1. **Behavioral Analysis:** SAGE semantically evaluates the requested tool call, its context, input parameters, and

potential operational impact before execution.

2. Access Policy Enforcement: Run-time security policies are verified at the infrastructure layer, enriched with SAGE context.

3. Identity Verification: The agent session is authenticated, and the system mints a short-lived token specifically scoped to that single tool call.

If an unauthorized action is attempted, such as a write or modification without an explicit policy scope, the transaction is immediately blocked before execution. For unexpected agent behaviors, Agent Rewind instantly and precisely undoes an autonomous agent's destructive action., addressing the widespread industry concern where **88% of leaders** worry about meeting recovery time objectives as agentic threats scale.

Strategic Ecosystem Integrations

Rubrik Agent Identity integrates seamlessly with Okta and Microsoft Entra ID, extending existing enterprise identities to autonomous machine actors without requiring new directories. The MCP Gateway provides a unified security checkpoint for all API-based and MCP resources across the enterprise. Ultimately, Rubrik Agent Identity advances the company's vision to deliver Agentic Cyber Resilience to our customers, helping them keep pace with machine-speed attacks powered by frontier AI models.

To learn more about Rubrik Agent Identity, visit [here](#).

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.

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