NEWS RELEASE

As Agentic AI Adoption Accelerates, Rubrik Warns of Growing Security Gaps

2026-04-16

New research from Rubrik Zero Labs highlights a critical lack of identity governance as organizations race to adopt autonomous systems they cannot fully observe or restore.

PALO ALTO, Calif.--(BUSINESS WIRE)-- The enterprise push into AI agents is outpacing the ability to secure them, according to **new research** from **Rubrik Zero Labs**.

Rubrik (NYSE: RBRK) announced today the findings from the report, which show organizations are operationalizing autonomous systems without the controls required to govern them, introducing a gap between innovation and security.

Based on a survey of more than 1,600 IT and security leaders, the report reveals:

- 86% expect AI agents to outpace their organization's security guardrails within the next year.
- Only 23% report full visibility into the agents operating in their environments, which the report notes is likely an over-estimation on the part of respondents. The result is the inability to secure identities that are already making decisions, taking actions, and interacting with critical data.

The gap is compounded by identity sprawl. Non-human identities tied to agents are proliferating faster than enterprises can track or govern them, forming what researchers describe as a "shadow workforce." These identities often operate with persistent access and limited oversight, creating new pathways for misuse, compromise, and lateral movement.

At the same time, the operational promise of AI agents is under strain. The report also found:

- More than 80% of respondents report agents require more manual oversight than they save in efficiency.
- 88% say they lack the ability to roll back agent actions without system disruption.
- Recovery and prevention are emerging as primary points of failure. Nearly nine in ten leaders expressed concern about meeting recovery objectives as agent-driven threats increase.

The threat itself is accelerating. Nearly half of respondents expect agentic systems to drive the majority of attacks in the coming year, reflecting a broader shift in how adversaries operate. Autonomous systems compress timelines, scale attacks, and blur the line between insider risk and external compromise.

> “AI adoption is outpacing our ability to control it. Enterprises are struggling because they’ve deployed systems they can’t fully observe, govern, or restore,” said Kavitha Mariappan, Chief Transformation Officer at Rubrik. “We have to move past the debate of whether AI is risky and address the harder reality: as decision-making shifts from human to machine, the critical challenge for every leader is maintaining operational safety in an increasingly autonomous landscape.”

For boards and executive teams, the implication is immediate. AI strategy is now inseparable from resilience strategy. Organizations that continue to prioritize deployment speed over control mechanisms risk creating environments where failures cannot be contained or reversed.

> "Identity verification is the fundamental underpinning that will allow us to get the greatest automation benefits of AI without imposing human bottlenecks," says Renown Health VP, Chief Information Security & Technology Officer Steven Ramirez. "Verification and visibility are prerequisites for sound, secure agentic implementation."

Rubrik Zero Labs’ report, The State of the Agent: Understanding Adoption, Risk, and Mitigation, combines global survey data with technical analysis of emerging attack vectors across the tool, cognitive, and identity layers of AI systems. The research outlines a shift already underway: security is no longer about preventing breach alone, but about maintaining control in systems that no longer wait for human input.

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