NEWS RELEASE

Rubrik Rolls Out Industry's First Semantic AI Governance Engine

2026-03-23

Domain-Specific Small Language Model Accelerates Trusted AI Agent Deployment and Control

SAN FRANCISCO--(BUSINESS WIRE)-- Rubrik (NYSE: RBRK), the Security and AI Operations Company, today unveiled its Semantic AI Governance Engine (SAGE), the data security industry's first AI governance engine designed to secure and control autonomous agents in real time. SAGE powers Rubrik Agent Cloud, replacing static, manual oversight with intent-driven governance to safely scale the enterprise AI workforce while maintaining total control over agent behavior.

Enterprise AI deployment is stalling at a governance bottleneck, as legacy systems rely on deterministic rules that cannot comprehend natural language nor adapt to dynamic and unforeseen actions taken by agents. Rubrik SAGE solves the bottleneck by using Rubrik's custom Small Language Model (SLM) to interpret the semantic meaning of policies, providing a real-time command center for agentic operations.

"SAGE marks a pivotal moment in AI security as we shift the focus from if agents can be deployed to how they can be governed at scale," said Devvret Rishi, General Manager AI, Rubrik. "With SAGE, we can move beyond simple monitoring to a future where AI helps us govern AI agents. Now, we give CISOs the guardrails they need to let their AI agents run at full speed without compromising the security and integrity of the enterprise."

AI Powers Rubrik Agent Cloud

SAGE evolves AI security from reactive monitoring to active, semantic enforcement. By understanding the intent

behind a policy, rather than just searching for keywords, SAGE ensures agents operate within safe boundaries without stifling their ability to solve complex tasks.

Key innovations within SAGE include:

- Semantic Policy Interpretation: SAGE translates natural language instructions (e.g., "Do not give financial advice") into machine logic, recognizing context that static filters miss.
- Proprietary SLM: Rubrik's custom SLM outperforms generalized LLMs in accuracy while operating at a fraction of the latency.
- Adaptive Policy Improvement: SAGE proactively identifies ambiguous guardrails and suggests refinements to administrators before a violation occurs.
- Integrated Remediation: In the event of an agent error, SAGE triggers Rubrik Agent Rewind to instantly undo destructive actions and restore data integrity.

Data-Driven Governance

To validate the efficiency of its governance engine, Rubrik conducted a head-to-head benchmark between Rubrik's custom SLM and OpenAI's GPT-5.2. In a comparative analysis using a standardized set of user-agent interactions, Rubrik's custom SLM:

- Processed messages 5x faster and detected violations correctly more often.
- Achieved a higher accuracy rate in detecting policy violations compared to generalized LLMs.
- Significantly reduced the compute overhead typically associated with real-time AI monitoring.

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 (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

925.785.9192

press@rubrik.com

Source: Rubrik