Rubrik Annapurna and Amazon Bedrock

Accelerating Generative AI with Security and Compliance

Enterprises today face significant challenges when moving generative AI applications from pilot projects to full-scale production. Gartner predicts that "[a]t least 30% of generative AI (GenAI) projects will be abandoned after proof of concept by the end of 2025, due to poor data quality, inadequate risk controls, escalating costs or unclear business value."[1]

To address these barriers, Rubrik is introducing Rubrik Annapurna for Amazon Bedrock. This solution will be designed to combine secure data access with high-performing AI models to help organizations deploy production-ready generative AI applications that meet stringent security and compliance standards.

NAVIGATING THE COMPLEXITY OF GENERATIVE AI ADOPTION

While generative AI presents transformative opportunities, enterprises struggle with the complexities of data integration, governance, and security. AI development teams must securely access enterprise data from various sources, filter sensitive information, and maintain compliance—all while enabling robust AI model performance. Without a comprehensive, secure data foundation, these AI projects risk stalling or failing to scale.

A SOLUTION BUILT FOR SECURE, SCALABLE AI

Rubrik Annapurna for Amazon Bedrock will be designed to overcome the challenges of enterprise-scale AI with a secure, compliant data pipeline. By integrating Rubrik's Security Cloud with Amazon Bedrock, the future solution aims to empower organizations to access an optimized, secure data platform that accelerates AI development while ensuring compliance across data environments.

---

1 [Gartner Predicts 30% of Generative AI Projects Will Be Abandoned After Proof of Concept By End of 2025](#)

KEY FEATURES AND BENEFITS OF RUBRIK ANNAPURNA

Rubrik Annapurna will be designed to offer essential capabilities that support secure, scalable, and compliant AI development, to help enterprises unlock the full potential of generative AI.

API-Driven Data Access: Rubrik's API-driven architecture allows access to data across on-premises, cloud, and SaaS environments, supporting dynamic data refreshes, real-time permissions updates, and automated sensitive data management to ensure compliance.

Application-Aware Data Embeddings: Rubrik's embedding architecture will be designed to create secure, application-aware data embeddings through a single API, making data available for retrieval-augmented generation (RAG) workflows. These embeddings will leverage Rubrik's understanding of common application schemas to help ensure relevant and compliant data for AI models.

Sensitive Data Suppression: Rubrik's solution will be designed to apply data filtering policies to remove sensitive information before it reaches AI models, to help organizations comply with data privacy laws.

Source-Based Role-Based Access Control (RBAC): Rubrik maintains role-based access control at the data source level, helping ensure secure user-based access permissions across AI applications.

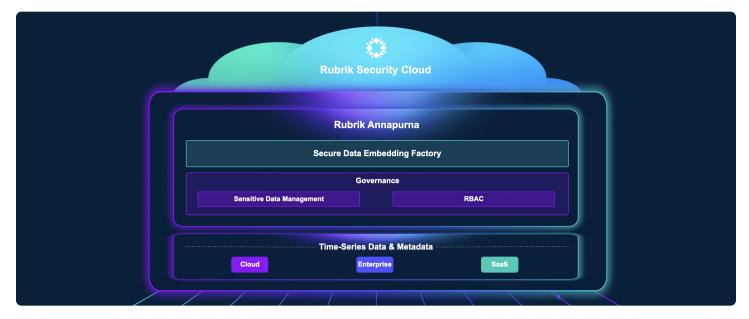## UNLOCKING REAL-WORLD AI USE CASES WITH RUBRIK AND AMAZON BEDROCK

Rubrik Annapurna aims to enable targeted AI use cases that leverage secure, real-time data access to drive enterprise-wide innovation.

- **Customer Support Intelligence:** Integrate data from Salesforce and Microsoft Teams for AI-driven support systems that can enhance customer interactions while helping ensure data privacy.

- **Sales Insights and 360° Customer Views:** Aggregate CRM, email, and communication data to deliver comprehensive customer insights that help inform sales strategies, with secure integrations that protect sensitive data.

- **Marketing Content Generation:** Generate high-quality content by consolidating insights from knowledge bases, OneDrive, and S3-stored call recordings, with built-in data filtering to help maintain compliance.

STREAMLINED SECURITY AND COMPLIANCE FOR AI

Rubrik Annapurna will be designed to integrate security at every stage of the AI lifecycle, to ensure organizations can trust the data that powers their AI models.

- **Data Freshness and Compliance:** Rubrik's SLA domains will be designed to automate data updates, maintaining data relevance and helping organizations meet regulatory requirements.

- **Amazon Bedrock Guardrails:** Amazon Bedrock's guardrails will be designed to complement Rubrik's protections with prompt filtering, content moderation, and contextual grounding checks, adding layers of security against risks like prompt injection.

- **Single Source of Truth:** By centralizing data management, Rubrik will be designed to avoid the need for duplicate data stores, to reduce complexity and help ensure that a compliant, secure version of enterprise data is available for AI applications.
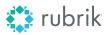

TRUSTED BY INDUSTRY LEADERS

Rubrik is trusted by organizations worldwide to help them scale their generative AI projects securely and reliably. Check out this demo to learn more.

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.

LEARN MORE