



NEWS RELEASE

Rubrik Unveils Rubrik Code Guardian, Harnessing Anthropic's Claude Mythos 5 to Red-Team Code and Prioritize Cyber Risks

2026-09-15

Frontier AI applied to secure, air-gapped code repositories accelerates testing of validated vulnerability chains and recommending remediation of potential issues

PALO ALTO, Calif.--(BUSINESS WIRE)-- As autonomous agents make the digital world more dangerous, Rubrik (NYSE: RBRK), the Security and AI Operations Company, unveils Rubrik Code Guardian, a custom Claude Mythos 5 harness that red-teams customers' code based on an air-gapped copy of their repository.

"Rubrik is one of the partners we are working with to put Claude Mythos 5's cyber capabilities in defenders' hands, so they can find and validate attack paths before attackers do," said Michael Moore, Cybersecurity lead at Anthropic. "Rubrik will use the model to test code faster and at far greater scale, and to bring cyber resilience up to the speed of AI."

The new service uncovers and prioritizes the multi-step vulnerability chains an attacker would actually exploit, validates each for exploitability, and turns confirmed critical issues into tracked remediation.

"Frontier models are advancing at a fast pace. In the wrong hands, these models can be used to discover, chain, and exploit vulnerabilities at machine speed," said Arvind Nithrakashyap, Co-Founder and Chief Technology Officer at Rubrik. "To move just as fast, we are using frontier AI to scale vulnerability detection faster than our traditional code scanning tools. We took Anthropic's powerful model and built a Rubrik software harness to test on our code. We are

using that experience and success now to give customers access to the harness, with a secure, isolated environment, which means we can run analysis of their code away from live repository and production systems.”

The Next Milestone in Agentic Cyber Resilience

Rubrik Code Guardian makes critical enterprise systems more resilient to even the most advanced frontier AI-powered attacks. The product embeds and harnesses Anthropic’s Claude Mythos 5 into a service that operates directly on air-gapped copies of source code, enabling frontier model level vulnerability analysis while minimizing risk and impact on production environments.

Rubrik Code Guardian proactively secures the core intellectual property that powers modern businesses:

- **Red-Team Customer Code, Safely:** Runs Claude Mythos 5 through Rubrik’s custom security harness against a secure clone of the immutable, air-gapped copy never against the live repository or production environment.
- **Attack Chains, Not Alerts:** Reasons across files, services, authentication patterns, and cloud boundaries to surface previously undetectable vulnerabilities, even “chained vulnerabilities” that advanced AI attacks now exploit.
- **Validated Findings, Prioritized by Business Criticality:** Validates attack chains for real exploitability before surfacing them and prioritizes findings by exploitability, blast radius, and business criticality.
- **Accelerated Remediation:** Pushes confirmed critical issues into developer workflows through Jira or GitHub issues with file-level remediation guidance.
- **Built-In Code Resilience:** Maintains recovery workflows so organizations can restore a known-good codebase if a security event or bad build occurs.

Rubrik Code Guardian is currently accepting select design partners for private preview.

To learn more about Rubrik Code Guardian and Rubrik’s ongoing work with Anthropic, visit www.rubrik.com or join Rubrik’s sessions at the **AI and Identity Resilience Summit**.

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) is the Security and AI Operations Company, delivering one platform built at the intersection of

data, identity, and AI. The platform enables agentic cyber resilience and trusted AI operations for enterprises worldwide, built to recover before disruption strikes and stay a step ahead, so security is never the reason ambition stalls. For more information, please visit www.rubrik.com and follow Rubrik on LinkedIn and X.

© 2026 Rubrik, Inc. All rights reserved. Rubrik and the Rubrik logo are trademarks of Rubrik, Inc. Other marks are the property of their respective owners.

Media Contact

Meghan Fintland

Head of Global PR

925.785.9192

press@rubrik.com

Source: Rubrik