

Rubrik Code Guardian

Built with Anthropic. Attack Your Code Before Attackers Do. Fix What Actually Matters.

EXECUTIVE SUMMARY

AI models can now find and chain code vulnerabilities as fast as they're written, a shift Gartner already tracks as its own category, Agentic Coding Security. Closing that gap is the customer's responsibility, not something a traditional scanner backlog was built to catch.

Rubrik Code Guardian harnesses Anthropic's Mythos to red-team your code from a secure copy of your repository. It finds and ranks the multi-step vulnerability chains an attacker would actually exploit, and turns confirmed critical issues into tracked remediation tickets. *Code Guardian is currently in private preview and subject to change; not generally available.*

THE CODE RESILIENCE GAP

Security teams face an AI-speed exposure across the SDLC: unranked findings, invisible attack chains, and triage queues that can't keep up.

- **Machine-speed attacks:** one low-severity bug, chained across services, becomes a full account takeover.
- **Blind spots, not clarity:** traditional scanners rate bugs in isolation as "low, won't fix," burying the paths that matter under unranked noise.
- **Not hypothetical:** a July 2026 breach chained a sandbox escape, stolen credentials, and a zero-day into a production compromise. (The Hacker News)
- **An industry-wide gap:** CVE submissions up 263% since 2020; NVD now plans to fully enrich only 15 to 20% of incoming CVEs.
- **AI-authored code is outpacing review:** 630M+ GitHub repos, LLM SDK usage up 178% YoY, 80% of new developers on Copilot within a week. (GitHub, Octoverse 2025)
- **More reviewers won't fix this:** human-driven remediation can't keep pace with AI-speed discovery, no matter how big the security team.

INTRODUCING: RUBRIK CODE GUARDIAN

Mythos doesn't just spot flaws. It reasons across files, services, and cloud boundaries, chaining minor weaknesses into the path an attacker would actually use. That's a different capability than traditional scanning, and few companies can run it against live code safely yet.

Code Guardian puts that reasoning to work: against a Rubrik air-gapped copy of your repository, with a prioritized list of validated chains before it reaches your team.

See the Attack Paths That Actually Matter

THINK LIKE YOUR ATTACKER

Chain minor bugs into multi-step takeover paths, the way an attacker would.

- **Threat-Model-Aware Analysis:** Reasons across files, services, auth patterns, and cloud boundaries the way an attacker would.
- **Attack Chains, Not Alerts:** Chains minor bugs into complete takeover paths, not isolated flags.
- **Proven on Rubrik's Own Codebase:** More findings than traditional code scanning tools, confirmed exploitable in an internal pilot.
- **Safe by Design:** Analysis runs from a secure, air-gapped copy; production and the live repositories are never touched.



Trust Every Finding, Skip the Noise NO FALSE-POSITIVE FLOODS, NO GUESSWORK

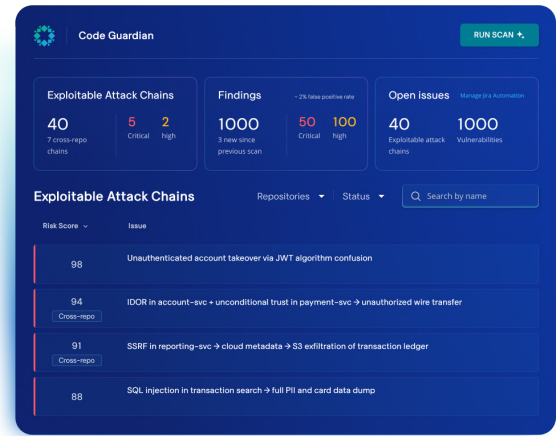
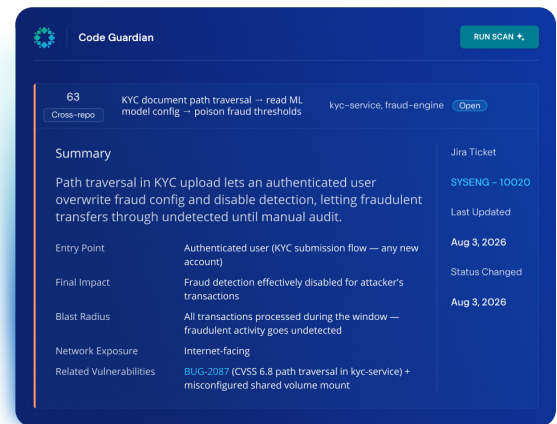
Every finding is prioritized before it reaches an engineer.

- **Exploitability Validation:** Every attack chain confirmed exploitable by Mythos before it ever reaches an engineer.
- **Business-Impact Ranking:** Exploitable (P0/P1) versus hardening (P2/P3), ranked by exploitability, blast radius, and criticality.
- **Continuous Self-Tuning:** Reviewer feedback sharpens precision every scan cycle.
- **Your Code Stays Yours:** Source code and model reasoning stay in Rubrik's infrastructure, never shared with Anthropic or any third party.

Turn Findings Into Fixes FROM FINDING TO ACTION

Confirmed critical issues become tracked tickets your team can act on immediately.

- **Drift Monitoring:** Every new commit is checked automatically; a critical new chain triggers an alert the moment it ships.
- **In-Workflow Alerts:** Alerts land as PR comments in the tools your team already uses, no new dashboard.
- **Auto-Opened Tickets:** Confirmed critical issues become Jira or GitHub tickets with file-level remediation guidance.
- **SLA Tracking:** Remediation stays on schedule with built-in tracking against your SLAs.



DELIVERING VALUE ACROSS THE ORGANIZATION



CISOS AND SECURITY EXECUTIVES

Set a security strategy that keeps pace with AI-speed attackers, backed by validated proof from Rubrik's own codebase, not just more alerts.



ENGINEERING LEADERS

Get a ranked, attacker-realistic list of what to fix first, instead of an unranked scanner backlog.



IT AND BACKUP ADMINISTRATORS

Get an active vulnerability discovery and remediation tracking program for your code, without standing up new AppSec tooling.

See the attack paths that matter, and fix them before attackers do, with Rubrik Code Guardian.



Global HQ

3495 Deer Creek Road
Palo Alto, CA 94304
United States

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 and may not be incorporated into any contract. Customers should make their purchase decisions based upon services and features that are currently generally available.

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

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.

brf-rubrik-code-guardian / 20260922