



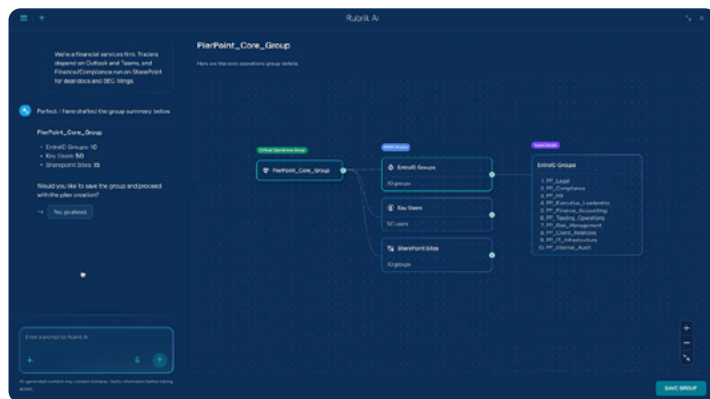
It Discovers. It Reasons. It Acts. It Collaborates.

Rubrik AI is the industry's most comprehensive cyber resilience agent, architected with frontier AI. It discovers, reasons, acts, and collaborates across data, identity, and applications, already inside the Rubrik Security Cloud (RSC) platform you run today: no new console, no new agent to deploy.

Security and IT teams face a widening gap between machine-speed threats and human-speed tools: siloed alerts, manual diagnosis, and agents that can't share what they know.

- ✖ **Machine-Speed Attacks:** Breakout time is now measured in seconds, not days, and a security model built around human minutes cannot simply ask people to work faster.
 - ✖ **Hours Lost to Manual Diagnosis:** A single backup failure can mean hours of cross-referencing error codes and manually stitching signals together before anyone finds the fix.
 - ✖ **Fragmented Agent Ecosystem:** A SOC agent flags a compromised host but doesn't know what's safe to recover, and that answer lives on a different platform, so someone stops to log in and relay it back manually.
 - ✖ **Generic AI Falls Short:** A chatbot or a RAG search over documentation can inform, but it doesn't know Rubrik's own error codes, API surface, or recovery procedures, so it can't act.

None of that gets fixed by working harder. It gets fixed by an agent that discovers what you'd miss, reasons faster than the attacker, acts the moment you say go, and shares what it knows with everything else in your stack. Agentic Cyber Resilience is built on two imperatives: assume breach, assume agentic overreach. Rubrik AI is not a tool you operate, it's an agent that pursues an outcome: your resilience. It discovers across your data, identity, and applications, reasons the right response at machine speed, acts through composable skills you already own, and collaborates across the stack you already run.



Visibility That Starts From Ground Truth

- **Full-Estate Answers:** Environment, cluster, and workload health, protection, capacity, and compliance answers across VMware, Hyper-V, NAS, Oracle, SQL Server, Salesforce, M365, and cloud-native workloads.
- **Grounded in Live APIs:** Calls real RSC data through the same GraphQL API the console uses, not text and documents alone. Draws on the knowledge base built from Rubrik's decade of protecting customer environments.
- **Proactive by Default:** Surfaces anomalies and protection gaps before an admin would know to go looking.

Diagnoses At Machine Speed, Not Human Speed

- **Deep Domain Expertise:** Encode Rubrik-specific diagnostics across VMware, Oracle, M365, Salesforce, and more: the institutional expertise a general model doesn't have.
- **One Policy, No Exceptions:** Every decision, whether triggered by a human or an agent, runs through the same policy engine and the same guardrails.

FROM DIAGNOSIS TO ACTION, WITHOUT THE MANUAL HANDOFF

Executes End To End, Nothing Skips Approval

State the intent, and Rubrik AI composes the outcome using capability you already own,

- **Agentic Recovery:** Automated scoping and surgical sequencing to restore your critical business operations first.
- **Instant Visibility:** On-demand data mapping and visual compliance reporting without manual script building.
- **Autonomous Diagnostics:** Proactive root-cause correlation and automated error resolution.



Human-in-the-Loop (HITL):

Every write asks for an explicit approval showing exactly what will change. There is no auto-approve mode in production.

Autonomous Business Recovery:

Builds an M365 recovery plan for a critical operations group from its real data footprint, turning hours of scoping into seconds.

Preemptive Recovery Engine:

Finds the problem, builds the plan, and executes it with your approval.

BUILT FOR EVERY SURFACE

Meets Practitioners Where They Already Work

Rubrik AI lives within the RSC console and extends beyond, sharing Rubrik's intelligence with other agents.

- **Agentic UX:** Natural-language interaction, blast-radius visualization, and automated recovery plans inside RSC.
- **MCP:** RSC interfaces let third party and custom agents query Rubrik metadata safely.

Governed by Design: Three layers keep every action safe: RBAC inheritance so Rubrik AI only ever sees what you can see, human-in-the-loop approval on every write, and guardrails against prompt injection, confidentiality risk, and hallucination. Every action is auditable, attributable, and nothing executes without your approval first.

Delivering Value Across the Organization

The same platform, read differently depending on who's asking.

CISOs & Security Leaders: Put one governable agent in front of the board and regulator, one that discovers, decides, and acts faster than the threat.

CIOs: Turn the platform you already run into the AI dividend, without a new procurement cycle.

AI & Governance Councils: Sign off on an agent that can't act without your approval and can't act without leaving a record, enforced by architecture, not a policy document.

Backup & Salesforce Admins: Diagnose a failed backup or job in minutes instead of hours of manual cross-referencing, and fix errors on approval.

Security Analysts & SOC Teams: Get blast radius and clean recovery point answers mid-incident, without switching consoles or waiting on the backup team.

Developers & Platform Teams: Build against Rubrik AI directly, governed the same way as everything else on the platform, without a new procurement cycle or a separate set of credentials.

Put the platform you already own to work as an agent, not just a tool. Learn more at rubrik.com/products/ai-powered-cyber-recovery.

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



Global HQ

3495 Deer Creek Road
Palo Alto, CA 94304
United States

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

Rubrik (NYSE: RBRK) is The Security and AI Operations Company, pioneering the AI Operations category as the enterprise control layer for artificial intelligence. We unify all AI agents across data, applications, and identity into one governed platform, transforming the way enterprises deploy, manage, and secure AI at scale. Built on our proven cyber resilience foundation, Rubrik uniquely delivers the visibility, control, and recovery capabilities that enable organizations to accelerate AI transformation while maintaining complete operational resilience.

For more information please visit www.rubrik.com and follow @rubrikinc on X (formerly Twitter) and Rubrik on LinkedIn. Rubrik is a registered trademark of Rubrik, Inc. All company names, product names, and other such names in this document are registered trademarks or trademarks of the relevant company.