Rubrik AI

Entwickelt mit Frontier-KI.
Ein KI-Agent, der erkennt, schlussfolgert, handelt und zusammenarbeitet.

KI hat die Zeit bis zur Ausbreitung eines Angriffs von 98 Tagen auf 39 Sekunden verkürzt. Mit diesem Tempo können weder Sicherheitsteams noch deren für menschliche Bediener ausgelegte Konsolen Schritt halten. Sie müssen diesen Rückstand jetzt aufholen. Das Problem darf nicht auf den nächsten Budgetzyklus verschoben werden.

Als branchenweit umfassendster Agent für Cyber-Resilienz basiert Rubrik AI auf Frontier-KI. Rubrik AI erkennt, schlussfolgert, handelt und teilt Informationen über Daten, Identitäten und Anwendungen hinweg, und zwar direkt innerhalb der RSC-Plattform (Rubrik Security Cloud), die Sie bereits nutzen. Ohne neue Konsole und ohne zusätzlichen Agenten.

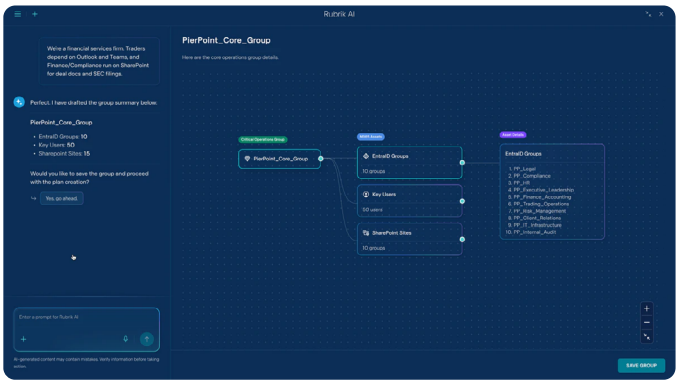
DIE RESILIENZLÜCKE IM MASCHINENTEMPO

Sicherheits- und IT-Teams sind mit einer wachsenden Kluft zwischen Bedrohungen im Maschinentempo und Tools im Menschentempo konfrontiert: isolierte Warnmeldungen, manuelle Fehleranalyse und KI-Agenten, die ihr Wissen nicht teilen können.

- **Angriffe im Maschinentempo:** Die Breakout-Zeit, also die Zeitspanne zwischen der ersten Infiltration und der Ausbreitung auf weitere Systeme, ist mittlerweile von Tagen auf Sekunden gesunken, doch ein Sicherheitsmodell, das auf menschlichen Reaktionszeiten basiert, kann nicht einfach verlangen, dass Menschen schneller arbeiten.
- **Zeitverlust durch manuelle Fehleranalysen:** Schon ein einzelner Backup-Fehler kann Stunden kosten, weil Fehlercodes abgeglichen und Signale manuell zusammengeführt werden müssen, um die Ursache zu finden.
- **Fragmentiertes Ökosystem aus KI-Agenten:** Ein SOC-Agent erkennt einen kompromittierten Host, weiß jedoch nicht, welche Daten sicher wiederhergestellt werden können. Diese Information befindet sich auf einer anderen Plattform, sodass ein Mitarbeiter die Daten manuell abrufen und Rückmeldung geben muss.
- **Generische KI stößt an ihre Grenzen:** Ein Chatbot oder eine Suche per Retrieval-Augmented Generation (RAG) in der Dokumentation kann Informationen liefern, kennt jedoch weder Rubrik-spezifische Fehlercodes noch API-Funktionen oder Wiederherstellungsprozesse und kann deshalb nicht handeln.

WIR STELLEN VOR: RUBRIK AI

Keines dieser Probleme lässt sich durch härteres Arbeiten lösen. Vielmehr brauchen Sie einen Agenten, der erkennt, was Ihnen entgeht, schneller Schlussfolgerungen zieht als Angreifer, in dem Moment handelt, in dem Sie das Signal geben, und sein Wissen mit Ihrer gesamten Umgebung teilt. Agentische Cyber-Resilienz basiert auf zwei Grundsätzen: Sicherheitsverletzungen sind unvermeidbar, agentisches Fehlverhalten ebenfalls. Rubrik AI ist nicht einfach ein weiteres Tool. Es ist ein Agent, der ein Ziel verfolgt: Ihre Resilienz. Rubrik AI analysiert Daten, Identitäten und Anwendungen, ermittelt in Maschinengeschwindigkeit die richtige Reaktion, nutzt vorhandene Fähigkeiten und macht sein Wissen im gesamten Technologie-Stack nutzbar.



KEIN SIGNAL BLEIBT VERBORGEN

Transparenz, die auf Fakten basiert

Rubrik AI arbeitet auf der Daten- und Identitätsebene, die Rubrik bereits schützt. Dadurch basiert die Analyse auf Ihrer tatsächlichen Umgebung und nicht auf Annahmen.

- **Antworten für die gesamte Umgebung:** Bietet Antworten zu Umgebungs-, Cluster- und Workload-Zustand, Schutzstatus, Kapazität und Compliance über VMware, Hyper-V, NAS, Oracle, SQL Server, Salesforce, M365 und cloudnative Workloads hinweg.
- **Basierend auf Live-APIs:** Greift auf echte RSC-Daten über dieselbe GraphQL-API zu, die auch die Konsole verwendet, nicht nur auf Texte und Dokumente. Nutzt die Wissensbasis, die auf Rubriks zehnjähriger Erfahrung beim Schutz von Kundenumgebungen basiert.
- **Standardmäßig proaktiv:** Erkennt Anomalien und Schutzlücken, bevor ein Administrator überhaupt auf die Idee kommt, danach zu suchen.

VOM SIGNAL ZUR ENTSCHEIDUNG – IN MASCHINENGESCHWINDIGKEIT

Fehleranalyse im Maschinentempo, nicht im Menschentempo

Rubrik AI analysiert Zusammenhänge auf Basis von Kontext, über den kein generischer Assistent verfügt, und plant anschließend in Maschinengeschwindigkeit die richtige Reaktion.

- **Umfassendes Fachwissen:** Bildet Rubrik-spezifische Diagnoseverfahren für VMware, Oracle, M365, Salesforce und weitere Umgebungen ab. Das ist institutionelles Wissen, das allgemeine Modelle nicht haben.
- **Eine Richtlinie, keine Ausnahmen:** Jede Entscheidung, unabhängig davon, ob sie von einem Menschen oder einem KI-Agenten getroffen wird, wird von derselben Richtlinien-Engine anhand derselben Leitlinien überprüft.

VON DER ANALYSE ZUR AKTION – OHNE MANUELLE ÜBERGABE

Von Anfang bis Ende ausgeführt – mit Freigabe bei jedem Schritt

Beschreiben Sie das gewünschte Ziel und Rubrik AI stellt mithilfe der vorhandenen Fähigkeiten zusammen, was getan werden muss, um es zu erreichen:

- **Agentengestützte Wiederherstellung:** Durch automatisierte Erkennung des Schadensumfangs und gezielte Priorisierung werden Ihre kritischen Geschäftsabläufe als Erstes wiederhergestellt.
- **Unverzügliche Übersicht:** Datenzuordnungen und visuelle Compliance-Berichte sind auf Abruf verfügbar, ohne dass Skripte manuell erstellt werden müssen.
- **Autonome Diagnose:** Vorfallsursachen werden proaktiv erkannt, abgeglichen und automatisiert behoben.



Human-in-the-Loop (HITL):
Jeder Schreibvorgang erfordert eine ausdrückliche Freigabe, die genau zeigt, welche Änderungen vorgenommen werden. Einen automatisierten Genehmigungsmodus für den Produktivbetrieb gibt es nicht.

Autonomous Business Recovery:
Erstellt für eine geschäftskritische Betriebsgruppe auf Basis ihres tatsächlichen Datenbestands einen Wiederherstellungsplan für M365 und verkürzt den Zeitaufwand für die Umfangsbestimmung von Stunden auf Sekunden.

Preemptive Recovery Engine:
Erkennt das Problem, erstellt den Plan und führt ihn nach Ihrer Freigabe aus.

FÜR JEDE UMGEBUNG GEEIGNET

Dort im Einsatz, wo Anwender bereits arbeiten

Rubrik AI ist in die RSC-Konsole integriert, agiert aber weiterreichend, indem es Rubriks Wissen mit anderen KI-Agenten teilt.

- **Agentenbasierte Benutzererfahrung:**
  Interaktionen in natürlicher Sprache, Visualisierung des Auswirkungsbereichs und automatisierte, in RSC integrierte Wiederherstellungspläne.
- **MCP:** RSC-Schnittstellen, über die Drittparteien- und benutzerdefinierte Agenten Rubrik-Metadaten sicher abfragen können.

„Governance by Design"-Ansatz: Drei Ebenen sorgen dafür, dass jede Aktion sicher bleibt – die Vererbung von RBAC-Berechtigungen, sodass Rubrik AI nur sieht, was auch Sie sehen können, Human-in-the-Loop-Freigaben für jeden Schreibvorgang sowie Sicherheitsmechanismen zum Schutz gegen Prompt-Injection, Vertraulichkeitsrisiken und Halluzinationen. Jede Aktion ist nachvollziehbar, kann der ausführenden Instanz zugeordnet werden und wird niemals ohne Ihre vorherige Zustimmung ausgeführt.

Mehrwert für das gesamte Unternehmen

Dieselbe Plattform, betrachtet aus unterschiedlichen Perspek**tiven:**

CISOs und Sicherheitsverantwortliche: Geben Sie Vorstand und Aufsichtsbehörden denselben steuerbaren Agenten an die Hand, der Bedrohungen beim Erkennen von Schwachstellen, beim Entscheiden und beim Handeln einen Schritt voraus ist.

CIOs: Nutzen Sie die Plattform, die Sie bereits betreiben, als Grundlage für Ihre KI-Dividende – ganz ohne neuen Beschaffungszyklus.

KI- und Governance-Gremien: Geben Sie einen Agenten frei, der nur mit Ihrer Zustimmung handelt und jede Aktion nachvollziehbar dokumentiert – verankert in der Architektur, nicht in einem Regelwerk.

Backup- und Salesforce-Administratoren: Erkennen Sie fehlgeschlagene Backups oder Prozesse in Minuten statt nach stundenlangem manuellem Abgleich und lassen Sie Fehler nach Ihrer Freigabe beheben.

Sicherheitsanalysten und SOC-Teams: Erhalten Sie während eines Vorfalls Antworten zum Angriffsausmaß und zu sauberen Wiederherstellungspunkten, ohne die Konsole wechseln oder auf das Backup-Team warten zu müssen.

Entwickler- und Plattformteams: Entwickeln Sie direkt auf Basis von Rubrik AI, mit denselben Governance-Mechanismen wie für alle anderen Plattformfunktionen – ohne neuen Beschaffungszyklus und ohne separate Anmeldedaten.

Setzen Sie die Plattform, die Sie bereits besitzen, als Agenten ein, nicht nur als Tool. Weitere Informationen finden Sie unter rubrik.com/de/products/ai-powered-cyber-recovery.

SAFE-HARBOR-ERKLÄRUNG:
In diesem Dokument angeführte unveröffentlichte Services oder Funktionen sind derzeit nicht verfügbar. Ob und wann diese allgemein bereitgestellt werden, liegt im Ermessen von Rubrik. Die genannten Services und Funktionen stellen keine Lieferversprechen, Zusagen oder Verpflichtungen von Rubrik dar und dürfen nicht Bestandteil eines Vertrags sein. Kunden sollten ihre Kaufentscheidung auf Services und Funktionen stützen, die derzeit allgemein verfügbar sind.

Hauptsitz
3495 Deer Creek Road
Palo Alto, CA 94304
USA

+1-844-478-2745
inquiries@rubrik.com
www.rubrik.com/de

Als führendes Unternehmen für Sicherheits- und AIOps-Lösungen etabliert Rubrik (NYSE: RBRK) den KI-gestützten Betrieb als Kontrollschicht für künstliche Intelligenz. Mit einer verwalteten Plattform, die alle KI-Agenten für Daten, Anwendungen und Identitäten zusammenführt, verändert Rubrik grundlegend, wie Unternehmen KI großflächig nutzen, steuern und sichern. Auf Basis unserer bewährten Cyber-Resilienz-Architektur bieten wir die entscheidende Transparenz, Kontrolle und Wiederherstellbarkeit, die es Unternehmen ermöglichen, die KI-Transformation zu beschleunigen, ohne Kompromisse bei der betrieblichen Ausfallsicherheit einzugehen.

Weitere Informationen finden Sie unter www.rubrik.com/de, unter @rubrikInc auf X (ehemals Twitter) sowie unter Rubrik auf LinkedIn.

Rubrik ist eine eingetragene Marke von Rubrik, Inc. Alle Firmennamen, Produktnamen und weiteren Bezeichnungen in diesem Dokument sind eingetragene Marken oder Marken des jeweiligen Unternehmens.

Rubrik-AI-Solution-Brief-Rubrik_IDML-de-DE#DTP_DUOOUU# / 20261001