rubrik

VEM DRIVING DIGITAL

TECH TALKS

AGENTI AI E IDENTITÀ:
cosa cambia per la sicurezza dei dati

IVAN ALBA

Senior Sales Engineer
Rubrik



40 YEARS ANNIVERSARY

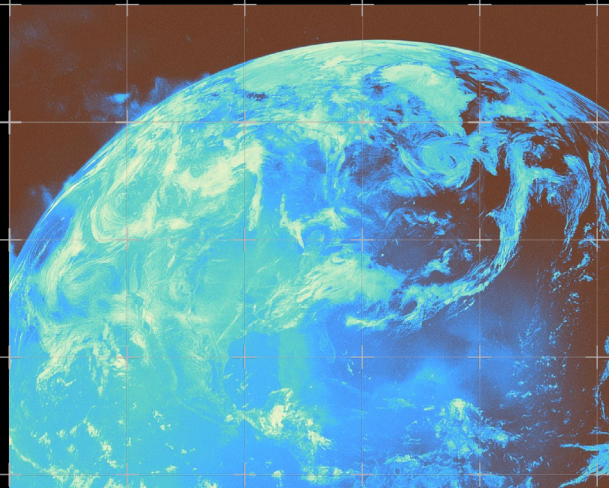
VALORI
ESPERIENZE
MERAVIGLIE

Own your identity before attackers (and agents) do.

Remove attacker persistence.
Recover clean and current.
Make it agentic resilient.

Ivan Alba
Senior Sales Engineer

rubrik



Identity is your single point of failure

82%

of detections involve no malware at all [1]

9 in 10

organizations had an identity-related incident last year [2]

AND AI IS DEMANDING A NEW PLAYBOOK FOR PROTECTING IT

OpenAI

"... AI-enabled cyber attacks will become **far more widespread and sophisticated**."

OpenAI letter
August 2026

Anthropic

"The cybersecurity community needs to **assume a fundamental change has occurred**."

"Disrupting the first reported AI-orchestrated cyber espionage campaign" report
Nov 2025

Google

"Industry standards are based on human response time and **insufficient to mitigate the threat**."

Sandra Joyce
VP, Google Threat Intelligence Group
June 2026

Microsoft

"The approaches built for a world of **human actors cannot keep pace with a world of AI**, agents and machine-speed attacks"

Hayete Gallot
EVP Microsoft Security
July 2026

© 2026 RUBRIK

1 CrowdStrike 2026 Global Threat Report
2 IDSA Trends in Identity Security 2025

The Modern Identity Attack

01

Gain access

- Phished credential
- Stolen session
- Helpdesk MFA reset

AI has made this easier

02

Escalate privileges

- Account to account
- Each one holds more
- Until one is admin

03

Move laterally

- Cloud and on prem
- Other IdPs
- AD sync servers

04

Build persistence

- Shadow admin
- Policy exclusion
- An IdP they control

05

Execute objective

- Backups deleted
- Encrypted, extorted
- Or nothing, for now

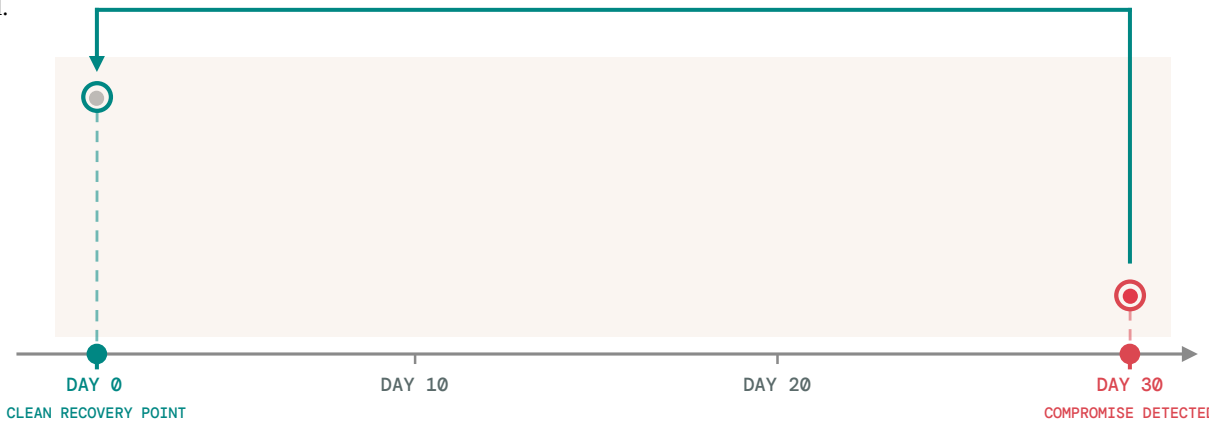
Restore to clean. Roll forward to current.

No other vendor removes attacker persistence AND brings every legitimate change forward

PHASE 01

Identify Clean Baseline

Go back to the last recovery point from before the attacker made changes. It's clean and persistence has been removed, but it's also weeks old.



© 2026 RUBRIK

Restore to clean. Roll forward to current.

No other vendor removes attacker persistence AND brings every legitimate change forward

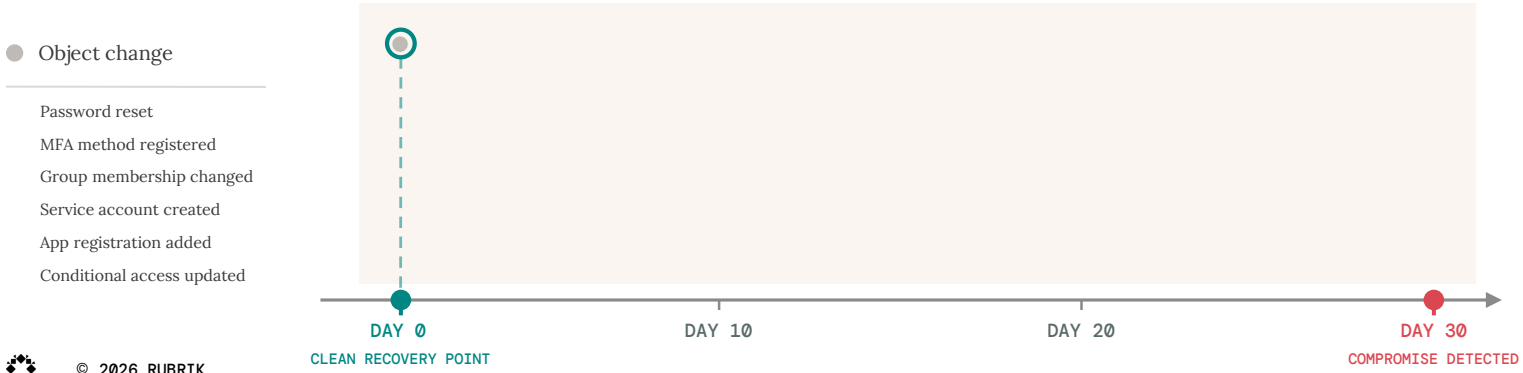
PHASE 01 — PHASE 02

Identify Clean Baseline

Go back to the last recovery point from before the attacker made changes. It's clean and persistence has been removed, but it's also weeks old.

Surface Every Change

Identify every user, group, and permission that changed between that point and now, across AD, Entra ID, and Okta.



© 2026 RUBRIK

Restore to clean. Roll forward to current.

No other vendor removes attacker persistence AND brings every legitimate change forward

PHASE 01 — PHASE 02 — PHASE 03

Identify Clean Baseline

Go back to the last recovery point from before the attacker made changes. It's clean and persistence has been removed, but it's also weeks old.

Surface Every Change

Identify every user, group, and permission that changed between that point and now, across AD, Entra ID, and Okta.

Classify Every Change

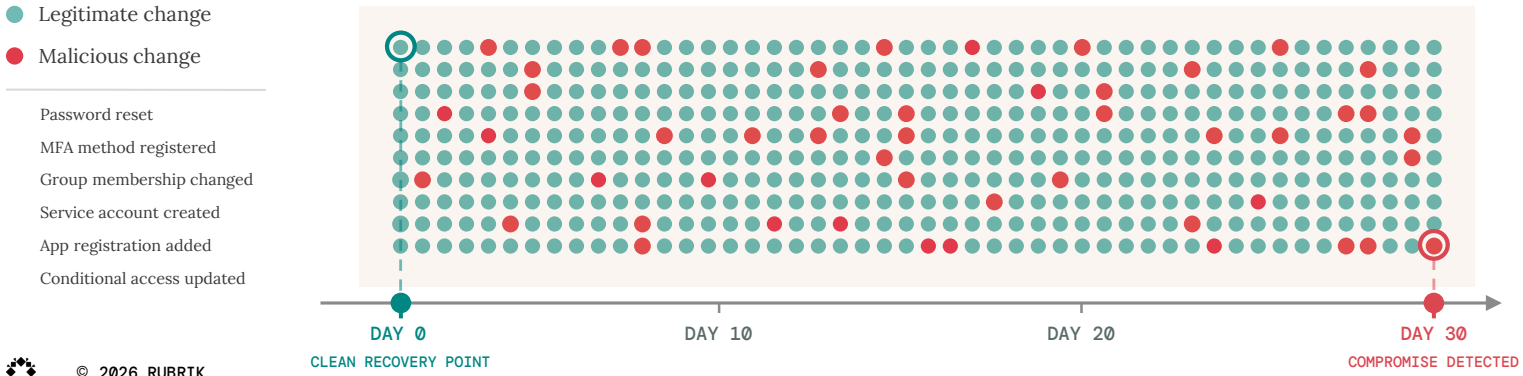
Check each one against your ITDR, HRIS and IGA to separate legitimate changes from malicious, so what took weeks now takes minutes.

Crowdstrike

Microsoft Defender

Sailpoint

Workday



© 2026 RUBRIK

Restore to clean. Roll forward to current.

No other vendor removes attacker persistence AND brings every legitimate change forward

PHASE 01 — PHASE 02 — PHASE 03 — PHASE 04

Identify Clean Baseline

Go back to the last recovery point from before the attacker made changes. It's clean and persistence has been removed, but it's also weeks old.

Surface Every Change

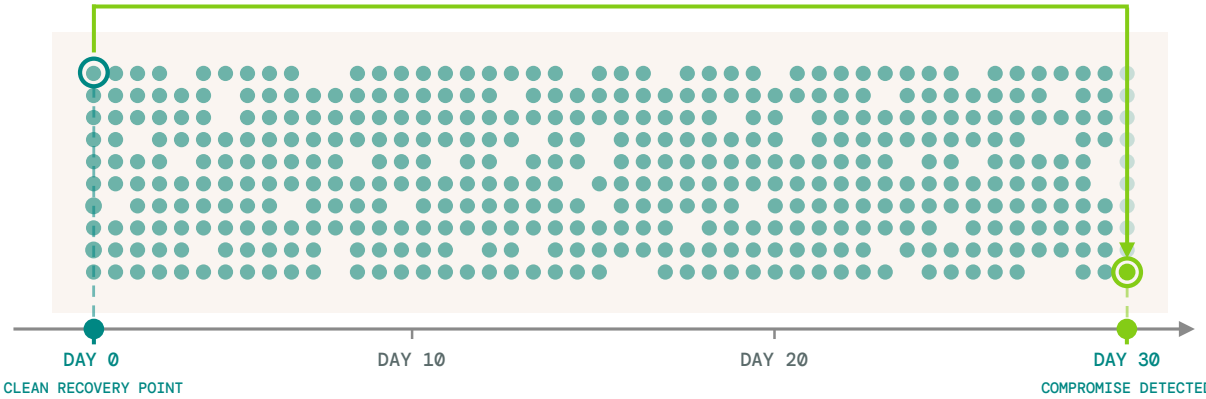
Identify every user, group, and permission that changed between that point and now, across AD, Entra ID, and Okta.

Classify Every Change

Check each one against your ITDR, HRIS and IGA to separate legitimate changes from malicious, so what took weeks now takes minutes.

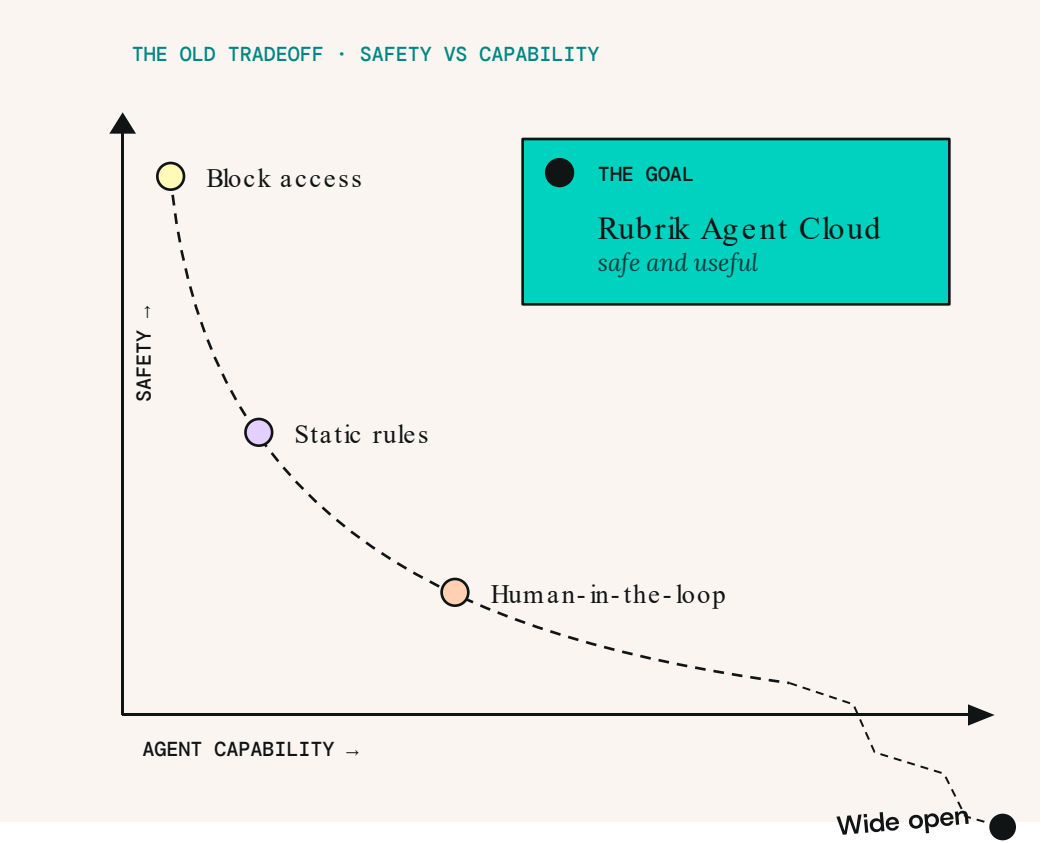
Roll Forward Legitimate Changes

Reapply the legitimate changes on top of the clean baseline, discarding the attacker's modifications



© 2026 RUBRIK

Your security stack wasn't built for agents



01 BLOCK ACCESS

Kills the ROI of AI

02 STATIC RULES

Captures 10–20% at best

03 HUMAN-IN-THE-LOOP

Not 24×7, not scalable

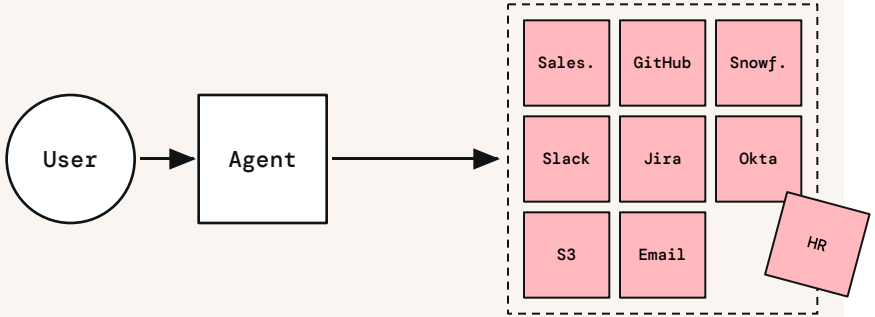
04 RUBRIK AGENT CLOUD

Every agent action verified in real time.
Useful and safe, at the same time.

© 2026 RUBRIK

Agent Identity

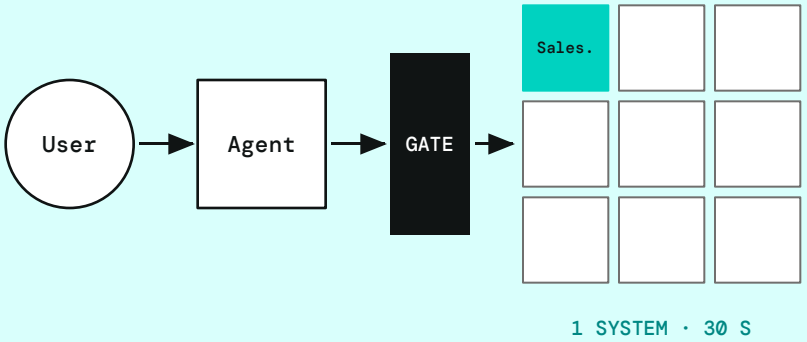
01 TODAY · BORROWED CREDENTIAL



The master key

Every door the user can open, for as long as the grant lives.

02 RUBRIK AGENT IDENTITY



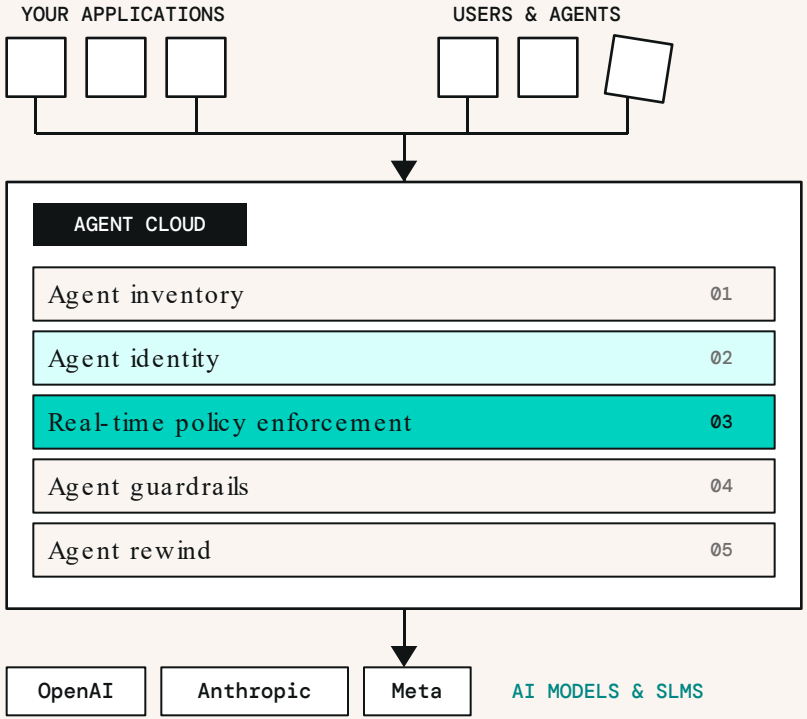
The day badge

Scoped, short-lived, named to the person and the agent.

Access decided at the moment of action. Nothing standing, nothing reused.

© 2026 RUBRIK

Rubrik Agent Cloud



01

Monitor

Full visibility into your agents and their actions, with granular app and identity understanding.

02

Secure with SAGE

Detect posture best practices at build time. Enforce custom AI guardrails at run time.

03

Remediate

Block dangerous actions and undo destructive actions to data.

© 2026 RUBRIK

One identity fabric, for humans and agents

From Agent Cloud we see identity. From Identity Resilience we see agents.

01 FROM IDENTITY RESILIENCE → AGENTS

Rubrik Identity Resilience

Agent activity on every identity
An identity's AI agent sessions, agents and models, right in the identity and alert pages.

Posture beyond humans
Service accounts, managed identities and agent identities, assessed for risk in one inventory.

Recover what agents depend on
Clean and current recovery of AD, Entra ID and Okta, the IdPs every agent authenticates through.

SHARED IDENTITY FABRIC



Active Directory



Entra ID



Okta

Humans · Service accounts · AI agents

02 FROM AGENT CLOUD → IDENTITY

Rubrik Agent Cloud

Every action has a name
Each tool call is attributed to a specific user + agent (on-behalf-of), never a shared service account.

Access minted by your IdP
Just-in-time, scoped tokens per tool call, federated with Entra ID and Okta.

Undo, not just block
Agent Rewind reverses the data and identity changes an agent already made.

Who did it, through which agent, with what access, and how to undo it. One platform, one answer.

© 2026 RUBRIK

Agentic Cyber Resilience: Data + Identity

Enterprise On-premises

Cloud

SaaS

Unstructured Data

Identity Providers

Agentic Platforms

Rubrik Security Cloud™

Cloud			
Enterprise	Data Discovery & Classification		
SaaS	Anomaly Detection	AD, Entra ID, Okta	Threat Containment
Unstructured	Threat Monitoring	Roll Back/Roll Forward	Orchestrated AD Forest Recovery
Identity Provider	Turbo Threat Hunting	Identity Recovery	Cyber Recovery Simulation
Data Protection	**Data Threat Analytics**	**Identity Resilience**	**Cyber Recovery**

Ruby AI Agent

Preemptive Recovery Engine

Automation | APIs

Autonomous MVB

CYBER INTEGRATIONS

- Palo Alto Networks
- Zscaler
- CrowdStrike
- Okta
- Mandiant

© 2026 RUBRIK

What Customers Achieve with Rubrik Identity Resilience

Deploy quickly. Recovery Faster. Simplify your identity security stack.

99%

Reduced AD forest recovery time from 11 days to just 3 hours

INTEGRIS HEALTH

<1 Day

Fully deployed Rubrik Identity Resilience within a single day

Renown® HEALTH

3 →1

Replaced three separate identity tools with one unified platform

RTX

© 2026 RUBRIK

Thank You and Let's Connect!

ivan.alba@rubrik.com



Ivan Alba

Senior Sales Engineer | Rubrik

© 2026 RUBRIK