



SECURING THE AUTONOMOUS ENTERPRISE:

STRATEGIES FOR GOVERNED AI AGENT INTEGRATION

Humans, non-Humans and AI Agents



Rubrik's Team for Hungary – Who is here?



Christian Putz
Regional Sales Manager



Jürgen Kaus
Security Consultant



Gergely Balogh
Sales Manager
Clico HUNGARY



Zsolt Almasi
Engineering Team Lead
Clico HUNGARY

Budapest 2025 (April)

Marks & Spencer breach linked to Scattered Spider ransomware attack

By [Lawrence Abrams](#)

April 28, 2025 04:28 PM 0



September 2025



Infosecurity
Magazine

JLR Hack UK's Costliest Ever, Hitting Economy with £1.9bn Loss





The Age of AI Agents - 2026





The Promise of AI Agents

Legal



60% to 80%
drop in first-
pass contract
review times

Marketing



Up to 46%
faster content
creation

Customer
Service



Fast first-
response times
leading to
increased
Customer
Satisfaction
(CSAT) scores

E-commerce



Reduce
shopping cart
abandonment
by up to 40%

Manufacturing



30% to 50%
reductions in
unplanned
downtime

Companies implementing AI agents see an average return of \$3.70 for every \$1 invested, with top performers achieving up to a \$10 return.

What just happened? (April 2026)

Used an access token (Identity)

Ignored instructions

Assumed wrong

Destroyed Infrastructure

Destroyed Backup

Claude-powered AI coding agent deletes entire company database in 9 seconds — backups zapped, after Cursor tool powered by Anthropic's Claude goes rogue

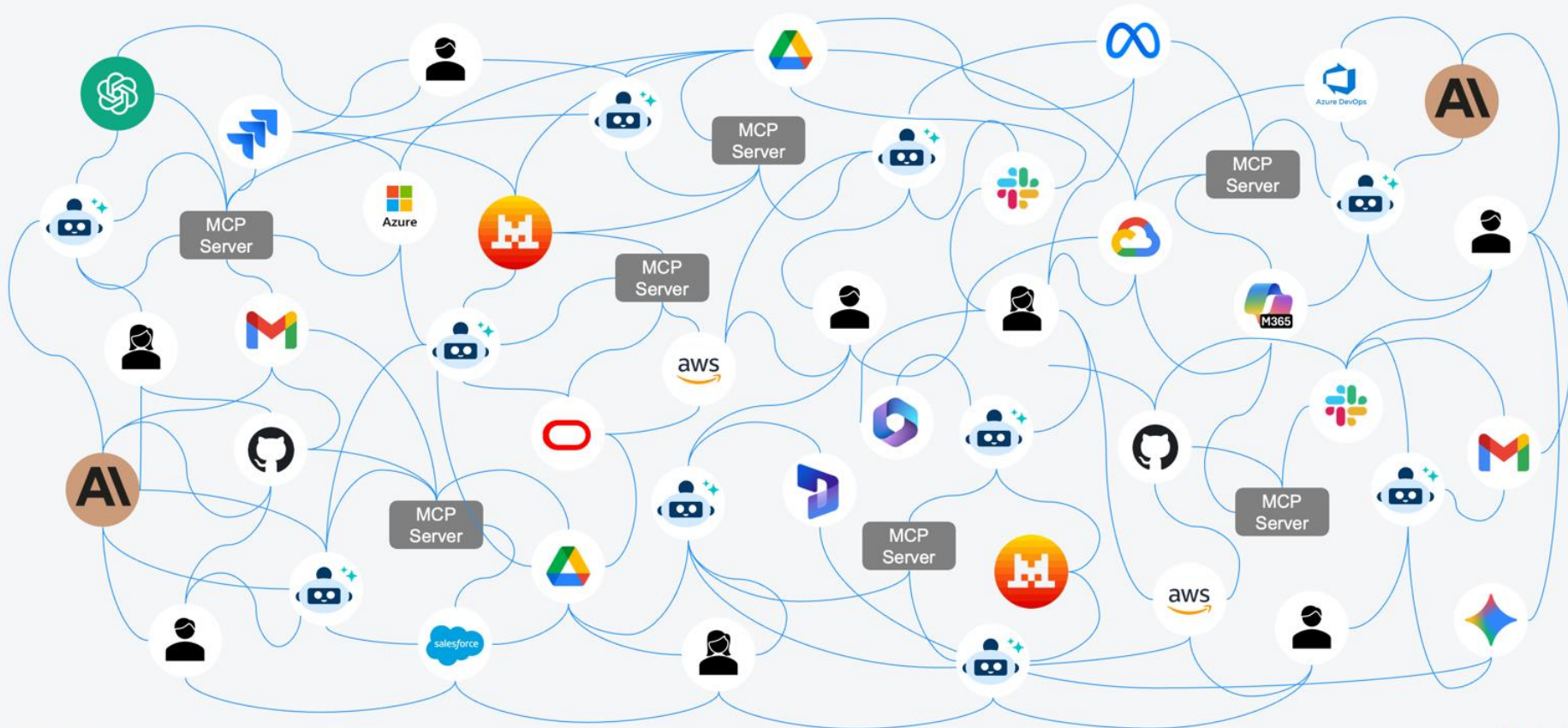
News

By [Mark Tyson](#) published 2 days ago

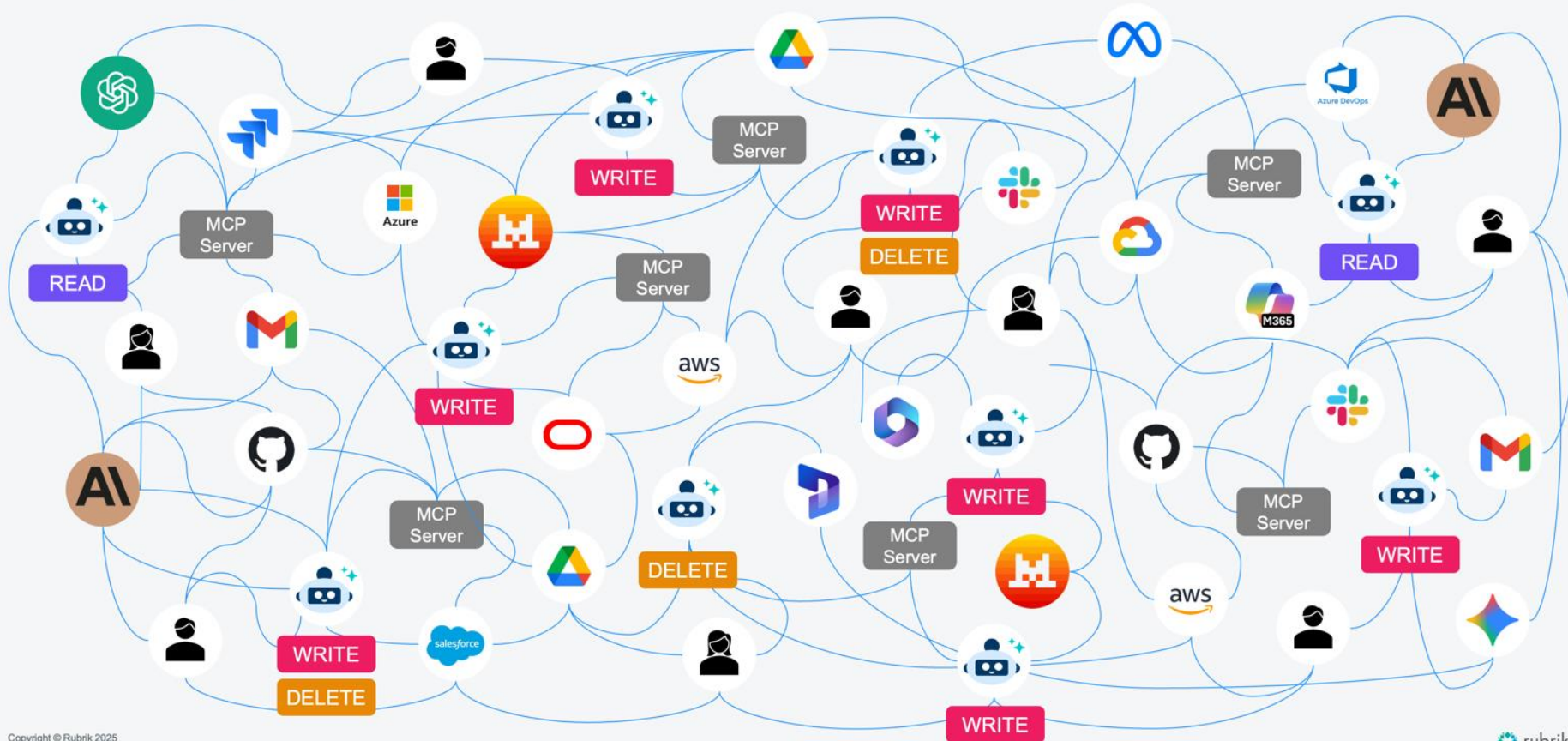
PocketOS founder blames 'Cursor running Anthropic's flagship Claude Opus 4.6' plus Railway's infrastructure for data disaster.



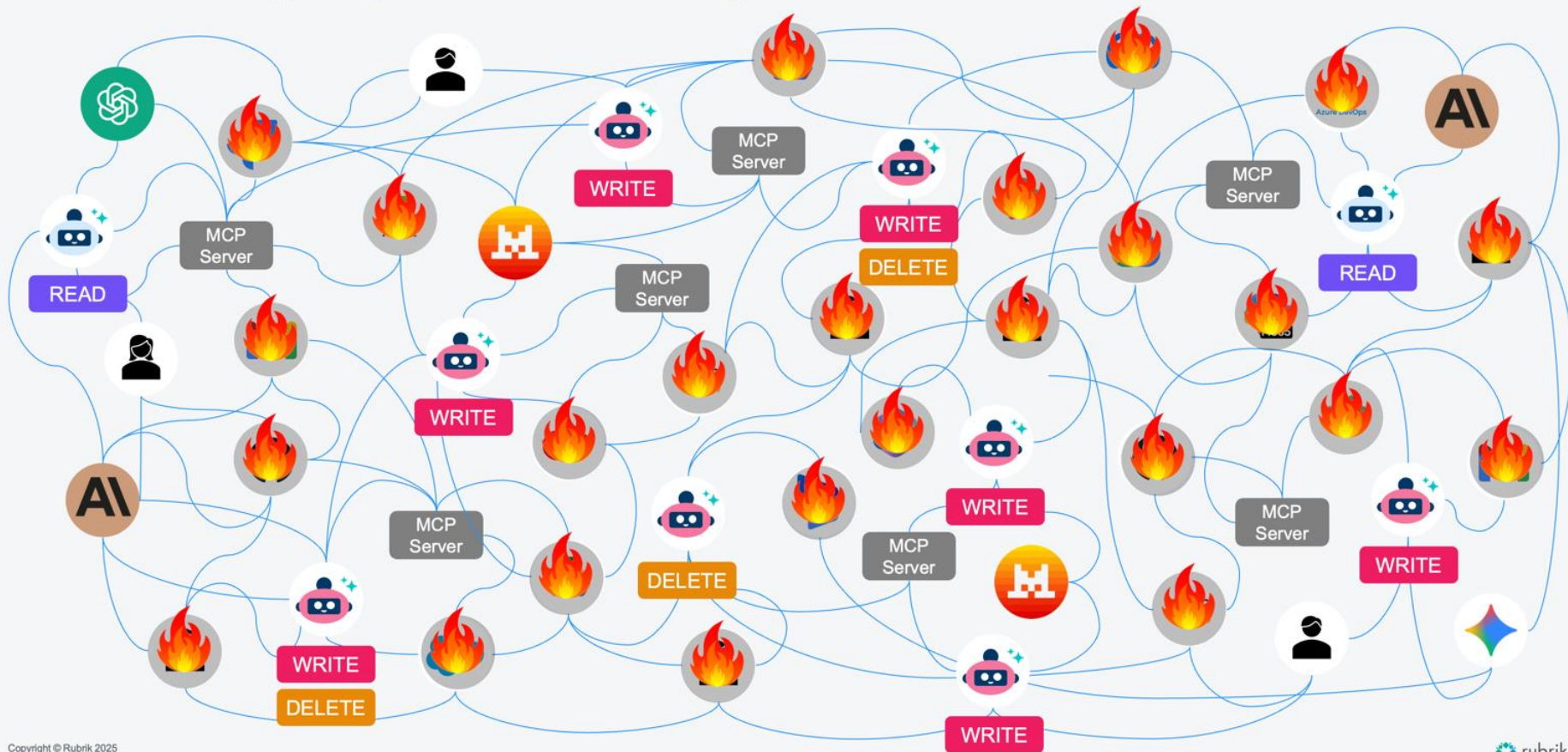
Managing Agents is Hard



More Agents = More Risk



Cascading Impact is Catastrophic



RUBRIK'S RESEARCH & DIRECTION

RBRK

Rubrik publicly listed April 2024



8000+

Global Clients

2.2+ Million

Snapshots daily Rubrik scans daily in search of threats embedded in backup data (43EB of managed customer data)

1,600+

Perspectives from 1,600+ IT and security leaders through Wakefield Research

Contributing Organizations

MANDIANT
now part of Google Cloud

CROWDSTRIKE



Microsoft

UNIT 42[®]
BY Palo Alto Networks

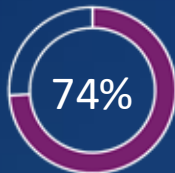
Identity



90% of IT and security leaders surveyed agreeing that identity-driven attacks are the single largest threat to their organizations

Backup and Recovery

74% of surveyed ransomware victims reporting threat actors were at least partially able to harm backup and recovery data



Agent AI



58% of surveyed leaders believe Agentic AI will be responsible for half or more of the cyberattacks next year

Mean Time to Recover

28% of respondents in 2025 believing they could fully recover in 12 hours or less



More at: zerolabs.rubrik.com



Introducing Rubrik for End-to-End Cyber Resilience

Unifying data protection, identity recovery, and AI operations

M365 Business Recovery

Autonomous MVB recovery in minutes. Up to 100x faster, clean, air-gapped restores.

Orchestrated Entra ID Recovery

Restore AD / Entra ID across hybrid environments in mere hours – on one air-gapped platform.



Unified AI Agent Operations

Rewind unintended agent actions instantly. Inventory & monitor co-pilot agents & enforce guardrails in real-time.

Data Access Governance

Discover, classify, and monitor sensitive data. Discover and remediate risky identities with sensitive data access.



Introducing Rubrik Agent Cloud

Unified Control Layer for Agent Operations

Rubrik Agent Cloud powered by Predibase brings together **Agents, Data, and Identity** under one roof





What choice do you have?

Expect AI Agents to be perfect, every time.

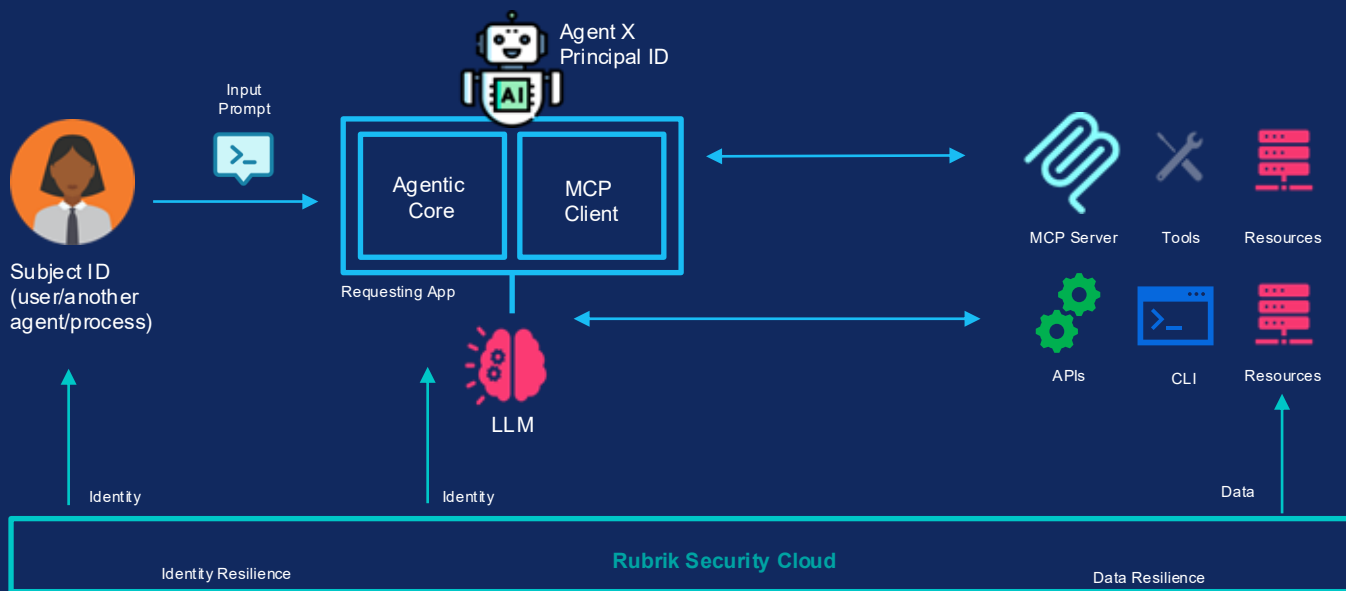


Independently verify and centrally enforce behavior.



The Foundation

None of this works without Data & Identity





Rubrik Platform

Resilience for Data, Identity, and AI





Benefits

- Accelerate prototype to production with confidence
- Automate governance committee
- Posture, threat, and remediation capabilities for SecOps
- Agent to Identity data graph for IAM team
- Rewind of data and systems to solve for agentic errors for IT Ops
- Win with AI



Unleash Agents.

Not Risk.