



NEWS RELEASE

New Rubrik Research Finds Identity Resilience is Imperative as AI Wave Floods the Workplace with AI Agents

2025-11-13

90% of Global Leaders Cite Identity Attacks as Top Concern, According to Rubrik Zero Labs

PALO ALTO, Calif.--(BUSINESS WIRE)-- New research from Rubrik Zero Labs uncovers a troubling gap between the expanding identity attack surface and organizations' ability to recover from resulting compromises. The AI wave is translating into an increase of AI agents in the workplace, which equates to a surge of both non-human identities (NHIs) and agentic identities. This is resulting in an urgent focus for CIOs and CISOs on identity threats and recovery. The report – Identity Crisis: Understanding & Building Resilience Against Identity-Driven Threats – shows that as AI adoption expands across organizations worldwide, enterprises are taking decisive action to strengthen identity resilience.

"I could have unlimited amounts of technology in place. But if someone socially engineers our support desk to hand over admin passwords, that's the end of the game," said Andrew Albrech, Chief Information Security Officer at Dominos. "That's why identity resilience is key."

Illustrating this trend:

- 89% of organizations plan to hire professionals within the next 12 months specifically to manage or improve identity management, infrastructure, and security.
- 87% of IT and security leaders actively plan to change Identity and Access Management (IAM) providers or



have already begun the process.

- 58% cite security concerns as the primary driver to switch IAM providers.

"The rise of identity-driven attacks is changing the face of cyber defense," said Kavitha Mariappan, Chief Transformation Officer at Rubrik. "Managing identities in the era of AI has become a complex endeavor, especially with the labyrinth of NHIs. We have an under-the-radar crisis on our hands where a single compromised credential can grant full access to an organization's most sensitive data. Attackers are no longer breaking in, but logging in, and comprehensive Identity Resilience is absolutely critical to cyber recovery in this new landscape."

Agentic AI Opens the Door to New Identity Challenges

As organizations integrate agents into their workflows, NHIs will continue to outpace the growth of human identities. In fact, industry **reports** contend that NHIs now outnumber human users by 82-1. Securing NHIs will become as essential – if not more – as securing human identities, given the growing complexity of managing AI agent operations.

Rubrik's research found that:

- 89% of respondents have fully or partially incorporated AI agents into their identity infrastructure, and an additional 10% have plans to.
- Over half of IT security decision makers(58%) estimate that in the next year, 50% or more of the cyberattacks they deal with will be driven by agentic AI.

Weakening Confidence in Recovery Strategies Highlights Need for Identity Resilience

Identities are the keys to access an organization's most sensitive data. Therefore, IT and security leaders must build resilient identity services and infrastructures to ensure a quick recovery and restoration of operations in the face of an attack.

However, overall confidence in recovery times is declining. Rubrik's research finds that:

- In 2025, only 28% of respondents believed they could fully recover from a cyber incident in 12 hours or less, compared to 43% in 2024.
- Over half (58%) of respondents believe it would take at least two days to recover and achieve full-service operations post-compromise.
- Of those who experienced a ransomware attack in the past year, 89% paid a ransom to recover their data or stop the attack.

Organizational concern over the state of identity security is valid, and IAM tools alone are not enough to properly

address these challenges. CIOs and CISOs need a comprehensive identity resilience strategy for when, not if, an attack strikes.

To read the full report, visit <https://zerolabs.rubrik.com/>.

Methodology

The Rubrik Zero Labs Survey was conducted by **Wakefield Research** among 1,625 IT Security Decision-Makers at companies of 500 or more employees with a 50/50 split of Directors/VPs and CIOs/CISOs. The research was conducted in three regions: US, EMEA (UK, France, Germany, Italy, Netherlands), and APAC (Japan, Australia, Singapore, India), between September 18th and September 29th, 2025, using an email invitation and an online survey.

About Rubrik

Rubrik (RBRK), the Security and AI Operations Company, leads at the intersection of data protection, cyber resilience, and enterprise AI acceleration. Rubrik Security Cloud delivers complete cyber resilience by securing, monitoring, and recovering data, identities, and workloads across clouds. Rubrik Agent Cloud accelerates trusted AI agent deployments at scale by monitoring and auditing agentic actions, enforcing real-time guardrails, fine-tuning for accuracy and undoing agentic mistakes. For more information, please visit www.rubrik.com and follow [@rubrikinc](https://twitter.com/rubrikinc) on X (formerly Twitter) and [Rubrik](https://www.linkedin.com/company/rubrik) on LinkedIn.

Media Contact

Meghan Fintland
Head of Global PR
925.785.9192
press@rubrik.com

Source: Rubrik