



Identity Management Found to be Critical Gap in Agentic AI Deployments, According to Survey of C-Level and IT Leaders by Technology Analysts

July 16, 2026

90% of respondents say they need identity-management improvements to address AI-related risks, including the surge of non-human identities gaining always-on access to corporate data

TINTON FALLS, N.J., July 16, 2026 /PRNewswire/ -- Commvault (NASDAQ: CVLT), a leader in unified resilience at enterprise scale, today announced findings from the IDC White Paper, Resilience Operations: The Discipline that Makes Readiness Provable, July 2026, sponsored by Commvault, that reveal a gap between the rapid pace of AI adoption and the identity resilience capabilities needed to support it. In tandem, the company also announced the IDC Cyber Readiness Assessment, sponsored by Commvault, an interactive tool that organizations can use to evaluate resilience preparedness for an AI-driven future.



The research was conducted among 539 IT and resilience decision makers in North America, of which approximately 85% have experienced a cyber incident. It found that 90% of respondents believe they need to improve identity-management capabilities to address risks introduced by agentic AI systems. Identity management is a discipline of controlling and governing digital identities, including both human and agent identities, and their access to systems and data across their lifecycle – from creation to decommissioning.

As more organizations deploy agents in volume, the rise in non-human identities – many of which have always-on access and can multiply on demand – may rapidly outnumber human identities. Nearly two-thirds of respondents (58.7%) say significant improvements or a complete overhaul of their identity-management approach is required.

The research also found that:

- Among respondents, 26.7% have dynamic role-based access control (RBAC) supporting AI and analytics.
- Also, 24.7% of respondents have documented and tested their Active Directory and Entra ID capabilities.
- Almost all (98.4%) respondents expressed the need for better collaboration between the teams responsible for IT and security. Additionally, 49.7% say major improvements are needed.

"AI is fundamentally changing how organizations operate, make decisions, and manage risk," said Vidya Shankaran, Field CTO, Commvault. "But many organizations are discovering that the systems designed to govern people are not prepared to govern a growing population of AI agents, machine identities, and autonomous workflows. Identity is a critical Tier 0 application and has a pivotal role to play in an organization's confidence in a clean recovery."

Minimum Viability Awareness is Lacking

The research also points to a broader resilience challenge. More than half of the organizations surveyed (57.7%) have not fully defined their Minimum Viable Business (MVB). At the same time, many continue to face gaps in recovery orchestration, cleanroom capabilities, and cyber-resilience readiness.

To address these challenges, there is a growing need for Resilience Operations (ResOps), an emerging operational discipline that continuously brings together business, security, infrastructure, data protection, and recovery teams around a common objective: maintaining business operations and accelerating recovery in the face of disruption.

"IDC predicts that ResOps will mature from an emerging discipline into a mainstream enterprise capability over the next three to five years," said Frank Dickson, Group Vice President for IDC's Security & Trust research practice. "Organizations that build the governance structures, technical capabilities, and testing disciplines now, before the next major incident, will be better positioned to absorb disruption, protect their customers, and sustain competitive operations in an increasingly hostile threat environment."

Putting Readiness to the Test

To help businesses better understand their current preparedness state, IDC's Cyber Readiness Assessment, sponsored by Commvault, will enable organizations to evaluate their cyber resilience maturity and identify areas where identity, protection, detection, response, and recovery capabilities may require improvement. The assessment is based on the same maturity framework developed through the research and provides participants with a personalized readiness profile.

Methodology

IDC surveyed 539 North American enterprise organizations. Eighty percent of respondents were from the United States, and the remaining 20% in Canada. All respondents were either senior IT decision makers or C-level leaders with extensive knowledge of their organization's resilience posture and strategy.

More Details and Availability

Findings are detailed in the IDC White Paper, Resilience Operations: The Discipline that Makes Readiness Provable, sponsored by Commvault (Doc #US54630626, July 2026). The Cyber Readiness Assessment and white paper are available [here](#). The Cyber Readiness Assessment tool will be available in the coming months.

About Commvault

Commvault (NASDAQ: CVLT) is a leader in unified resilience at enterprise scale. In a constantly evolving threat landscape, Commvault keeps customers ready by unifying data security, identity resilience, and cyber recovery, on one cloud-native, AI-enabled platform. Customers trust Commvault to conduct the fastest, most complete recoveries – not just their data, but their entire business. Purpose-built for the agentic enterprise, Commvault also enables organizations to safely embrace AI while protecting against AI-driven threats.

 View original content to download multimedia: <https://www.prnewswire.com/news-releases/identity-management-found-to-be-critical-gap-in-agentic-ai-deployments-according-to-survey-of-c-level-and-it-leaders-by-technology-analysts-302826656.html>

SOURCE COMMVAULT

Kevin Komiega, Commvault, 978-834-6898, kkomiega@commvault.com | Investor Relations Contact: Michael J. Melnyk, CFA, Commvault, 646-522-6160, mmelnyk@commvault.com