Commvault Encourages Organizations to Adopt a Four-Step Approach to Resilience in the Age of Frontier AI

June 1, 2026

Frontier models like Mythos and GPT-5.5-Cyber excel at rapidly identifying vulnerabilities, but may also expose exploitable threats to bad actors faster, making resilience essential

TINTON FALLS, N.J., June 1, 2026 /PRNewswire/ -- Commvault (NASDAQ: CVLT), a leader in unified resilience at enterprise scale, recommends four steps organizations should take to stay resilient in the age of Frontier AI – where advanced AI models are accelerating vulnerability discovery, compressing exploitation timelines, and elevating the need for resilience.

Frontier AI is reshaping the threat landscape in two ways. First, advanced models are generating a deluge of Common Vulnerabilities and Exposures (CVEs) – Palo Alto Networks research shows AI cybersecurity models identified more than seven times the typical number of vulnerabilities found within a single month during testing.[1] Second, attacks are becoming autonomous: once a vulnerability is disclosed, AI-assisted exploitation can now emerge within minutes, not weeks.[2] The remediation window for organizations is collapsing – no vendor is immune. Resilience is no longer a recovery plan, it's an operating requirement.

"Frontier models change the economics of vulnerability discovery. AI models will reveal exploitable vulnerabilities at such a fast pace, remediation programs must evolve," said Nick Patience, VP and AI Practice Lead, Futurum Group. "While a rigorous patching strategy remains critical, the key now is also making sure readiness, resilience, and clean recoveries are top priorities."

Four Critical Steps for Resiliency in the Frontier AI Era
To help enterprises prepare for the Frontier AI era, Commvault recommends that organizations embrace a preparedness framework that includes four key steps:

1. **Evaluate recovery risks:** IT and security teams should assess whether their current recovery posture can withstand fast-moving vulnerability discovery and exploitation cycles. This means looking beyond whether backups exist and asking harder questions: Can critical systems be restored cleanly? Are recovery environments isolated from compromised production systems? Are recovery plans mapped to key dependencies?
2. **Make isolated recovery and air gapping the baseline:** Organizations should assume that some vulnerabilities, software flaws, or third-party exposures may outpace normal remediation cycles. Maintain immutable, isolated copies of critical data and workloads, separated from production identity, network, and management planes. These copies help provide a clean fallback when patching or when remediation cannot keep pace. Organizations should also pressure-test RTOs and RPOs against realistic attack scenarios – not just failure modes. If your recovery time objective was set before autonomous exploitation was possible, it was set for a different world.
3. **Prioritize systems the business cannot operate without:** Identify the systems required to function as a minimum viable company, including identity platforms, billing systems, operational databases, and cloud services, and define the order in which they must be recovered. As AI becomes embedded into business operations, organizations should also assess newer dependencies such as data pipelines, model repositories, vector databases, and agentic workflows.
4. **Automate resilience and test continuously:** Recovery plans cannot remain static documents in the Frontier AI era. Organizations should automate threat scanning, clean recovery point identification, dependency-aware restoration, and recovery orchestration, while regularly testing plans in isolated cleanroom environments before incidents occur.

"Organizations that embrace this four-step process will be better suited to take advantage of rapidly evolving AI models while also mitigating the risks," said Patience.

"Resilience continues to be a high priority for us," said Jayson Morgan, SVP Infrastructure, BOK Financial Corporation. "What matters isn't simply whether backups exist, but whether we can recover cleanly, validate integrity, and resume operations fast when it matters most."

Embracing Resilience Operations (ResOps) for a Resilient Future
ResOps is the operating model that makes this framework actionable. It operationalizes resilience through continuous testing, measurable recovery readiness, clean recovery validation, and protection of both production and recovery environments. It's foundational for business continuity during cyberattacks, outages, and AI-driven disruptions.

"AI models will continue to evolve that accelerate remediation timelines and require a new approach to readiness," said Bill O'Connell, Chief Security Officer, Commvault. "ResOps gives organizations a way to continuously validate readiness, advance clean recoveries, restore systems with confidence, and build resilience into the way they operate."

More Details
To learn more about preparedness in the age of Frontier AI, check out the following:

- A companion blog that delves further into best practices for resilience.
- Four Critical Steps for Resiliency in the Frontier AI Era, a video to help organizations close the gap between AI-powered attacks and recovery readiness.
- A webinar that discusses how AI is changing the threat landscape, and the practical steps organizations can take to build stronger resilience.

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.

[1] Sabin, S. (2026, May 13). Exclusive: Palo Alto Networks says new AI models found 7x more vulnerabilities. *Axios*. https://www.axios.com/2026/05/13/palo-alto-networks-mythos-gpt-cybersecurity
[2] Ferreira, B. (2026, May 12). Standard 90-day vulnerability disclosure policy is likely dead thanks to AI, expert warns that AI can weaponize patches in 30 minutes — LLM-assisted bug-hunting ushers in a new cyberworld order. *Tom's Hardware*. https://www.tomshardware.com/tech-industry/cyber-security/standard-90-day-vulnerability-disclosure-policy-is-likely-dead-thanks-to-ai-leaving-worlds-systems-exposed-to-zero-day-attacks-security-expert-details-how-llm-assisted-bug-hunting-ushers-in-a-new-cyberworld-orders

View original content to download multimedia:https://www.prnewswire.com/news-releases/commvault-encourages-organizations-to-adopt-a-four-step-approach-to-resilience-in-the-age-of-frontier-ai-302786510.html

SOURCE COMMVAULT

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