Commvault Expands Threat Scan with Layered Threat Detection to Advance Verified Clean Recoveries

March 18, 2026

Delivers 'defense-in-depth' with rapid IOC-based hunting and advanced file level inspection; integrates threat hunting with Synthetic Recovery to unify resilience workflows

TINTON FALLS, N.J., March 18, 2026 /PRNewswire/ -- Commvault (NASDAQ: CVLT), a leader in unified resilience at enterprise scale, today announced expanded threat hunting capabilities within Commvault Cloud Threat Scan. The enhancements help organizations rapidly identify risks within backup environments and recover validated clean data, reducing reinfection risks and prolonged downtime.

According to recent reports, the median dwell time for a non-actor disclosed breach is 24 days[1], giving attackers ample opportunity to silently embed malicious code across systems. While security operations teams often possess intelligence tied to specific indicators of compromise (IOCs) or indicators of attack (IOAs), that intelligence must also be applied across backup data before restoration begins. Without clear visibility into backup integrity, organizations risk reintroducing threats, extending outages, and compounding business disruption.

Intelligence-Driven Threat Hunting at Enterprise Scale
To address this challenge, Commvault now delivers two complementary scanning modes within Commvault Cloud Threat Scan:

- **Hyper Threat Hunting** enables targeted searches across backup data using threat hunting artifacts such as hashes and YARA rules to identify known indicators of compromise at scale. Hash-based hunting provides fast, index-based detection, while YARA-based analysis supports more targeted pattern matching for deeper investigation.
- **Deep Inspection** provides layered file-level analysis using malware signatures, machine learning, heuristic analysis, and AI-enabled encryption detection to uncover known threats, suspicious variants, and ransomware related activity that may evade exact-match indicators alone.

Together, these detection modes allow close collaboration across incident response and recovery teams to isolate affected data and make informed recovery decisions. They can schedule recurring scans for continuous monitoring or conduct targeted searches during active incident response scenarios, providing flexibility for both ongoing protection and time-sensitive response.

"In an era where attacks adapt faster than defenses, our priority is to get ahead of every threat," said Dr. Erika Voss, Chief Security Officer at Blue Yonder. "Being able to validate recovery data against current threat indicators is one way to stay ahead of it — ensuring we have more control in an unpredictable landscape."

From Detection to Verified Recovery
Commvault integrates these threat detection capabilities with its patent-pending Synthetic Recovery technology – unifying detection and recovery workflows. Once risks are identified, Commvault's AI-enabled Synthetic Recovery offering can help surgically remove compromised datasets during recovery while restoring clean data to production systems. With Synthetic Recovery, organizations can maximize data preservation while simultaneously achieving data cleanliness.

"We're seeing a fundamental shift in how organizations approach recovery operations. The market is demanding integrated solutions that combine threat detection with recovery workflows, and Commvault's layered approach to verified clean recoveries represents where the industry is heading," said Fernando Montenegro, VP and Practice Lead Cybersecurity at The Futurum Group.

This announcement continues to demonstrate how Commvault is advancing the ResOps operating model. Instead of operating in silos across IT and security, ResOps connects people, processes, and technology, so organizations can manage resilience as a continuous enterprise-wide discipline.

"Security and IT teams need to operate from the same playbook during an incident. Threat intelligence at scale is increasingly table stakes — what sets us apart is what happens next," said Pranay Ahlawat, Chief Technology and AI Officer at Commvault. "By layering our proprietary signal correlation and AI-enabled algorithms on top of targeted threat hunting, and connecting that directly to verified recovery, we give organizations something powerful: not just the ability to find threats fast, but the confidence

that what they restore is clean."

Availability
Threat Scan is available globally and is sold as a standalone offering as well as part of Commvault's cyber resilience bundle. The new threat hunting capabilities are generally available and will be provided at no additional cost to existing Threat Scan customers.

Join Commvault at RSAC 2026
Commvault's latest Threat Scan offerings take center stage at this year's RSA Conference (Booth #S-0634) from March 23-26 in San Francisco. Show attendees can grab a ringside seat for the ResOps Rumble where resilience and operations join forces to deliver unified cyber recovery, identity resilience, and data security. Register today for ransomware recovery demos and sessions, expert insights on identity resilience and clean recovery, and the ultimate prize – unified resilience for your organization.

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] Verizon. (2025). *2025 Data Breach Investigations Report*. https://www.verizon.com/business/resources/T16f/reports/2025-dbir-data-breach-investigations-report.pdf

View original content to download multimedia:https://www.prnewswire.com/news-releases/commvault-expands-threat-scan-with-layered-threat-detection-to-advance-verified-clean-recoveries-302716567.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