Commvault Expands Microsoft Security Integration to Turn Threat Intelligence into Recovery Action

November 18, 2026

New integration connects Microsoft Defender for Endpoint with Commvault Threat Scan to investigate potentially affected recovery points and make better-informed recovery decisions to reduce reinfection risk

TINTON FALLS, N.J., Nov. 18, 2026 /PRNewswire/ -- Commvault (NASDAQ: CVLT), delivering continuous recovery for the AI era, today announced a new integration between Commvault Threat Scan and Microsoft Defender for Endpoint. When Microsoft Defender detects a potential cyberattack, Commvault uses that information to identify which systems and backups may be affected, helping organizations investigate potential risks and make faster, better-informed recovery decisions.

After a breach, organizations need to know what data they can trust to restore critical operations. Yet only 35% of organizations have automated processes that identify backups as safe for recovery, according to a recent IDC study sponsored by Commvault.[1]

The new integration helps close that gap by adding another signal to identify recovery points that may require a closer look. Organizations can now:

- **Identify potential threats to backups:** Use Microsoft Defender security alerts to find potentially affected systems and backups, automatically scanning them for threats.
- **Make better-informed recovery decisions:** Give security and recovery teams shared threat context to better understand potential risks before selecting data to recover.

"A cyberattack isn't over when the threat is contained. It's over when the business can recover cleanly," said Pranay Ahlawat, Chief Technology and AI Officer, Commvault. "Bringing Microsoft Defender signals into Threat Scan gives teams more intelligence to identify risk in their backups and choose clean recovery points with confidence."

"After a cyberattack, recovery teams need to know why security flagged a system and which backups may be affected," said Don Gentile, Analyst, Data Platforms and Resiliency at HyperFRAME Research. "Connecting Microsoft Defender alerts with Commvault Threat Scan helps teams use that security intelligence to focus their investigation and choose a recovery point with greater confidence."

Availability
The Microsoft Defender for Endpoint integration with Commvault Threat Scan is generally available today. There is no change in pricing for the integration. Customers must have Microsoft Defender for Endpoint and Commvault Threat Scan.

This new integration builds on existing security integrations Commvault has with Microsoft today. Commvault also integrates with Microsoft Sentinel across Threat Scan and Risk Analysis, helping customers connect security intelligence with resilience and recovery workflows.

Additional Resources

- Learn more about Commvault Threat Scan
- Learn more about Commvault and Microsoft
- Visit Commvault at Microsoft Ignite 2026

About Commvault
Commvault (NASDAQ: CVLT) delivers continuous recovery for the AI era. We help organizations stay ready for constant disruption by returning critical data, applications, identities, and AI systems to a clean, trusted state. Our purpose-built recovery solutions span cloud-native and hybrid environments, leveraging AI to enable resilience at enterprise scale.

[1] Goodwin, P., Dickson, F., & Robinson, C. (2026). *Resilience Operations: The Discipline That Makes Readiness Provable.* IDC. https://www.commvault.com/resources/analyst-report/resilience-operations-the-discipline-that-makes-readiness-provable

View original content to download multimedia:https://www.prnewswire.com/news-releases/commvault-expands-microsoft-

security-integration-to-turn-threat-intelligence-into-recovery-action-302942510.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