IDC Link
Real-Time IDC Research® Opinion on Industry News, Trends, and Events

Commvault Introduces "Resilience Ops" at SHIFT 2025

November 21, 2025

By: Phil Goodwin, Archana Venkatraman, Johnny Yu

IDC'S QUICK TAKE

No one disputes that resilience — whether business, data, or cyber — is an organizational imperative, and putting the necessary people, process, and technology into place can be challenging. At its recent Commvault SHIFT 2025 event in NYC, Commvault introduced the concept of "Resilience Operations," or "ResOps," as a framework to bring together the needed components within organizations.

EVENT HIGHLIGHTS

Commvault SHIFT is the company's annual event during which it makes its most important announcements. This year's event carried a number of such announcements, including:

- **"ResOps":** While not a product announcement, Commvault coined the term *ResOps* to describe its efforts to consolidate the people, processes, and technologies needed to improve business resilience. Although Commvault does not claim to supply all elements, ResOps is a way for IT organizations to think about creating the ecosystem needed to achieve resilience. ResOps, as described by Commvault, includes data discovery and access control, anomaly and indicators of compromise (IoCs) detection, and clean recovery of trusted data.
- **Commvault Cloud Unity:** This cloud-native platform, the next generation of Commvault Cloud, is directly related to ResOps as it unifies Commvault's solutions around data security, identity security, governance, and recovery across data and applications whether on premises or in the cloud.
- **Synthetic recovery:** Determining the last known clean data point is essential for recovering from cyberattacks with minimal data loss. Commvault's synthetic recovery is an AI-enabled method to curate backups and snapshots and assemble a safe recovery point based on last known clean versions of individual files and objects.
- **AI-driven UI for enterprisewide backup policies:** Though introduced in SHIFT 2023, the company's AI agent, "Arlie," has been enhanced to offer "conversational resilience" utilizing voice interaction for Arlie Advisor and Arlie Recovery agentic automation.
- **Enhanced security:** Security in Commvault Cloud Unity is based on an adaptive fabric across on-prem and cloud environments. It enhances trust using security

zones, a hardened OS based on Linux the company has dubbed "vault OS", zero trust, and advanced encryption including post-quantum cryptography (PQC).

- **Identity resilience:** Commvault has announced expanded protection for Microsoft Active Directory with support for EntraID and Okta in the near future. As cyberattackers focus more on disabling identity management systems as a means of extracting a ransom, the ability to protect and recover these systems is increasingly important. Commvault's focus is on adding proactive capabilities such as vulnerability assessments and audit to offer a clear view of the security posture of identity and access management.
- **Acquisition integration:** Commvault's acquisitions of Satori (AI data governance and security) and Clumio (autonomous AWS data protection) are now appearing as integrated components of Commvault Cloud Unity.

IDC'S POINT OF VIEW

The data protection software market has been evolving rapidly over the past several years, driven by cyberattacks and, more recently, AI. Although more than 40 vendors participate in this market worldwide, the top 7 vendors control almost 60% of the market share. (According to IDC data, Commvault was number 5 for market share for data protection software in 2024.) Some of these other top vendors have pivoted to positioning themselves as data security vendors, others as AI vendors, as well as other variations on these themes.

We believe Commvault's decision to double down on resilience as a company positioning is a solid strategy. Repositioning is not easy, and resilience is an extension of Commvault's core competence. Moreover, this does not mean the company is eschewing either AI or data security as the recent acquisitions and SHIFT 2025 announcements illustrate. Planting a flag as a leader in ResOps gives Commvault the opportunity to define the category.

Shift Left But Also Extend Right

Amid growing complexities, risks, and customer expectations, resilience has become a strategic priority for organizations. As a result, many technology providers (infrastructure, security, and monitoring vendors) focus on enhancing digital resilience. But this is primarily from the detection and identification perspective. These platforms orient the teams with root cause analysis to take quick action instead of looking for a needle in the haystack. These providers urge organizations to consider resilience in the journey and be signals driven.

With its ResOps vision, Commvault is seeking to extend its resilience solutions to the left by adding data security capabilities with its recent Satori acquisition (e.g., data discovery and classification, access policy monitoring, and enforcement), as well as extend to the

right with multiple layers building on each other. One such example is its updates to Threat Scan monitor for identifying risks in protected data. Its Synthetic Recovery identifies latest clean data for recovery at file, object, or VM level. Finally, its Cleanroom Recovery provides a secure space to automate testing and data validation before returning recovered data to production. This shows a complete end-to-end modern recovery workflow in action. This makes resilience a reality.

ResOps brings a two-fold opportunity for Commvault:

- Empower its traditional buyers in the IT admin domain to contribute effectively to an organization's resilience strategies. Commvault's ResOps-focused technologies allow its users to constantly prove their readiness to recover from any incident and provide quantifiable confidence in business continuity by reducing recovery time, costs, or errors.
- Synergize with observability, security, and infrastructure vendors for a better-together narrative around complete, continuous resilience for true ResOps. This can bring early insights into digital operations to guide product road map for Commvault while also being part of a strategic security ecosystem.

It is not without risk, however, as its success depends upon IT organizations' willingness to adopt the term and accept it as a category. It takes time for the market consciousness to become aware of a new term, and Commvault will need patience and persistence to carry through.

Confusion and ambiguity also could set it back. IDC believes Commvault should emphasize to its customers and partners that "ResOps" doesn't imply a disruptive operational change for their organizations. Instead, it should highlight how it can plug some of the operational resilience gaps and be added to existing frameworks to extend resilience to the right. For this, Commvault needs to develop a coherent ResOps maturity journey highlighting the clear value that its core users bring to their organizations' existing resilience framework.

Nevertheless, we believe ResOps has an opportunity to resonate with customers as it is concise with powerful implications and operational value.

It is also important to highlight that Commvault's ground-up pivot to SaaS five years ago (now Commvault Cloud Unity) has been a turning point for the company, laying the foundation for ResOps. It has given the vendor the right foundation to build new resilience-focused innovation and integrate newly acquired technologies at speed to give gravitas to its ResOps vision.

Subscriptions Covered:

Cloud Data Logistics and Protection, European Cloud Data Management Strategies

Please contact the IDC Hotline at 800.343.4952, ext.7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC or Industry Insights service or for information on additional copies or Web rights. Visit us on the Web at www.idc.com. To view a list of IDC offices worldwide, visit www.idc.com/offices.