MARKET NOTE

Commvault Unveils Cleanroom Recovery and More Cyber-Resilience Capabilities at Shift London

Archana Venkatraman

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: Commvault Unveils Cleanroom Recovery and More Cyber-Resilience Capabilities at Shift London

Data protection services are becoming strategic in organizations' comprehensive protection, recovery, and cyber-resilience strategies. Data protection vendor Commvault has envisioned a comprehensive approach to resilience, aligning with MITRE CREF and NIST frameworks with its cyber-resilience platform approach and has put recovery front-and-center of resilience with its innovative Cleanroom Recovery offering.

Key Takeaways

- Cyber-resilience is a top concern for the C-suites across organizations of all sizes, verticals, and regions.
- Cyberattack surfaces and attack types are rapidly increasing and becoming sophisticated.
- One of the key pain points in developing cyber-resilience is modernizing, testing, and validating recovery strategies because traditional DR strategies are incapable of delivering resilience against sophisticated attacks.
- At its Shift event in London, Commvault unveiled its Cleanroom Recovery service aimed at modernizing testing recovery plans and recovering at speed and scale that digital businesses demand.
- Commvault presented a comprehensive approach to cyber-resilience that covers hybrid environment, strengthening the "identify" and "recover" pillars of the NIST framework with its capabilities, ecosystem integrations, and acquisitions of the past couple of years.

Source: IDC, 2024

March 2024, IDC #EUR151935024

IN THIS MARKET NOTE

This IDC Market Note analyzes data protection vendor Commvault's features and capabilities unveiled at the Commvault Shift event held in London in February 2024. The analysis focuses on Commvault's Cleanroom Services and its value in organizations' cyber-resilience strategies.

IDC'S POINT OF VIEW

Data protection services are becoming strategic in organizations' cyber-resilience strategies. Data protection vendor Commvault has envisioned a comprehensive approach to resilience with its cyber-resilience platform approach and has put recovery front-and-center of resilience with its innovative Cleanroom Recovery offering. It is continuing to develop capabilities aligned with MITRE CREF and NIST frameworks for resilience.

Why Cyber-Resilience is a Top Concern for C-Suites

Among the top concerns for C-suites is cyber-resilience, particularly ransomware attacks. Digital businesses are characterized by data growth; high interconnectedness of devices, people, applications, data, and networks; as well as cloud migration. These characteristics increase vulnerability to cyberattacks. Ransomware attacks have multiplied exponentially, and now, generative AI is threatening with more sophisticated attacks. Combining this with a shortage of skilled cybersecurity professionals, organizations are faced with challenges to respond effectively.

This requires savvy organizations to plan for "when it happens" scenarios rather than "if it happens." This is where data recovery through intelligent and automated backup strategies becomes paramount. IDC believes that without holistic recovery infrastructure and recovery testing strategies, cyber-resilience plans are half-baked.

To mitigate their exposure to cyber-risks, organizations need to improve in five key areas:

- Starting with securing the directory service such as Active Directory (AD). Ensuring backup servers are not sitting on the same AD environment because shared authentication is a risky strategy.
- Implementing robust identity and access management mechanisms.
- Continuously monitoring and patching systems in an automated way.
- Devising and testing cyber-recovery plans.
- Making sure no data is left behind (including data in on-premises, cloud, SaaS, edge, and IoT environments).

The key challenge is that in traditional security and data protection approaches, there is over-investment in security tools. However, teams operate in silos, resulting in key tasks such as recovery readiness and testing becoming "someone else's responsibility." Recovery testing is complex, resource-intensive, and requires high skills.

IDC believes organizations wanting to be at the forefront of cyber-resilience need to move beyond seeing recovery testing as a tabletop exercise to making it a strategic priority embedded in resilience strategies with clear RACI matrix for stakeholders. Attacks can be managed if they are detectable and if there are clear controls to mitigate risks.

Traditional backup and disaster recovery (DR) strategies are not enough for cyber-resilience. Modern recovery strategies require:

- Early warning mechanisms
- Data integrity monitoring

- Enhanced separation of duties embedded in tech and process design as well as separation of backup and recovery infrastructure
- Ability to access recovered data at scale and speed for business continuity

Commvault aims to help organizations modernize their recovery strategies with its holistic resilience platform approach. Its vision unifies security, resilience (identifying, protecting, and monitoring) and recovery (responding and recovering) to ensure organizations can meet NIST framework's individual five pillars and execute better on the holistic "govern" pillar.

Commvault Cloud's Cleanroom Recovery Service

Cleanroom Recovery is Commvault's latest testing and failover cloud service. It provides a safe and isolated environment for organizations in three key use cases:

- Test their cyber-recovery plans cost-effectively without disrupting production environments
- Conduct forensic analysis for compliance, audit purposes, and root cause analysis
- Ensure business continuity in case of a data breach through quick, clean restores in the cloud
- Provide business access with complete production failover system for reduced downtime

It facilitates automated recovery of the control plane, integration with a copy of data in air-gapped environment, and an easy-to-use recovery pathway. The service uses Microsoft Azure's new, clean tenant for restores. The costs of the cloud resources are included in the service. In IDC's opinion, Cleanroom Recovery Service solves a critical problem in cyber-resilience – recovery readiness – by making recovery testing and actual recovery easier.

In a conversation with IDC, one customer said it had not tested its recovery or business continuity plan, and realized it had to rely on 24 different partners for recovery. At the same time, the IT department is busy dealing with the legal team and data protection authorities and have less time to focus on recovery. IDC estimates that less than 20% of organizations test their recovery strategies frequently.

Ransomware has fundamentally challenged the traditional disaster recovery strategy, and never has instant, tested recovery strategy been more important.

Many data protection vendors are building security-oriented features either organically or through acquisitions.

The differentiator of Commvault's strategy is its resonating focus on the key pain points and gaps in resilience.

But Commvault hasn't built these capabilities in a day. It can deliver these capabilities as a result of a few strategic steps it undertook in the past two years and building them on its SaaS venture Metallic, which was launched in 2019. These include:

- Acquisition of deception technology company TrapX
- Investing in AI and ML capabilities across data protection capabilities
- Launching early warning system to surface threats early with decoys to trap bad actors (Metallic ThreatWise)
- Adding SaaS, container, and edge backup and recovery offerings
- Building Commvault Cloud, powered by its SaaS venture Metallic and new AI features
- Forging strong integrations with security and storage platforms including Palo Alto Network, Crowdstrike, Splunk, Microsoft Sentinel, cloud hyperscalers, and storage vendors such as Vast Data, and NetApp
- Investing in security professionals including CISOs and building security certifications

- Identifying customer gaps in NIST framework and developing features to address identify, response, and recover functions

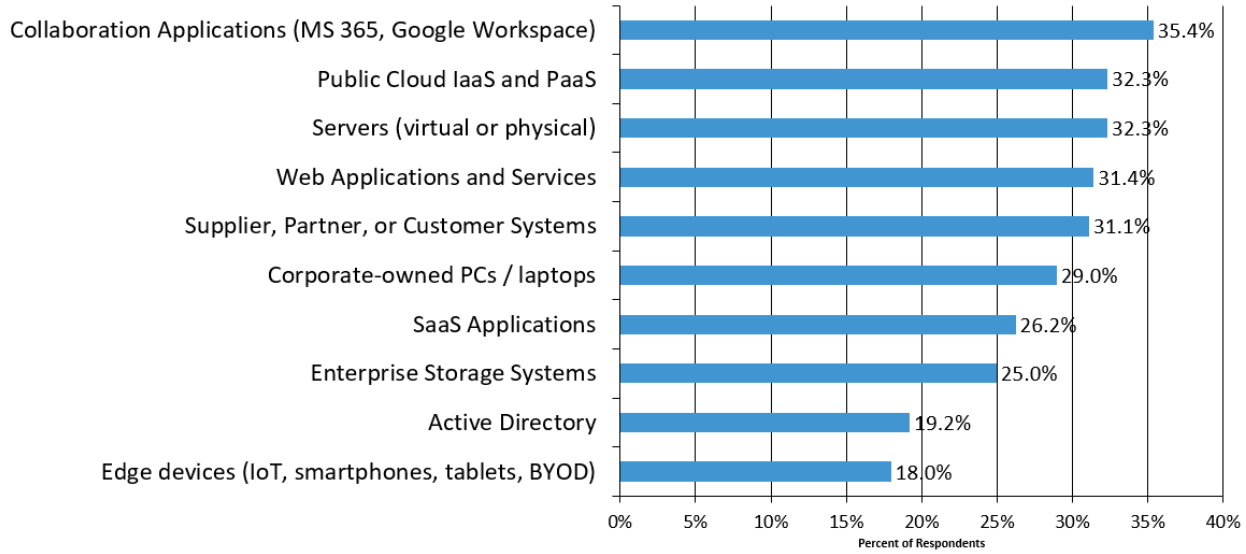
Commvault's cyber-resilience portfolio focuses on the ground reality of hybrid cloud.

IDC believes such an approach is essential because attack surfaces are widening to include containers, IoT, remote environments, SaaS, and cloud. Ransomware attacks impact a wide range of environments. In IDC's *Future Enterprise Resilience & Spending Survey* from December 2023 (Wave 11), EMEA respondents identified multiple environments including collaboration apps, cloud environments, servers, web applications, and supplier systems as being directly impacted by ransomware attacks (Figure 2).

FIGURE 2

IT Environments Impacted by Ransomware Attacks

Q. Overall, which of the following were directly impacted as a result of ransomware attacks?



Source: IDC, 2024

Commvault Cloud's Approach to Cyber-Resilience

At its London Shift event, its executive team highlighted how Commvault's holistic three-stage approach includes risk identification, response readiness, and recovery strategy, and it is aimed at strengthening some NIST pillars such as "identify" and "recover" as much as the "protect," "detect," and "respond" pillars. "Most investment we see are in the Protect and Detect areas but the ends of the spectrum are ignored," said Commvault EMEA CISO Darren Thomas at the event. The "identify" area is important because any micro-change to the data or any entropy needs to be closely watched and caught early, and taking detection closer to data can boost resilience.

Commvault's platform addresses risks in the *pre-backup* environment through features for risk analysis, anomaly detection, and threat detection (ThreatWise). For the *in-line backup* stage, it has features such as monitoring file activities, backup sizes, operations, and extensions. For the *post-backup* phase, its technologies help in threat scanning, risk analysis, data verification, and auto recovery. In addition, Commvault integrates with the security ecosystem including SIEM/SOAR environments, threat intelligence platforms, and XDR platforms.

According to IDC's 2023 *CloudOps Survey*, the top 3 capabilities organizations see as essential for successful cloud data governance are data availability, data integrity and quality, and cyber/ransomware resilience. As organizations invest in resilience, they are likely to embrace services such as Cleanroom Recovery.

IDC predicts that by 2028, 75% of IT organizations will implement AI-driven anomaly detection built into infrastructure components to thwart never-before-seen ransomware attack types. Commvault is ready with its cloud, AI features, and Cleanroom Recovery capabilities to boost its customers' cyber-resilience.

Commvault now needs to engage beyond its traditional personas (backup specialists and IT infrastructure teams) through channel, ecosystem partners, and security-led leadership. It also needs to keep its channel community incentivized with templates or blueprints on what services they could add further to the Commvault Cloud platform to add value to their customers.

The security and cyber-resilience landscape is crowded with resilience-washing messaging, thus Commvault needs to continue building its credibility with its resonating focus on the two pillars of NIST. Done right, Commvault is ready for the next phase of delivering value with Commvault Cloud.

LEARN MORE

Related Research

- *Holistic M365 Data Management: Data Protection, Security, and Data Preservation of M365 Data* (IDC #EUR151850824, February 2024)
- *Do Organizations' Cyber-Recovery Plans Include Containerized Application Data Protection yet?* (IDC #EUR151827024, February 2024)
- *Market Analysis Perspective: European Cloud Data Management, 2023* (IDC #EUR151407923, December 2023)

Synopsis

This IDC Market Note analyzes the cyber-resilience capabilities unveiled by Commvault at its Shift event in London in February.

"The threat landscape has fundamentally changed, and cyber-resilience is a continuum ranging from risk assessment, response readiness, and quick recovery, making backup and recovery tools and testing strategies paramount for comprehensive resilience," said Archana Venkatraman, research director, CloudOps and Cloud Data Management, IDC Europe. "Commvault is aiming to respond to that precise pain point – recovery – in its customers' cyber-resilience plans."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
blogs.idc.com
www.idc.com