Enterprise Strategy Group™

ECONOMIC VALIDATION

Analyzing the Economic Benefits of Commvault Cleanroom Recovery and Cloud Rewind

Modernize Your Cyber Recovery Plan and Accelerate Recoverability

By Nathan McAfee, Principal Economic Validation Analyst
Enterprise Strategy Group

June 2025

Contents

Enterprise Strategy Group™

Economic Validation: Key Findings Summary

Customer Validated Benefits of Commvault Cleanroom Recovery and Cloud Rewind

- **99% faster recovery**
- **94% faster rebuild**
- **Improve testing frequency by 30x**
- **Reduce testing time by 99%**

"Now that we are using Commvault Cleanroom, my execs and board of directors understand that we can literally restore anything, and to wherever we need to restore it."

Global Infrastructure Director, Industrial Manufacturing

Introduction

This Economic Validation from Enterprise Strategy Group focuses on the quantitative and qualitative benefits organizations can expect from adopting Commvault Cleanroom Recovery and Cloud Rewind technologies.

These solutions are built on the Commvault Cloud platform and create recoverability options that transcend most systems for cyber resilience. In addition to the analysis for this paper, the benefits discussed might include those from Enterprise Strategy Group's Economic Validation on Commvault Cloud. To read that study, click here.

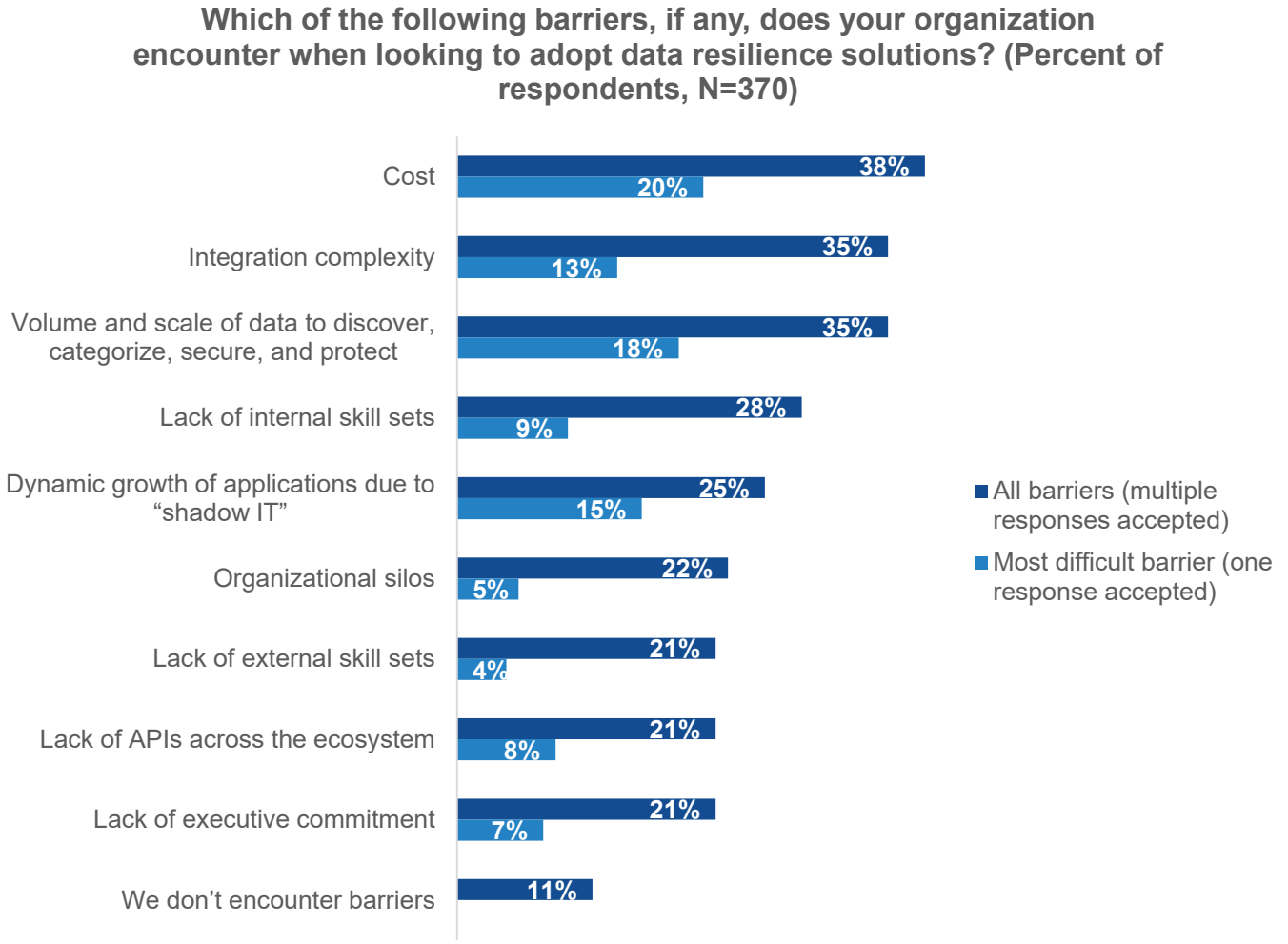
Customers interviewed for this analysis are in various global industries, including energy, healthcare, manufacturing, education, technology, IT consulting, financial services, retail, and government. They range in annual revenue from $2.4B to $20.5B. While each of the interviewees had unique use cases for Commvault Cleanroom Recovery and Cloud Rewind, we found the benefits shown in our financial model to scale across organizations of all sizes analyzed.

Challenges

Most seasoned IT professionals are familiar with stories of recovery events where data could not be restored to a usable state. This is typically the result of inadequate planning, tools, implementation, or testing or a general lack of expertise to navigate the complexity of today's hybrid IT environments. Enterprise Strategy Group research has identified the top barriers organizations face with data resilience and found these to be the key issues (see Figure 1).[1]

[1] Source: Enterprise Strategy Group Research Report, *Achieving Cyber and Data Resilience: The Intersection of Data Security Posture Management With Data Protection and Governance*, September 2024.

Figure 1. Barriers to Adopting Data Resilience Solutions



Source: Enterprise Strategy Group, now part of Omdia

As part of our analysis, we interviewed Commvault Cleanroom and Cloud Rewind customers to understand some of the specific challenges they faced in their previous cyber resiliency methodology and solutions. These were consistent across most of the interviews:

- **Ability to completely and consistently recover.** Being able to back up data is less than half the battle; the ability to effectively restore data and related infrastructure is what minimizes the impact of a loss and recovery event. Enterprise Strategy Group research showed that only 11% of respondents said their organization was able to fully recover all of its data on a regular basis.[2]
- **Recoverability of platform state.** Many organizations build their recovery plans around the ability to restore data. While important, this is only part of the solution. Organizations also need to be able to quickly recreate the entire ecosystem, including applications, drivers, networking, and connections, before data restoration becomes even possible. Furthermore, when recreating the underlying infrastructure, interdependencies require that components be recreated in a specific, step-by-step sequence.
- **Complexity and cost of recoverability testing.** Recovery plans are too often not fully tested until an actual recovery event happens. Interviews with customers found few companies complete recoverability testing while

[2] Source: Enterprise Strategy Group Research Report, *Cloud Data Protection Strategies at a Crossroads*, August 2023.

many build their strategies around once-a-year tests that only cover a few of their critical systems. These decisions are a result of the cost and complexity to complete thorough testing of full recovery and can leave organizations in an admitted high level of self-inflicted risk and potential exposure.

- **Lack of ability to undo unwanted recovery changes.** Rolling back from a change, or even an ineffective recovery event, is hard, if not impossible, for most organizations. These rollbacks can be extremely disruptive and too often result in data loss and unplanned downtime.
- **Ability to check and sanitize data before recovery.** A major issue in recovering from a ransomware event is the ability to verify data is clean before it is restored. Traditional testing environments make this task complex, uncertain, and often impossible.
- **Recoverability into isolated environments.** Many organizations find themselves limited to recovering into the same environment where the backup occurred or into another environment that cannot be verified as 100% clean from potential infection. In events like cyber recovery, that environment might be damaged or unavailable. In a cyber/ransomware recovery, organizations need the ability to recover into an on-demand, isolated environment to ensure the data is clean and free from reinfection. Although most organizations treat disaster recovery (DR) and cyber recovery as the same process, they often fail miserably in a cyber recovery situation, creating career-impacting results when ransomware strikes.
- **Dedicated plans for a different threat landscape.** A fundamental difference between DR and CR lies in the recognition of distinct threats. Traditional DR plans may not adequately address the complexities of a cyberattack, particularly ransomware. Therefore, CR necessitates dedicated plans focused on recovery into an isolated and verifiably clean environment.
- **Lack of integration across data resilience and security ecosystems.** The companies we studied relied on a collection of tools, many with 15+ different solutions for DR and cyber resilience. Lack of quality APIs and interoperability creates the need for these multiple tools and leads to high levels of technical debt.
- **Auditability and verification of cyber recovery plans.** Enterprise Strategy Group found auditability of recovery tests and plans was a challenge for the organizations we studied. These plans are critical for senior leadership (including boards of directors), required for certain compliance and regulating bodies, necessary to secure business with many customers, and even to reduce the cost of cyber insurance.

The Importance of Returning to Minimum Viability After a Cyberattack

The impact of downtime can be devastating, and the ability to quickly return to a viable state of operations after an attack or outage is essential. Minimum viability is the ability to rapidly and cleanly restore the minimum capabilities (applications, assets, processes, people) required for an organization to effectively operate after an attack, and this is a key component of continuous business practice. An organization must have confidence in its ability to quicky return to a state of a minimum viability to minimize disruption to the business with a well-defined plan in place for subsequent full recovery and improved resilience.

The Solution: Commvault Cleanroom Recovery and Cloud Rewind

To bolster cyber resilience and accelerate DR after a security incident or ransomware attack, Commvault provides Cleanroom Recovery. This automated, isolated, and secure cloud environment enables organizations to validate recovery strategies and investigate threats with forensic analysis. It also enables them to quickly restore operational environments, ultimately maintaining business continuity during unplanned downtime, catastrophic events, ransomware attacks, and other threats.

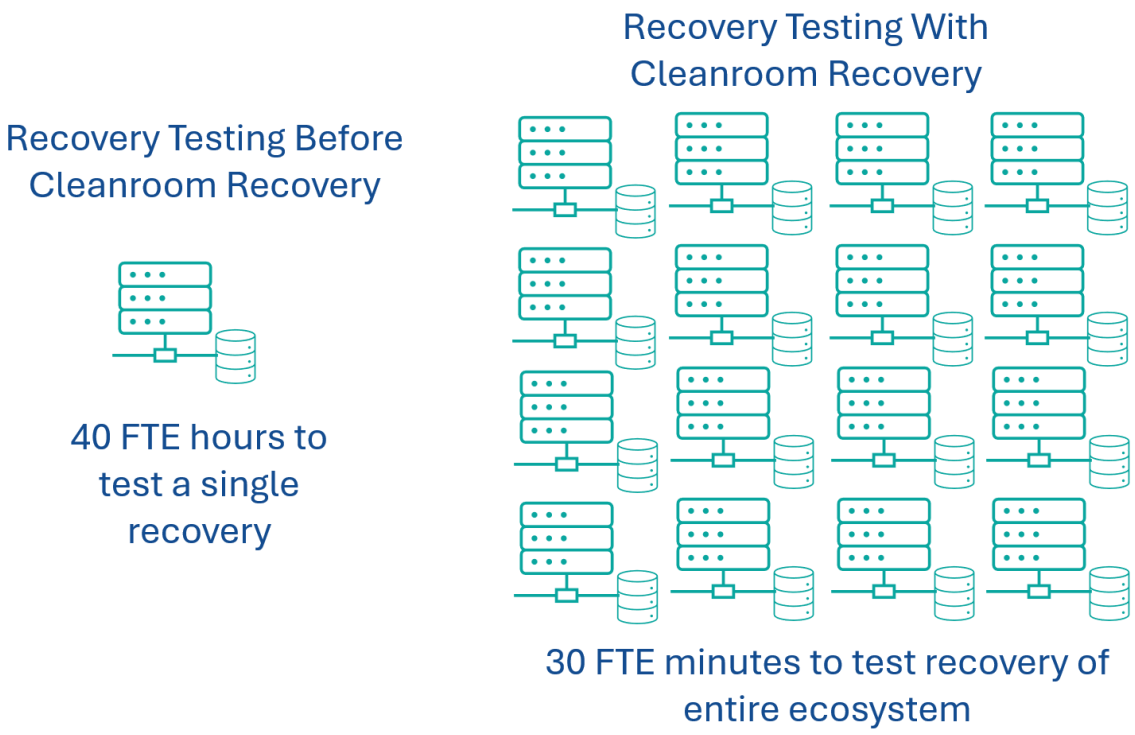
Commvault Cleanroom brings capabilities, including:

- **Cloud-based isolation.** Cleanroom Recovery operates in isolated cloud environments such as Azure and is designed to work in conjunction with Commvault Airgap Protect. Airgap Protect provides immutable and indelible copies of protected data, while Cleanroom Recovery offers a completely sterile and isolated environment with zero-trust access controls, rapid deployment, and unlimited scaling as needed. Airgap Protect helps organizations mitigate ransomware risks and maintain data compliance and supports recovery readiness in the event of a cyber incident or data loss.
- **Recoverability testing.** Cleanroom Recovery facilitates recoverability testing at whatever scale and frequency best fits the company's business model. Additionally, Commvault offers recoverability training that re-creates the chaos of an actual recovery event and builds the insight and experience that lead to an effective CR plan, as well as the execution of that plan. As seen in Figure 2, companies we analyzed reported conducting recoverability tests on only a single server or workload per month, with each test requiring an average of 40 FTE hours to complete. Testing using Commvault Cleanroom Recovery can significantly reduce the time required for recoverability testing. While standing up a cleanroom environment can take as little as 30 minutes, the total duration of a recovery test depends on the scope and complexity of the systems and data being recovered. However, it offers the capability to include recoverability tests for the entire ecosystem within a significantly compressed timeframe compared to traditional methods, which often take days or weeks and involve substantial FTE hours. In this analysis, we found resilience testing with Commvault Cleanroom Recovery can facilitate recoverability strategies that reduce risk exposure by 97% while significantly improving recoverability.

Building an Effective Cyber Recovery Plan

Too often, organizations do recoverability testing using a checklist. They test one part of recovery and then the next until all boxes are checked. This plan quickly falls apart in the chaos of a true recovery event, leaving the organization ill-prepared to recover and ensure a continuous state of business. Many of the customers we interviewed placed high value on participation in both Commvault's experiential "Minutes-to-Meltdown" immersive event that recreates the chaos of an actual cyberattack and in Commvault's Cyber Resilience certification programs, citing these as essential to their teams' cyberattack readiness and recoverability level.

Figure 2. The Impact of Increasing Recovery Testing With Cleanroom Recovery



Source: Enterprise Strategy Group, now part of Omdia

- **Rapid deployment.** A Cleanroom can be created and populated in minutes. This reduces the time to minimum viability and enables companies to quickly get their core business recovered when a cyberattack strikes, enabling continuous business.
- **Forensic analysis.** Cleanroom Recovery provides an isolated secure environment for forensic analysis of infected systems to identify the root cause of an attack. Cleanroom Recovery can also isolate an infected environment to safely explore and understand the infection scope and process, providing valuable insights for enhancing future cyberattack prevention and readiness.
- **AI-driven recovery.** Commvault uses AI-driven reporting and automation throughout the recovery process. This helps identify the last-known clean recovery point and rebuild the entire ecosystem to add dependencies in the necessary order.
- **Clear and detailed auditing and reporting.** Commvault provides extensive reporting capabilities used for activities like audits, cyber insurance certification and reduction of cyber insurance premiums, and compliance with local and global laws and regulations. This detailed reporting, according to many customers interviewed, also satisfies board-level requirements for proof of cyberattack readiness.

Commvault Cloud Rewind provides application recovery and rebuild capabilities tailored for cloud-based applications and infrastructure. It is designed to help organizations rapidly recover from cyberattacks, outages, or disasters and enables organizations to prioritize what they need first to maintain continuous business (i.e., minimum viability).

Commvault Cloud Rewind capabilities include:

- **Rapid recovery of cloud applications and environments.** Cloud Rewind can automatically create an application environment time machine, enabling an organization to rewind applications and infrastructure, along with the essentials of the environment, to return to the point in time prior to a damaging cyberattack.
- **Cloud configuration discovery**. Cloud Rewind continuously discovers cloud service configurations to map dependencies and adapt to an organization's specific cloud architecture and services.
- **Reduced risk from cloud misconfigurations.** Cloud Rewind's automation and orchestration reduce the risk of application failure with predictable recovery paths and processes and by limiting the potential of human error.
- **Continuous cyber resilience.** Hyperscale clouds require hyperscale cloud resilience. Cloud Rewind supports instant recovery and rebuilding within the same zone as well as across zones, regions, and accounts, creating ultimate flexibility for rapid recovery and continuous business operations.
- **Patented dual-vault cloud time machine.** Cloud Rewind uses secure, immutable vaults for instant application recovery. Separate vaults are used for cloud configuration and application data for faster recoveries and continuous operations.

Enterprise Strategy Group Economic Validation

Enterprise Strategy Group completed a quantitative economic analysis to understand how Commvault Cleanroom Recovery and Cloud Rewind can help an organization reach its IT and business goals. Our Economic Validation process is a proven method for understanding, validating, quantifying, and modeling the economic value propositions of a product or solution. The process leverages Enterprise Strategy Group's core competencies in market and industry analysis, forward-looking research, and technical/economic validation. We conducted in-depth interviews with Commvault customers to understand how the move to Cleanroom Recovery and Cloud Rewind has affected their organizations, particularly their recovery testing and overall recoverability in the event of a cyber or ransomware attack and other potential threats.

The qualitative and quantitative findings were used as the basis for a simple economic model comparing the expected costs and benefits of improved recoverability with Cleanroom and Cloud Rewind. The organizations interviewed represent a range of global industries, including energy, healthcare, manufacturing, industrial equipment, biomedical, education, technology, IT consulting, financial services, retail, and government, with annual revenues spanning from $2.4B to $20.5B.

Commvault Cleanroom and Cloud Rewind Economic Analysis

Enterprise Strategy Group's economic analysis revealed that organizations that use Commvault Cleanroom Recovery and Cloud Rewind as the foundation of their testing and recoverability strategy should enjoy benefits including:

- **Improved business continuity.** Fast, clean, and complete recoverability is a cornerstone of an effective business continuity strategy. Enterprise Strategy Group found that companies that utilize Commvault Cleanroom Recovery and Cloud Rewind have a significantly higher probability of full recoverability.
- **Lower recovery and testing costs.** We found that the cost of recoverability testing was lowered substantially when moving to Cleanroom Recovery.
- **Reduced complexity and technical debt.** Cleanroom Recovery and Cloud Rewind are part of the Commvault Cloud, a comprehensive data protection and cyber-resilience platform designed for modern hybrid environments. The move to a simplified and highly integrated solution removes decades of technical debt and reduces the number of staff and the skill level of staff needed to manage and scale the Commvault solution.

Improved Business Continuity

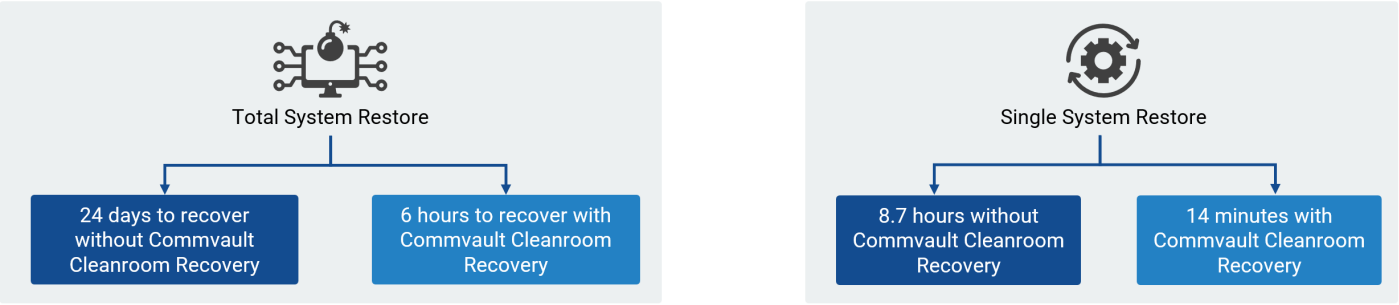
Data resilience is the top IT priority for more than a third (36%) of organizations and a top five priority for 88% of organizations.[3] Enterprise Strategy Group interviews found that most organizations struggle to build, create, and test effective cyber resilience and recovery plans. We found that Commvault Cleanroom Recovery and Cloud Rewind are cornerstones of an enterprise-level business continuity plan for many reasons, including:

- **Enablement of recoverability testing.** Even though most organizations said that data resiliency is a top priority, only a few that we interviewed for this analysis had pre-Cleanroom Recovery testing plans that were comprehensive, frequent, and reliable. We found that Cleanroom Recovery has the flexibility and ease of use to enable any level of recoverability testing that fits a company's needs. An environment can be spun up quickly, and Commvault's Metallic AI automates much of the testing without disturbing production systems. Users can tailor recovery sequences to recover data in a prioritized and logical order, and networking, storage and applications can be recovered to test a full cyber recovery scenario using Cloud Rewind.

> **"Before we adopted Commvault Cleanroom Recovery, we did annual recoverability testing on one of our server farms. We were forced to assume that recovering one meant we could recover all. Now, with Cleanroom, we do monthly recoverability tests on all of our critical assets and know that we can quickly restore in the event of a cyberattack."**
>
> – Director, Global IT, Services and Solutions Provider

- **Facilitating near-instant recovery.** With Cleanroom Recovery, a recovery environment can be spun up in minutes, accelerating the full recovery process. We found that recovery took an average of 8.7 hours before Cleanroom Recovery, with some examples taking multiple times that time. As seen in Figure 3, the Director of IT for a university system shared, **"It used to take 24-36 hours to recover a single server instance and up to 24 days to recover from a cyber event. We can now restore everything in less than an hour."**

Figure 3. Recoverability Time Benefits



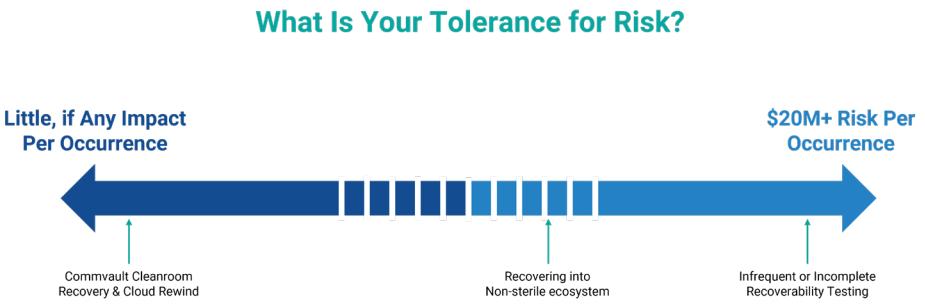
Source: Enterprise Strategy Group, now part of Omdia

Another example we studied was an energy equipment manufacturing organization that does full test recoveries each evening. This provides that organization with an immediate environment to switch over to in the event of failure. The global infrastructure director of this energy equipment manufacturer explained, **"I wake up every day, check my Cleanroom Recovery report about the previous night's restore, and know we are protected and can recover. Downtime is expensive in our business, both in terms of monetary costs and customer satisfaction. We have eliminated downtime by always being able to recover from cyber events."** With the customer-reported costs of a cyber event being $20M and recent examples in the news of events exceeding $100M, along with immeasurable negative impact to their

[3] Source: Enterprise Strategy Group Research Report, *Achieving Cyber and Data Resilience: The Intersection of Data Security Posture Management With Data Protection and Governance*, September 2024.

reputations, companies need to evaluate their tolerance for risk and ensure their resilience strategy matches their tolerance level (see Figure 4).

Figure 4. Understanding the Correlation Between Resilience Strategy and Risk



Source: Enterprise Strategy Group, now part of Omdia

- **Enhanced recoverability.** A fundamental truth for data resiliency is that if critical data and infrastructure can't be recovered, it should never be backed up. In studying the states of our analysis participants before Commvault Cleanroom Recovery, we saw far too many examples where there was no certainty of recoverability. The IT director of infrastructure for a worldwide manufacturing conglomerate summarized this well: **"With Cleanroom, I can absolutely guarantee that my last backup is recoverable. In the past, this was just hope and theory."**
- **Shifting expertise to proactive thinking.** The AI capabilities of Cleanroom Recovery were frequently called out as game-changing for three main reasons: the speed and completeness of recovery, the ability to isolate and identify the cause of failures, and the way that IT staff can free up their time to shift to more proactive thinking by leveraging Commvault's Metallic AI automation and orchestration tools as a significant augmentation to their IT staff. The director of IT solutions engineering for a hospital and healthcare network shared, **"Since we moved to Cleanroom Recovery and Cloud Rewind, I have been able to shift some of my best team members to forward-thinking work that allows us to solve some of the problems that impact our doctors and patients. Because of this move, our people are happier and work better together, leading to improved patient care and higher customer satisfaction and retention."**
- **Isolated investigation.** When an intrusion or infection happens, the investigative process can take months, if not longer, to understand how the problem entered the IT ecosystem and how it propagated. Additionally, more than a third of organizations that have been the victim of a successful ransomware attack were re-attacked within 12 months.[4] When asking our interviewees why they think these re-attacks happen, they noted the complexity of trying to identify and remedy all aspects of breach or infection before restoring. A security and recovery expert from an enterprise cyber-resilience organization summarized this by saying, **"If we can't trust the integrity of the data during a recovery event, we can't restore it to our production environment. With Cleanroom Recovery, we can isolate the restored environment and actually run our minimum viable company out of it. This allows us to do business in a protected and isolated environment."** Other interviewees shared requirements to retain the availability of an infected environment for insurance purposes. One VP of infrastructure for a global services company explained, **"Cleanroom allows us to leave our infected environment in a truly protected instance where we can examine it and understand how it propagated. This also allows us to meet insurance and compliance requirements while we restore minimum viability elsewhere, getting the business back to normal business operations (or minimum viability) without disruption."**

[4] Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023.

- **Commvault preparation assistance.** The quality of Commvault education and learning programs available to customers stood out as we were examining the combination of technology and expertise that Commvault offers. We were told, **"Where Commvault really shines is helping us test recoverability in a chaotic state. We used to go through a checklist and say we were good. However, in a true cyber event, things are not orderly. Commvault helps us effectively mimic that chaos and plan for the unexpected."** This is accomplished through offerings such as Commvault's Minutes-to-Meltdown, an in-depth session led by Commvault subject matter experts designed to help participants understand modern ransomware attacks. This highly experiential event involves participants actively participating in the roles of the CISO, CIO, and others to develop a plan for improved cyber readiness. Commvault Recovery Range is a hands-on lab simulating real cyberattacks, with a focus on achieving successful recovery. Participants race against the clock to save a major enterprise under attack. Full-blown cyber resilience certification programs are also available from Commvault for its customers.

> **"We meet with Commvault quarterly to examine our recoverability plans and share best practices. None of our other IT vendors do this. We work with over 100 vendors; Commvault is absolutely at the top as far as treating us like partners."**
>
> – Director of IT, University System

- **Elimination of complexity in a recovery event.** Recovery goes far beyond restoring data. Multiple systems must be brought back up in a specific order to meet dependency requirements. An IT leader from a global backup solutions organization explained, **"Our recovery matrix has 20+ different distinct levels of bringing services up in the right order. With Cleanroom Recovery, we automate this in exactly the right order for success."**
- **Flexibility in recovery options.** Recovering from a true cyberattack can require a repair or rebuild of underlying infrastructure and even locations. Commvault Cleanroom Recovery and Cloud Rewind can create a recovery environment in minutes, completely independent of hardware or location requirements.
- **Increased customer satisfaction and business growth acceleration.** When asked about the business impact of recoverability testing, interviewees shared multiple stories about how their customers viewed their improved capabilities. A cloud services VP shared, **"When I tell my customers that we can test restorability monthly instead of on a yearly basis, they have a higher level of trust in doing business with us. By doing this, we offer a level of service that our competitors can't, or won't, be able to match."** They also shared how they were able to sell more cloud services specifically because of their move to Cleanroom Recovery: **"We keep our customers happier and get new customers because we can show our commitment to cyber recovery readiness. Our revenue has gone up 3.5% directly because of this move to Commvault Cleanroom Recovery."**

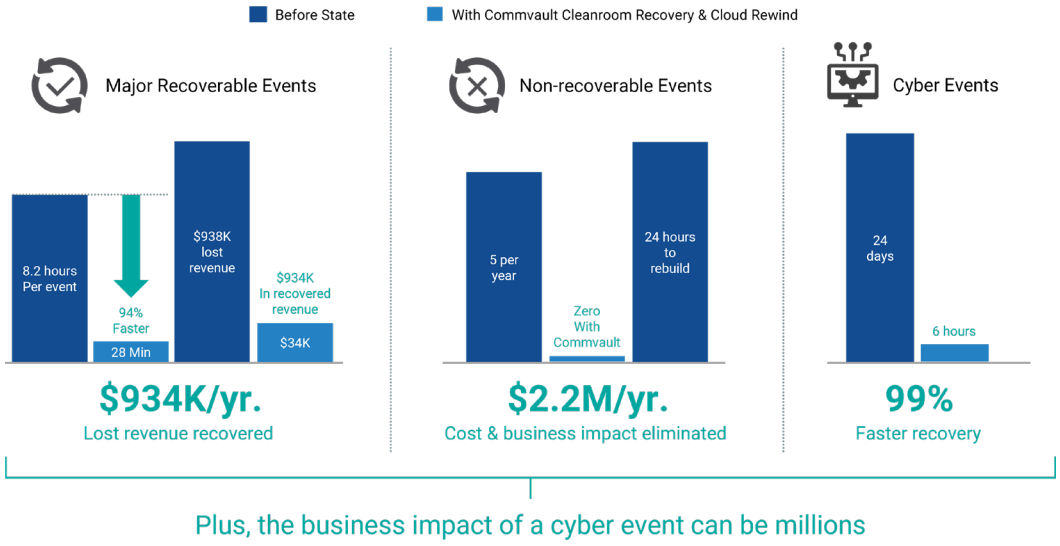
Lower Recovery and Testing Costs

Comparing the before and after costs of recovery testing for customers moving to Commvault Cloud is challenging because of the dramatic differences in how organizations test after the move to Commvault. Companies we studied went from testing a small portion of their entire ecosystem yearly to testing their entire data, storage, and application platforms monthly, including an organization that does full recoverability tests nightly to reduce the potential impact of downtime. While there is variance across these examples, we found the following benefits to be consistent across all organizations we studied:

> **"Switching to Commvault Cleanroom Recovery is not just a cost savings. The level of expertise it would take to truly create a clean recovery environment is beyond our skillset."**
>
> – Director of IT Solutions Engineering, Global Cloud Services

- **Reduced impact of downtime.** When exploring the benefits of improved recovery, the first metric that most organizations discussed is the change in downtime based on accelerated recovery. We found that Commvault Cloud Rewind can reduce minor recovery events per year and lower the impact of each event. For major events, no interviewee said its previous state could compare to the complete state that Commvault Cleanroom Recovery provides. We made the assumption that recovered states were equal in our metrics examining the impact of different recovery scenarios on our sample modeled company (see Figure 5).

Figure 5. Before and After Commvault Cleanroom Recovery and Cloud Rewind



Source: Enterprise Strategy Group, now part of Omdia

- **Removing cost barriers to testing.** Organizations we interviewed had many answers for why their recoverability testing plans did not match their cyber resiliency intentions. The first of which was the cost of FTE time to test and the second was the cost and complexity of trying to create and maintain a testing environment. We studied customer-provided examples where they spent up to $20M trying to create an environment like Cleanroom Recovery, with results that were not as effective as the results Cleanroom Recovery has shown to deliver. Others tried to create cloud-based recovery environments but found their speed to be lacking, and the results were lower than expected. The IT director of a university system shared, **"Cleanroom is 60% cheaper than using VM-based recovery environments, and we can get to minimum viability right out of a Cleanroom. There is no way we could easily run our minimum viable company out of a VM recovery."**

> **"We get discounts on our cyber insurance because of the improvements that Cleanroom Recovery provides. Commvault makes it extremely easy to document our plan in detail. This saves us over $100K a year."**
>
> – Global Infrastructure Director, Industrial Manufacturing

- **Reduced FTE costs for planning and testing recovery.** The average testing cost for the companies we studied included monthly tests taking five FTEs a total of 40 hours. This equates to $141,864 per year spent. When moving to Cleanroom, these costs went down to under $11K per year. However, our research showed that tests increased from 12 per year to 365 per year with one person using half an hour per test.
- **Impact of AI guidance and best practices.** As the director of IT for a cloud services company told us, **"Everything I can automate in my testing and recovery process saves time and money and increases the likelihood that we will be successful when a cyberattack strikes and clean recovery takes place.**

Commvault AI constantly identifies improvements and best practices to improve our CR plans and lower our costs."

- **Lower cyber and business insurance costs.** Interviewees shared that cyber and business insurance was easier to obtain and at a lower cost, specifically because of their investment in Commvault and their ability to show detailed testing and recovery plans along with detailed reports required for compliance and regulatory audits.
- **Reduction of technical debt.** When examining the pre-Cleanroom Recovery states of the customers we interviewed, we found diametrically opposed realities between their cyber resiliency needs and their actual capabilities. We found pieced-together plans that were incomplete, untested, and had costs that did not match their benefits. We saw decisions being made because of constraints or being forced because of past decisions. With Cleanroom Recovery and Cloud Rewind, these same customers are able to match testing frequency and completeness with their cyber resilience goals and to plan recovery into whatever environment is needed to address the situation at hand. This enables these customers to quickly regain the minimum viable state that enables operations to continue without risk of lost business or damage to their reputation and brand value.

Reduced Complexity and Technical Debt

Commvault Cleanroom and Cloud Rewind are based on the Commvault Cloud Data Platform. Enterprise Strategy Group conducted a comprehensive economic analysis on the benefits of Commvault Cloud here and found these benefits to be achieved by the additional customers interviewed for this analysis:

"We trust Commvault and Microsoft and value their partnership. We know that our Commvault Cloud solution is complete and secure, plus the flexibility of its Azure integration allows us to focus on our business."

– Director of IT, University System

- **Cost efficiency.** Commvault Cloud can lower costs and provide a much more predictable cost structure when compared to alternative environments. Commvault is a cornerstone that companies can use to optimize their cloud environments and reduce overall spending while improving their cyber resiliency and cybersecurity.
- **Increased agility.** Agility, in both the way that employees can work and in an organization's ability to protect its data during times of rapid change, enables companies to focus on their core business instead of worrying about data security and recovery after the impact of a cyberattack and other cyberthreats. A major benefit of Commvault's approach is its industry-leading depth and breadth of workload coverage. Several of the customers interviewed described this as the assurance Commvault brings that there will be "no workload left behind" in the accelerated journey to the cloud for improved cyber and data resilience in efforts to optimize their transformation with underlying goals of cost reduction with increased agility.
- **Reduced risk.** Commvault, which has provided data protection for over 27 years, has been integrated with Microsoft's cloud solution since Azure's inception in 2010 for a holistic and cloud-native approach. In 2019, Commvault extended its platform to include a SaaS offering built upon the same technology as the core Commvault software offering, enabling the ability to secure and protect data, regardless of the location of the data or chosen method of deployment for data protection and cyber resilience (on premises, public cloud, or SaaS). This integrated approach has enabled joint Microsoft and Commvault customers to replace, on average, 15 existing data protection solutions by moving to Commvault Cloud on Azure, significantly reducing the risk level through their data estate.

Commvault Cloud brings together Commvault's SaaS solution with a software solution, providing a unified control plane that delivers enhanced capabilities and ease of use at scale. This enables organizations to realize the data security and cyber-recovery capabilities expected from Commvault, without the complexity that normally comes with enterprise-level protection, while providing a roadmap for seamless transformation to SaaS data protection. Commvault Cloud also significantly enhances an organization's cyber resilience and data security posture.

Conclusion

Most organizations have a huge gap in their cyber resilience needs compared to their capabilities to quickly restore when cyberattacks strike. The cost and complexity of testing outstrips their budget and capabilities, and true chaos that comes with a major recovery event is hard to duplicate in testing. While Enterprise Strategy Group research validates that cyber resiliency is a top five priority for 88% of organizations,[5] we interviewed enterprise-level customers to understand their recovery testing strategy and found that most did partial and infrequent tests that were really a checklist and not a proven plan to enable full recovery. Our customer interviews uncovered cost of downtime ranging from $10,000 per hour up to examples where downtime cost millions of dollars per minute. We found that too many organizations make cyber resilience investments like risk is someone else's problem, and the level of risk that is being accepted by many should be considered unacceptable.

We analyzed the impact that Commvault Cleanroom Recovery and Commvault Cloud Rewind can have on improving recovery testing, as well as cyber resilience and recovery overall. We found that Cleanroom Recovery provides not only a recovery environment that is far beyond what most organizations can create, it also provides sterile, AI-enabled environments that can actually be used to recover to minimum viability often within minutes instead of hours, days, weeks, or months, reducing downtime to nearly zero. We found that Cloud Rewind can quickly recover applications and related infrastructure in the cloud by rolling back to a previous point in time, prior to the impact of a cyberattack. We also believe that the partnership between Commvault and Microsoft in cyberattack readiness and recovery provides the added benefit of providing organizations with a robust foundation for navigating the full spectrum of potential disruptions while planning for rapid recovery to minimum viability.

Additionally, we believe that Commvault has “cracked the code” for recoverability, with customer-reported examples of 94% faster rebuild (Cloud Rewind) and 99% faster recovery (Cleanroom Recovery), enabling organizations to rapidly restore critical systems and data in the event of a cyber disruption. We found that the benefits of a cyber resilience readiness plan that include Commvault Cleanroom Recovery and Commvault Cloud Rewind can be the difference between significant business loss and long-lasting brand damage as compared to cyber events that are remediated with little or no business interruption when a recovery plan includes Commvault Cloud integrated with Microsoft Azure.

Commvault Cleanroom Recovery and Cloud Rewind are cornerstones of an effective and modern cyber resilience plan. Enterprise Strategy Group highly recommends that any organization that has a mismatch between its resilience capabilities and its ability to execute on a proven cyber resilience plan explore what Commvault and its long partnership with Microsoft can do to help enable and accelerate crucial steps towards true cyber certainty and recovery.

[5] Source: Enterprise Strategy Group Research Report, *Achieving Cyber and Data Resilience: The Intersection of Data Security Posture Management With Data Protection and Governance*, September 2024.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com