TECHNICAL REVIEW

APRIL 2024

Ensuring Cyber Readiness With Commvault Cloud Cleanroom Recovery

Tony Palmer, Principal Analyst and Practice Director, Validation Services

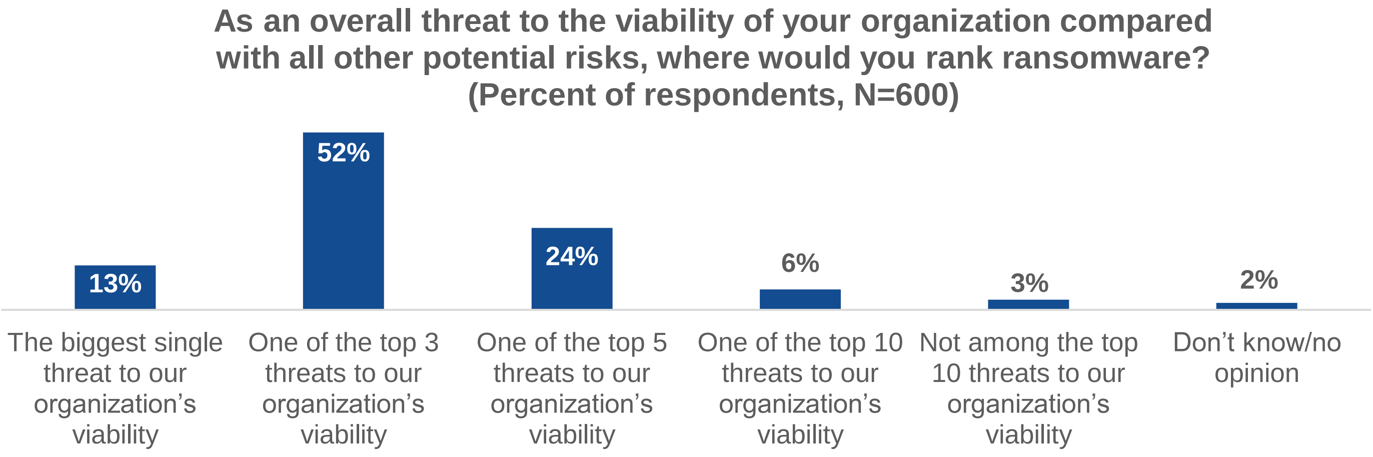
Abstract

This Technical Review by TechTarget's Enterprise Strategy Group details the analysis of Commvault Cloud Cleanroom Recovery, with the goal of validating how Cleanroom Recovery can help organizations improve their cyber resilience by providing a comprehensive solution for testing, analysis, and failover.

The Challenges

Enterprise Strategy Group research revealed that ransomware is a significant threat that can potentially devastate organizations. While 89% of respondents ranked ransomware as one of the top five threats to the viability of their organization, nearly two-thirds (65%) placed it in the top three (see Figure 1).[1]

Figure 1. Wide Majority Rank Ransomware as a Top Threat to the Viability of Their Organization



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

This is especially concerning when you consider that ransomware attacks are not a matter of if, but a matter of when: 75% of organizations reported a successful attack, with 37% of those organizations having experienced more than one. Paying the ransom doesn't mean you'll actually get your data back. More than half (56%) of organizations that experienced an attack reported paying a ransom to regain access to their data, and many of those organizations were asked to pay more after they paid the first time.[2] Attackers employ many different techniques and targets to motivate payment. Data, or access to it, is the prize—and extortion by threatening

[1] Source: Enterprise Strategy Group Research Report, [2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation](), December 2023. All research in this Technical Review was taken from this research report, unless otherwise noted.
[2] Source: Enterprise Strategy Group Complete Survey Results, [2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation](), November 2023.

exposure is what's in play. Attacks hurt organizations in many ways, including data exposure (53%), data loss (51%), operational disruption (46%), and direct impact on customers, partners, and employees (42%).

Despite prevention investments, attackers still find ways to evade safety measures. Attacks are no longer initiated primarily through malware; attackers have a varied set of tools to help them acquire valid authentication credentials.

Traditional cyber-recovery testing methods, such as tabletop exercises, often fail to adequately prepare organizations for the complexities and chaos of real-world cyber-recovery scenarios. Today, organizations must be assured that the environment they restore to is clean, as todays cyberattacks impact the environment in which the data resides along with the data itself. Organizations must adopt proven testing and recovery best practices for cyberattack preparedness and recovery readiness.

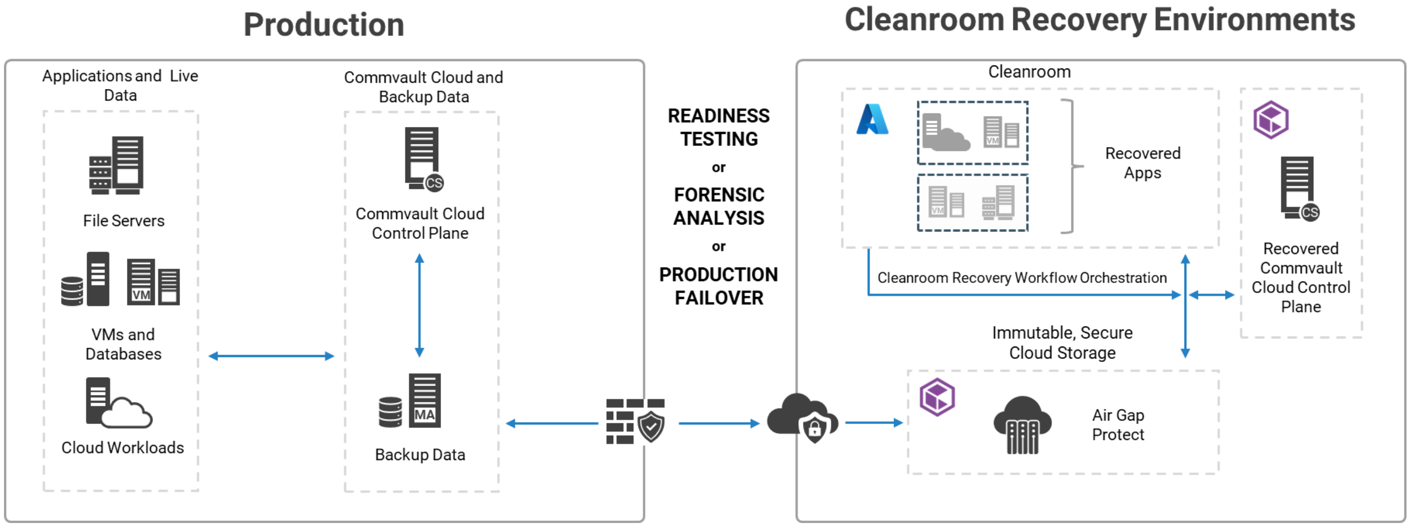
Commvault Cloud Cleanroom Recovery

Commvault Cloud's Cleanroom Recovery is a testing and failover solution that enables organizations to ensure clean recovery and business continuity in the event of a breach. For the purposes of this paper, the term cleanroom at its most basic level is defined as a secure, separate recovery environment that is guaranteed to be clean.

Cleanroom Recovery enables recovery to an assured-to-be-clean environment, made possible by Commvault's any-to-any portability. The concept of a cleanroom is much more than just a secure physical space. Commvault sees the cleanroom as a comprehensive approach to cyber recovery, encompassing not only a secure, standalone environment, separate from the production network, but also detail-oriented planning, established processes, best practices, testing, and well-defined procedures.

Cleanroom Recovery helps organizations mitigate cyber-risk by providing a safe and isolated environment for testing cyber-recovery plans so organizations can identify and address gaps before an attack occurs without disrupting production systems. In addition, Commvault's cleanroom environments can be used for conducting forensic analysis of infected systems to help organizations understand the root cause of an attack and take steps to prevent future incidents.

Figure 2. Commvault Cloud Cleanroom Recovery Workflow


Production
Applications and Live Data
File Servers
VMs and Databases
Cloud Workloads
Commvault Cloud and Backup Data
Commvault Cloud Control Plane
Backup Data
READINESS TESTING
or
FORENSIC ANALYSIS
or
PRODUCTION FAILOVER
Cleanroom Recovery Environments
Cleanroom
Recovered Apps
Recovered Commvault Cloud Control Plane
Cleanroom Recovery Workflow Orchestration
Immutable, Secure Cloud Storage
Air Gap Protect

Source: Commvault and Enterprise Strategy Group, a division of TechTarget, Inc.

There are three parts to a cleanroom recovery: control plane recovery into the Commvault Cloud environment, a tertiary copy of data in Air Gap Protect (formerly Metallic Recovery Reserve), and utilization of the Auto Recovery feature for predefined recovery groups. A clean Microsoft Azure subscription and tenant, supplied by the client, is required, as are licenses for Commvault Cloud Software, Air Gap Protect, and Cleanroom Recovery. The following are key features of Commvault Cloud's Cleanroom Recovery:

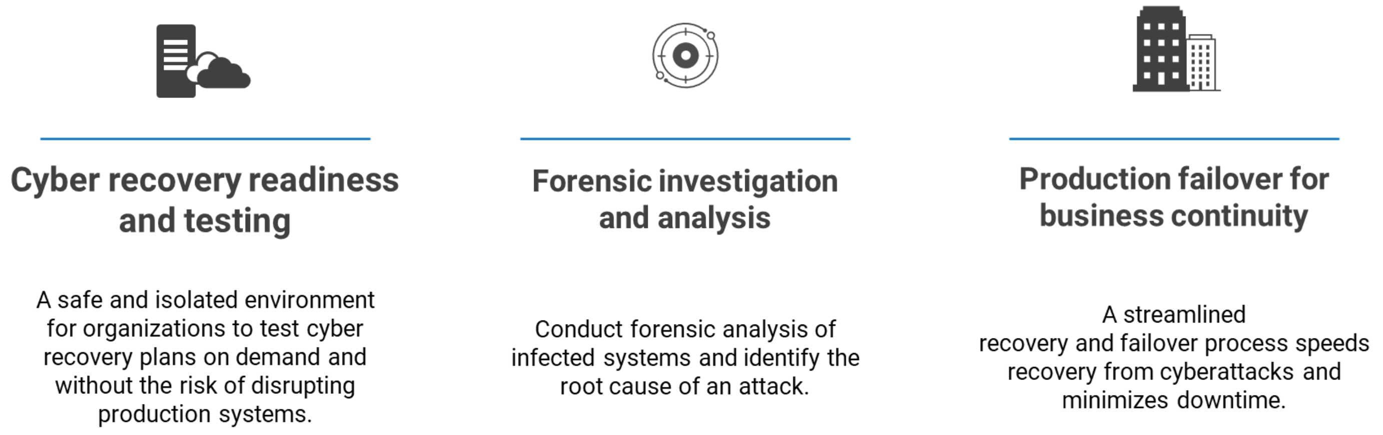
- **Safe and isolated testing environment.** Cleanroom Recovery provides an environment where organizations can test their cyber-recovery plans without the risk of disrupting production systems.
- **Secure forensic analysis.** Cleanroom Recovery can be used to conduct forensic analysis of known infected systems and identify the root cause of an attack.
- **Streamlined recovery process.** Cleanroom Recovery can help organizations recover from cyberattacks more quickly.
- **Reduced downtime.** Cleanroom Recovery can help organizations minimize downtime by providing a production failover solution.

Commvault Cleanroom Recovery recovers into a new Azure tenant, supported by Commvault's any-to-any data portability. The assured clean environment in Azure is the heart of the solution. This enables Commvault Cloud to test and recover a wide array of workloads and environments including VMware, Azure Virtual Machines, Amazon Elastic Compute Cloud (EC2), and Microsoft Hyper-V. It's important to note that Commvault supports a much broader range of sources and targets for recovery, and as those workloads are tested by Commvault, they will be supported in Cleanroom Recovery.

Enterprise Strategy Group Analysis

Enterprise Strategy Group looked at how Cleanroom Recovery works and how it can be applied across multiple use cases critical for cyberincident recovery: cyber-recovery readiness and testing, forensic investigation and analysis, and production failover for business continuity (Figure 3).

Figure 3. Critical Use Cases for Cleanroom Recovery



Cyber recovery readiness and testing

A safe and isolated environment for organizations to test cyber recovery plans on demand and without the risk of disrupting production systems.

Forensic investigation and analysis

Conduct forensic analysis of infected systems and identify the root cause of an attack.

Production failover for business continuity

A streamlined recovery and failover process speeds recovery from cyberattacks and minimizes downtime.

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

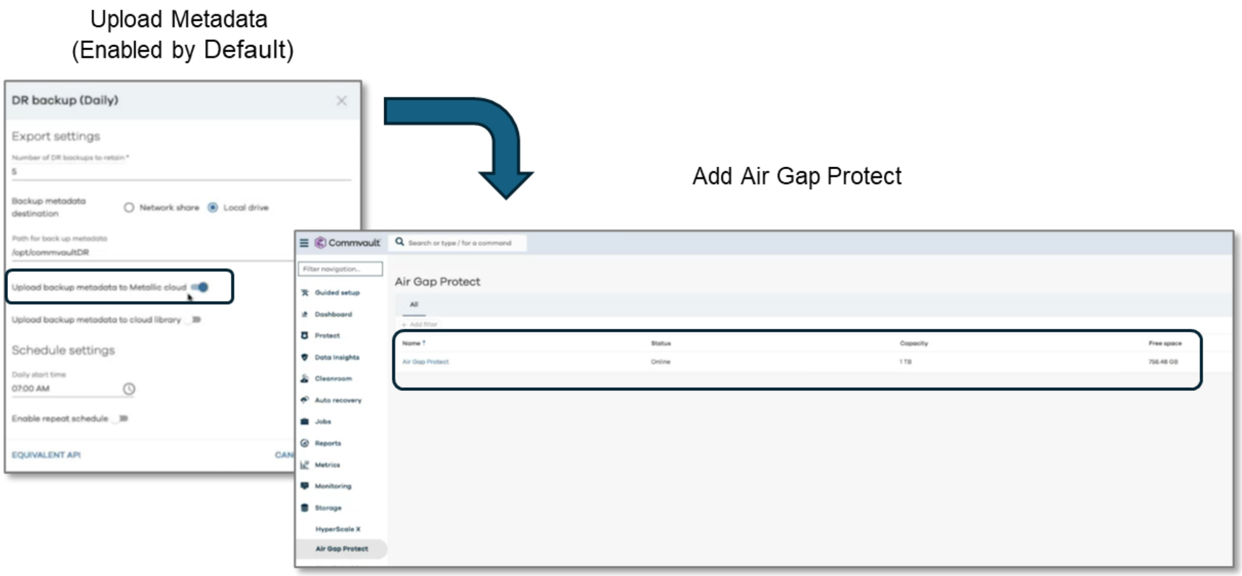
Organizations can use the cleanroom environment to simulate cyberattacks and test their incident response plans, enabling them to identify and address potential weaknesses before facing an actual attack. Conducting regular drills using Cleanroom Recovery can help security and IT teams stay sharp and apply continuous improvements to the cyber-recovery plan for effectiveness in real cyberattacks.

The cleanroom provides a controlled environment for forensic analysts to investigate the attack timeline, identify the attack's origin, and gather evidence for potential legal proceedings. Once vulnerabilities are identified, the cleanroom can be used to develop, test, and deploy security patches in a safe and controlled environment before applying them to production systems.

Even if some data is compromised on production systems, a cleanroom can be used to extract clean versions of critical data from uninfected backup sources. When the integrity of production is in question, a cleanroom allows for a safe and secure place to begin recovery while the production environment is being remediated. In completely compromised environments, a cleanroom creates a safe target to recover into and begin running the business from. If a new production environment is desired, clients can move workloads out of the cleanroom when ready.

First, we examined how a customer would implement Cleanroom Recovery in their environment. A requirement for Cleanroom Recovery is to upload backup metadata to Commvault Cloud. This is the default configuration in Commvault deployments, so no action is needed. Users need only to add Air Gap Protect to their environment to enable Cleanroom Recovery (Figure 4).

Figure 4. Enabling Cleanroom Recovery in 1 Step



Upload Metadata
(Enabled by Default)

DR backup (Daily)

Export settings

Number of DR backups to retain *: 5

Backup metadata destination: ○ Network share ● Local drive

Path for back up metadata: /opt/commvaultDR

Upload backup metadata to Metallic cloud: on

Upload backup metadata to cloud library: off

Schedule settings

Daily start time: 07:00 AM

Enable repeat schedule: off

Add Air Gap Protect

Air Gap Protect

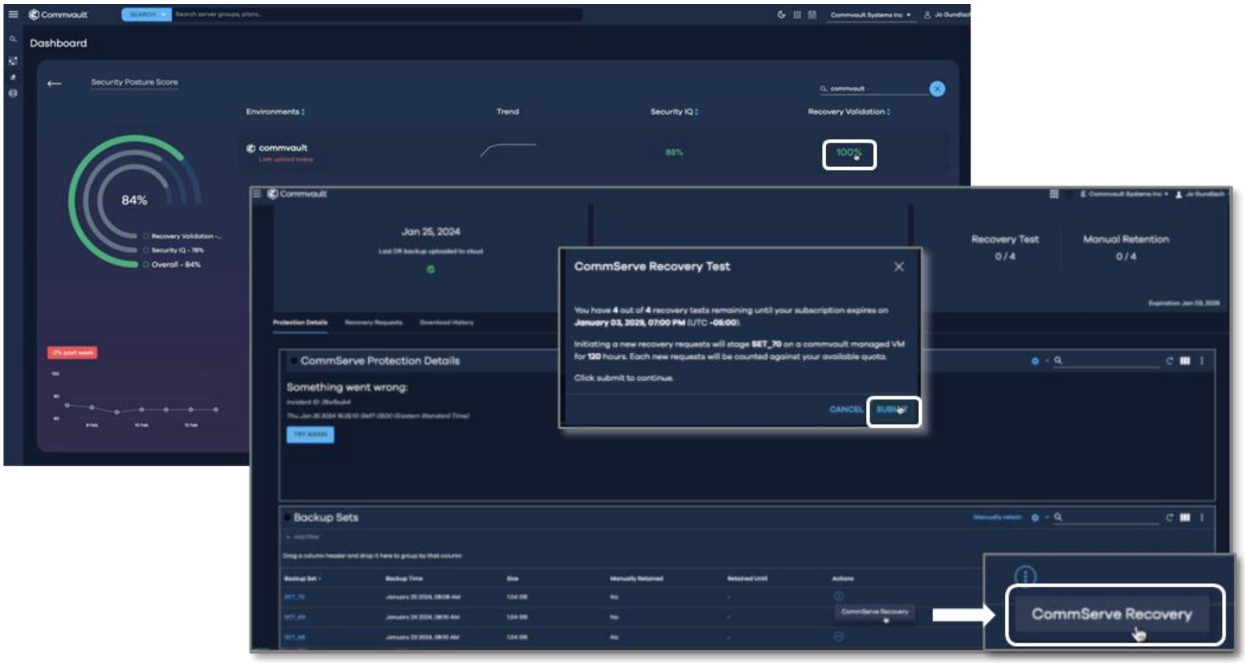
Name ↑	Status	Capacity	Free space
Air Gap Protect	Online	1 TB	756.48 GB

Source: Commvault and Enterprise Strategy Group, a division of TechTarget, Inc.

Cleanroom Recovery supports the recovery of predefined recovery groups for virtual machines into a Microsoft Azure tenant, provided by the client, that has never been accessed by production accounts or connections. The control plane, Commvault's CommServe database, is recovered to Commvault's SaaS environment.

Executing Cleanroom Recovery begins with the user logging into the Commvault Cloud environment and selecting **Recovery Validation** from the Security Posture screen. On the Recovery Validation screen, we selected the environment to recover, then chose a recovery point to restore.

Figure 5. Initiating Cleanroom Recovery



CommServe Recovery Test

You have **4** out of **4** recovery tests remaining until your subscription expires on **January 03, 2029, 07:00 PM** (UTC **-05:00**).

Initiating a new recovery requests will stage **SET_70** on a commvault managed VM for **120** hours. Each new requests will be counted against your available quota.

Click submit to continue.

CANCEL SUBMIT

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

At the confirmation window, we clicked **Submit,** and the control plane recovery test proceeded. It's important to note that the control plane is restored with a read-only, limited-access user and password to protect against compromised credentials. Once the recovered control plane is live, a user creates the Azure hypervisor(s) to recover to and recovery groups. In the recovery group, the servers to recover to the cleanroom are defined. Users can set recovery order and priority to ensure application dependencies are met.

While we performed a manual recovery in this test, Cleanroom Recovery can serve as an automated production failover solution in the event of a breach or other availability event, ensuring that production operation recovery into a sanitized environment can be conducted with a minimum of effort.

Why This Matters

Ransomware poses an existential threat to businesses. While many organizations have a cyberincident response strategy, they lack the ability to reliably test cyber-recovery plans to ensure readiness. Periodic and successful testing, documentation, and validation—which many organizations have found hard to achieve—is essential to a comprehensive and executable cyber-resilience strategy and working plan. Because testing cyber-recovery plans is complex and expensive, many organizations rely on simulations, tabletop exercises, and checklists.

Enterprise Strategy Group found that Commvault Cloud Cleanroom Recovery provides a clean, secure environment that enables organizations to perform frequent, auditable testing and forensic analysis, enabling them to recover quickly and safely, regardless of where their source data lives.

Conclusion

The vast majority (89%) of respondents to Enterprise Strategy Group research ranked ransomware as one of the top five threats to the viability of their organization, and three in four of those organizations reported a successful attack in the last 12 months. Multiple attacks are the norm, as are multiple demands for payment, even after an organization has paid the ransom. Attack methods have become diverse and creative, with bad actors using social engineering and other techniques to acquire valid credentials, rather than relying solely on malware to deliver their payloads.

Enterprise Strategy Group validated that Commvault Cloud Cleanroom Recovery provides a verified, clean, and isolated environment to prepare for and respond to cyberincidents. Commvault Cleanroom Recovery automates the recovery of the Commvault Cloud control plane into a Commvault Cloud SaaS tenant, then automates the recovery of virtual machines out of Commvault Cloud Air Gap Protect into a client-provided Azure tenant based on the recovery groups that are defined by the client.

In short, Commvault Cleanroom Recovery is the first and only solution to date Enterprise Strategy Group has validated that enables recovery to an assured-to-be-clean environment, made possible by Commvault's any-to-any portability.

We found that Commvault Cleanroom Recovery helps organizations achieve the following goals:

- **Auditable, periodic cyber recovery plan testing.** The recovery audit feature enables organizations to meet compliance requirements with auditable evidence and proof of success. Automation enables organizations to test more frequently, based on threat signals.
- **Forensic analysis.** Organizations can use Cleanroom Recovery to investigate attack timelines, identify attacks' origins, and gather evidence for potential legal proceedings.
- **Secure data recovery.** A cleanroom can be used to extract clean versions of critical data from uninfected backup sources, even when data is compromised on production systems. A cleanroom allows for a safe and secure location to begin recovery while the production environment is being remediated.

Cyber resilience requires a detailed and secure cyber recovery plan with regular, auditable testing to ensure that an organization can recover quickly and—more importantly—into a clean environment free from infection. Enterprise Strategy Group confirmed that Commvault Cleanroom Recovery delivers what is needed to accomplish this.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group 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