Commvault®

INCREASE YOUR CYBER RESILIENCE

———

WITH COMMVAULT CLOUD® CLEANROOM™ RECOVERY

CONTENTS

WHAT IS A CLEANROOM?

A cleanroom, also known as an Isolated Recovery Environment, is **not** just a physically secure space.

It's a fortress of data protection, a comprehensive approach to cyber recovery. It's a secure, standalone environment, meticulously planned and executed, with established processes, best practices, testing, and well-defined procedures.

The technology behind a cleanroom is not magic; its true power lies in its ability to bring these diverse elements together into a cohesive and effective unit, enhancing your data's safety and security.

Commvault®

WHY DO YOU NEED ONE?

Cyberattacks have increased and escalated dramatically in recent years, posing a substantial and immediate threat to organizations across all industries.

These attacks can have devastating consequences, including data breaches, financial losses, and irreparable reputational damage. The urgency to protect your data has never been more pressing.

Most cyberattacks begin without malware. This means the attackers will still gain access regardless of how strong a frontline defense your security has.

Attackers today no longer hack in.

They login.

According to IBM's Security Group, once the attacker has gained access, the **average time they are in an enterprise is**

204 DAYS.[1]

Within the first

84 MINUTES,

attackers move laterally. This means that during those 204 days, attackers quietly move east and west throughout the environment, exploring and exploiting vulnerabilities. This time is known as the left of bang, a term used to describe the period before the full impact of an event is felt.

When attackers enact the encryption event, known as "bang," the damage is so pervasive that, **on average, it takes**

21 DAYS

to restore critical systems. The days spent analyzing and recovering from the cyberattack are the right of a bang, a term used to describe the period after the full impact of an event is felt.

Companies that don't have a recovery option and decide to pay the ransom do not fare better. **Over**

90% OF COMPANIES

that pay the ransom do not get all their data back; on average, they **recover less than 70% of their data**.[2]

However, you can be confident in your data recovery with cleanroom technology. Companies are discovering that **decryption times**

FAR EXCEED

the time it would have taken to restore from backups, making cleanroom technology a more effective and efficient solution. Businesses that pay the ransom are attacked again within a month because they are still operating in an infected environment.

1   https://www.ibm.com/reports/threat-intelligence
2   https://www.sophos.com/en-us/content/state-of-ransomware

KEY USE CASES FOR CLEANROOM ENVIRONMENTS

A cleanroom environment is essential for cyber recovery strategies. It provides a cost-effective and flexible space for testing and a secure area to analyze, restore, and remediate systems affected by cyberattacks. Cleanrooms provide faster recovery, minimize data loss, and enhance resilience against cyber threats.

Here are some critical use cases for a cleanroom in cyber recovery:

Continuous Cyber Recovery Plan Testing

- Organizations can utilize the cleanroom to replicate cyberattacks and assess their incident response plans, identifying and rectifying potential weaknesses before encountering an actual attack.

- Regular drills in a cleanroom environment can help security and IT teams stay sharp and continuously improve the cyber recovery plan for real cyberattacks.

Incident Response and Forensics: Post-Mortem Analysis

- The cleanroom offers a controlled environment for forensic analysts to investigate the attack timeline, pinpoint the attack's origin, and collect evidence for potential legal proceedings.

- The cleanroom can develop, test, and deploy security patches in a safe and controlled environment before applying them to production systems.

Secure Data Recovery

- A cleanroom can extract clean copies of critical data from uninfected backups even if some data is compromised on production systems.

- When production integrity is questioned, a cleanroom provides a safe and secure place to begin recovery while the production environment is being remediated.

- Cleanrooms provide a safe and secure environment for starting recovery while the production environment is being remedied when production integrity is questioned.

COMMVAULT® CLOUD CLEANROOM™ RECOVERY

Cleanroom Recovery offers an affordable, clean, secure, isolated recovery environment on demand for testing cyber recovery plans, conducting secure forensic analysis, and ensuring uninterrupted business continuity.

Commvault's solution can recover workloads from any location to a secure, cloud-isolated cleanroom, enhancing your cyber resilience and readiness. **Our key differentiators include:**

Any-to-Any Portability

This allows recovery of any workload from any location to another. Traditionally, apps and data from various systems would require duplicating all environments for rest and recovery.

Reduce Cost and Complexity

Able to utilize a flexible cleanroom approach, reducing cost and complexity. Pay for what you need when you need it.

Read-Only Control Plane

We initiate cleanroom recovery with a read-only control plane to prevent access if the production environment is compromised.

AI/ML Technology

Utilizing AI/ML technology to identify and select reliable recovery points automatically.

Traditional Cleanrooms

Traditional cleanroom methods are often **too expensive and complex** for many organizations. Other data security solutions with similar offerings are limited to disaster recovery and constrained by a limited set of workloads and recovery options.

Commvault®

INTEGRATION DETAILS

Commvault Cleanroom Recovery automates the recovery of the Commvault Cloud Control Plane into a Commvault Cloud SaaS tenant. Then, it automates the recovery of virtual machines out of Commvault Cloud Air Gap Protect into a client-provided Azure tenant based on the defined recovery groups.

Figure 5 (below) illustrates what a client environment would look like today for a Commvault software client. The Recovered Control Plane will be in the same region as the Air Gap Protect storage (for example, US Central), and the target environment should be in the same region.
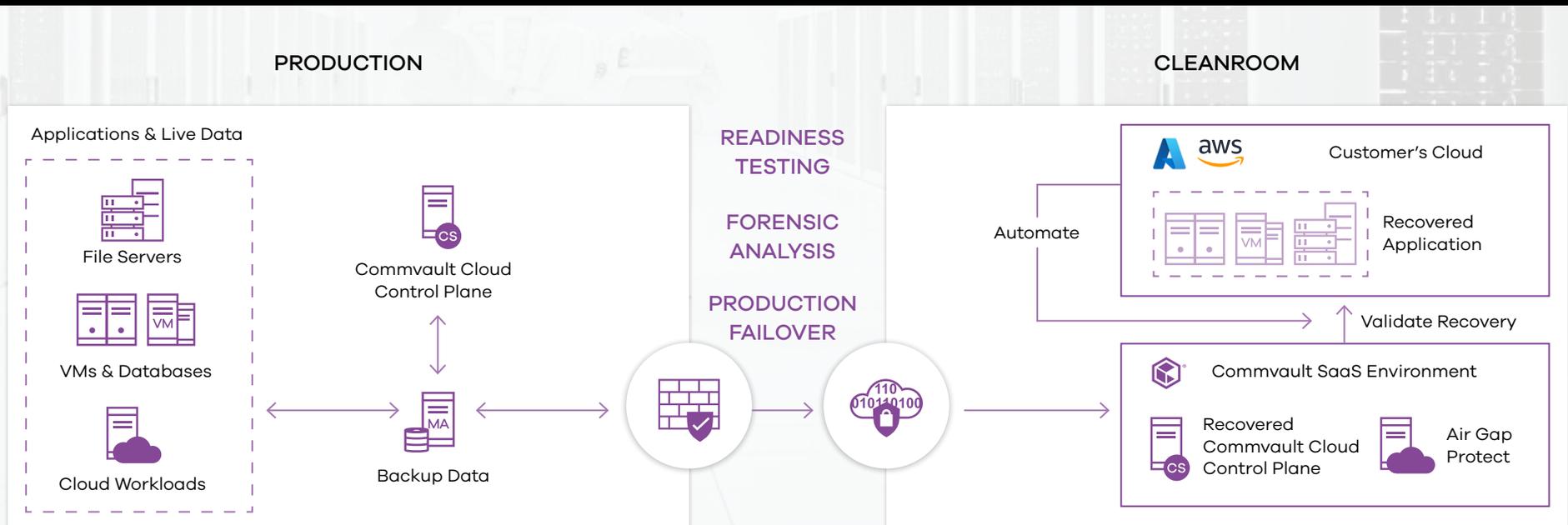
Recovered VMs will be automatically cleaned up (deleted from the cleanroom target) **four days** after the control plane recovery. The recovered VMs can be kept longer by contacting Commvault support. Customers who want to transition the recovered VMs into production can work with Commvault professional services and local service providers.

STEPS TO INITIATE CLEANROOM RECOVERY

STEP 01

Recover the Control Plane

Log into cloud.commvault.com and initiate the control plane recovery process. You will receive emails notifying you of the start and completion of the control plane recovery.

STEP 02

Prepare the Recovery Environment

Create a separate Azure tenant.

STEP 03

Add Target Azure Hypervisor

Log into the newly recovered Commvault UI and add the Azure hypervisor as a recovery destination.

STEP 04

Add a Cleanroom Recovery Target

Log into the Commvault UI and create the recovery target that points to the Azure environment created in Step 02.

STEP 05

Create a Recovery Group

Create a recovery group and add the workloads you want to recover, or choose an already existing recovery group and initiate the recovery.

CLEANROOM SERVICES

Commvault offers a suite of Cleanroom services to design, install, test, and when required, respond. By using Commvault services, you can be confident that our experts bring years of Commvault Cloud experience to help develop your recovery strategy and work with you so that you are ready in the event of a cyberattack.

This table details the benefits and scope of the Cleanroom Design & Install, Readiness Testing, and Incident Response services.

SERVICE	BENEFITS	SCOPE
Design and Install	✓ Plan and build the capability to quickly recover production assets into an isolated recovery environment, the cloud.	**Plan and Configure the Commvault Features** • CommServe Recovery Validation Service • Air Gap Protect • Cleanroom Application Recovery **Initial Testing** • Control Plane Recovery Test • Recovery Group Test
Readiness Testing	✓ Build confidence in your IT team's ability to recover from a cyberattack by regularly testing your Cleanroom Recovery Plan and updating it as needed.	**Control Plane Recovery** • Recover the control plane • Perform a test restore • Export evidence **Recovery Test** • Execute Control Plane Failover • Restore recovery group(s) in Azure as needed for analysis
Incident Response	✓ Recover production assets quickly into an isolated environment for forensics and analysis when recovering from a cyberattack.	**Cleanroom Recovery** • Execute Control Plane Failover • Restore Recovery Group(s) in Azure as needed for analysis

COST BREAKDOWN

What is needed to make the purchase?

Cleanroom Recovery is sold in 10 TB increments. To determine the 10 TB measurement, the customer configures data into a Recovery Group based on front-end terabytes.

For example, suppose a customer configures 100 TB of data into the recovery groups (based on the data size at the time of configuration). In that case, the customer must purchase 10 units. If the client needs to configure 104 TB of data, they must buy 11 units. A 10-unit SKU is $1,590 USD.

To leverage Commvault Cloud Cleanroom Recovery, customers need:

• Cleanroom Recovery SKU

• Air Gap Protect

• Backup & Recovery (from any of the packages)

  - For software: Version 11.34.13 or higher

  - For SaaS: Version 11.36 or higher

• Any of the Commvault Cloud tiers—Operational Recovery, Autonomous Recovery, Cyber Recovery, Platinum Resilience

Book a meeting with Commvault today to learn more about how you can increase your resilience with Cleanroom Recovery.

commvault.com | 888.746.3849 | get-info@commvault.com

Commvault®