WHITE PAPER

ESSENTIAL GUIDE TO CLEANROOM RECOVERY

v1.4e | April 2026

Commvault®

Commvault

Table of Contents

Introduction

WHAT IS A CLEANROOM

A cleanroom, often termed an Isolated Recovery Environment (IRE), is a secure, separate environment designed for cyber recovery. To understand why cleanrooms are essential, you must first recognize a critical challenge. During a sophisticated cyberattack, it is not just your production systems that are at risk; your backup infrastructure can be compromised as well. Attackers are increasingly targeting backups directly, knowing that organizations rely on them for recovery. This means that recovering from traditional backups might inadvertently restore the very threats you are trying to eliminate, reinfecting your rebuilt environment.

Cleanrooms solve this problem through isolation. By maintaining a separate environment that is disconnected from your production network, a cleanroom provides a space where you can safely recover and analyze data without risk of cross-contamination. This isolation works in both directions. Threats in your production environment cannot spread into the cleanroom, and any malware discovered during recovery within the cleanroom cannot reinfect your production systems. If you find ransomware on a virtual machine recovered in the cleanroom, it was present in the backup itself and not the result of a new infection.

At its core, the cleanroom concept is simple. For example, backup tapes stored in a disconnected colocation facility would meet the technical requirements of a cleanroom. However, the reality of executing recovery this way during a crisis involves significant manual effort, coordination challenges, and time constraints. A cleanroom's true value comes from making this operationally practical by combining infrastructure with orchestration, automation, planning, and procedures that enable fast, reliable recovery. Commvault's cleanroom functionality transforms the concept into a practical solution by streamlining what would otherwise be a complex, time-consuming process.

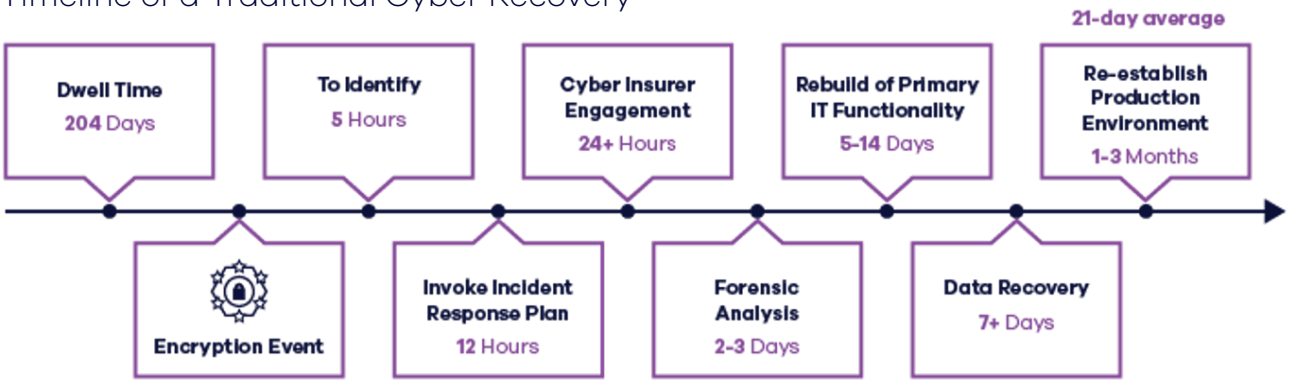
A truly effective cleanroom encompasses more than just isolated infrastructure. It requires meticulous planning, established processes, best practices, testing, and well-defined procedures. The power of a cleanroom lies in bringing all these elements together into a cohesive and effective cyber recovery strategy.

CYBERATTACKS: A RETROSPECTIVE

Why have cleanrooms become a **critical** capability for a successful cyber-resiliency posture?

- Most cyberattacks begin without malware (Liu et al.). This means that regardless of the strength of your security's frontline defense, it will not stop the attackers from gaining access. Attackers do not need to hack in when they can login.
- Once the attacker has gained access, the average time they are in an environment, according to IBM's Security Group, is 204 days. Within the first 84 minutes, according to CrowdStrike, attackers are moving laterally. This means that during those 204 days, attackers quietly move east and west throughout the environment. These 204 days are known as left of bang, referring to the position on a timeline preceding an event.
- When attackers enact the encryption event, (the "bang") the damage can be so pervasive that on average recovery from a cyberattack takes 21 days just to restore critical systems. The days spent analyzing and recovering from the cyberattack are known as right of bang.
- Companies that do not have a recovery option and decide to pay the ransom do not fare better. Over 90% of companies that pay the ransom do not necessarily get all their data back. On average they recover less than 70% of their data. Additionally, decryption times can exceed the time it would have taken to recover from backups.
- Businesses that pay the ransom are attacked again within a month, on average, because they are still operating in an infected environment.

Timeline of a Traditional Cyber Recovery



- Once signs of an attack have been identified, an individual with the proper authority declares the breach and initiates the Incident Response Plan.
- The first several days are taken up by processes outside of recovery.
- 98% of all companies use Active Directory, and Active Directory is a frequent target (Prakash). Therefore, a clean Active Directory must be recovered or created before any other recovery can begin.
- Many attacks are so devastating that the environment is impossible to recover back to. Customers are left scrambling for hardware and a location to recover when this happens.
- Attackers often target data protection solutions because they are both the last line of defense for recovery and a single repository containing all the company's critical data.

RPO/RTO AND THEIR LIMITATIONS IN CYBER RECOVERY

Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are primary metrics in disaster recovery, defining acceptable data loss and restoration timeframes. However, several factors make their direct application problematic in cyber recovery.

Identifying and isolating clean data from potentially infected backups make defining a clear RPO impractical when relying on forensic investigations and deep analysis to validate data integrity before restoration.

The time needed for investigation, remediation, and secure restoration varies depending on the attack's complexity and scope. Setting a fixed RTO during an ongoing threat can be misleading and counterproductive.

While minimizing data loss is important, cyber recovery prioritizes delivering a securely recovered environment and preventing further compromise. Think of it this way. If you can meet a 24 hour RTO through a full data recovery in 20 hours, that leaves four hours to spare. But, if that recovery reintroduces malware from a cyber event into the environment, the data will be re-encrypted in hours, forcing at least one more attempt recovery that requires even more time. The holistic approach with a security mindset encompasses system forensic analysis, and hardening and vulnerability patching, which can extend the recovery timeline beyond the RPO defined by the DR.

RTO and RPO strategies rely heavily on critical items of the environment, such as Active Directory, databases, and network switch configurations, leveraging replication for protection. During a cyberattack, replication cannot be trusted because it has no built-in anomaly detection. It will propagate compromised accounts, exploits, and hidden infections. Since replication cannot be trusted, these items must be rebuilt, adding to the time required for recovery going beyond the standard RTO and RPO.

Sole reliance on conventional disaster recovery plans and rigid adherence to RPO/RTO metrics during cyberattacks can leave organizations exposed. Recognizing this, CISOs are shifting their focus toward Maximum Allowable Downtime (MAD) or Maximum Tolerable Downtime (MTD).

MAD or MTD offers a more holistic perspective on cyber resilience. Rather than solely emphasizing data and system restoration to a specific point, it defines the maximum duration of outage an organization can sustain without significant harm to the business, such as inability to produce, sell, or generate revenue. This comprehensive lens encompasses the entire incident response lifecycle, from initial attack to full business resumption, including impacts on people, processes, and technology.

Implementing a dedicated, security-focused cyber recovery plan with tools and expertise is crucial for achieving successful and secure restoration while minimizing damage and enhancing future resilience. Organizations need both disaster recovery and cyber recovery plans. Each addresses different types of disruptions and requires distinct approaches, metrics, and expertise to achieve robust organizational resilience.

USE CASES

A cleanroom plays a crucial role in cyber recovery strategies by providing an air gapped environment for recovery, as well as a safe and secure space to analyze, test, and remediate systems affected by cyberattacks. Just as a DR plan cannot be reused as a cyber recovery plan, a DR site cannot be repurposed as a cleanroom. DR sites must remain accessible to users and applications to function during a disaster, while cleanrooms require complete network isolation to prevent contamination. These conflicting requirements mean organizations need separate infrastructure for each purpose. This presents a challenge for businesses from both cost and flexibility perspectives.

Given the financial challenges of a physical cleanroom design (cold compute, storage, backup infrastructure, networking, facility, etc.), Commvault's Cleanroom Recovery capabilities deliver value by deploying one-to-many cleanrooms on demand in the cloud, eliminating the high upfront capital costs.

Continuous Cyber Recovery Plan Testing:

- A cleanroom can be used to simulate cyberattacks and test incident response plans, identifying and addressing potential weaknesses before facing an actual attack.
- Regular drills using the cleanroom environment can help security and IT teams stay sharp and apply continuous improvements to the cyber recovery plan for effectiveness in real cyberattacks.

Incident Response and Forensics – Post-Mortem Analysis:

- 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.

Secure Data Recovery:

- 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 a completely compromised environment, a cleanroom provides a safe target for recovery and a secure place from which to restart business operations. If a new production environment is needed, workloads can be moved out of the cleanroom when ready.

By leveraging these capabilities, cleanrooms are critical in any organization's cyber recovery strategy, enabling faster recovery, minimizing data loss, and improving overall resilience against cyber threats.

WHEN IS CLEANROOM RECOVERY NOT RECOMMENDED

While cleanrooms offer significant advantages for cyber recovery, there are situations where there might be better solutions. Here are some cases where using a cleanroom might not be recommended.

Insufficient data redundancy:

- Cleanroom Recovery relies on clean backups for restoring data. If adequate backups are unavailable or have not been properly isolated from the attack, the cleanroom environment becomes less helpful.

Highly specialized systems:

- Certain complex systems might depend on specific hardware or software configurations that cannot be easily replicated with Cleanroom Recovery.

Inability to use the cloud:

- If regulations do not allow customers to run workloads in a cloud environment, they cannot take advantage of Cleanroom Recovery.

The decision to use a cleanroom for cyber recovery depends on many factors, including the organization's risk profile, resources, and the nature of the cyberattack. Carefully evaluating the specific situation and comparing the benefits and drawbacks is crucial for choosing the most effective approach.

Commvault's on premises cleanroom recovery can be combined with cloud cleanroom recovery to deliver isolated recovery for many of the above use cases, however it is important to remember that the complexities and costs of architecting on premises cleanrooms means that only the workloads that cannot be recovered in cloud should use this mechanism.

A cyber recovery strategy should be comprehensive and multi-layered, utilizing different methods and tools depending on the circumstances. While cleanrooms provide valuable capabilities, considering alternative approaches and understanding their limitations delivers a well-rounded defense against cyber threats.

Details of Cleanroom Recovery

Commvault Cleanroom Recovery automates the recovery of Commvault's Control Plane within a Commvault Cloud SaaS tenant. Then, it automates the recovery of virtual machines within a recovery group into your organization's cloud tenant (Azure or AWS). Because Commvault must control the end-to-end movement of data, this feature only works for virtual machines that have a protection copy within Commvault Cloud Air Gap Protect (Commvault's immutable, air gapped cloud storage).

AUTO-SCALING RECOVERY

In the face of increasingly sophisticated cyberattacks, organizations need a robust and agile data protection strategy. Auto-scaling recovery is a cornerstone of Commvault's Cleanroom Recovery solution, designed to address the complexities of modern data recovery. When a cyber event strikes, you do not want to manually provision infrastructure and guess at capacity requirements. Auto-scaling eliminates this concern by automatically adjusting the number of access nodes (cloud resources deployed to perform recovery operations) based on workload demands. This intelligent approach delivers optimal performance and recovery times, while controlling costs by only consuming the cloud resources needed to achieve required recovery performance during active restoration operations. For Cleanroom Recovery, these scaling operations occur within your Azure or AWS environment, preserving data sovereignty and control. This unique combination of automation, performance, and security makes auto-scaling an invaluable asset for any organization seeking to bolster its cyber resilience.

REPAVE VM

Following a sophisticated cyberattack involving exploits and compromised accounts, the cleanliness of both the overall system and the data are key to a successful recovery. The repave process provides a robust solution by provisioning an unaffected system and reinstalling it with clean, verified software, creating a fresh starting point for recovery.

Even if malware is completely removed, the system would still contain the vulnerabilities that allowed the initial attack. These entry points must be addressed, and the manual process of identifying and remediating each one is both time consuming and error prone. A single missed vulnerability can lead to immediate reinfection. To validate the integrity of restored systems, repaving the virtual machine using a trusted, known, good image acts as a safeguard against such risks. By implementing these measures, organizations can significantly reduce the risk of reinfection and improve their overall cyber resilience.

This approach is particularly valuable when the attacker's dwell time would force recovery from an older backup, resulting in significant data loss. If forensic analysis determines that application data from recent backups is clean but the underlying system is compromised, the repave approach allows organizations to deploy a clean OS image while recovering application data from a more recent point in time. This reduces data loss while maintaining security as the known, good image eliminates existing system-level compromises.

AUTOMATION: ORCHESTRATION VS. SCRIPTING

One of the key benefits of Commvault's Cleanroom Recovery is the use of orchestration over scripting. While scripting is great for automating individual tasks, do-it-yourself scripts cannot be used to fully manage the complex needs of a cleanroom recovery. Thinking of all the situational requirements such as recovered workloads, access definitions for isolation, varying scenario-based runbooks and validated and current golden images (just to name a few) quickly leads to the key problem. The scripts will have to be modified and free of human error for every recovery effort. Human error is a key component here as well. Imagine a scenario where access to the recovery environment is not isolated or restricted, facilitating a vector for the bad actors to exploit.

The advantage that Commvault brings to automating a cleanroom recovery is that it has all the variables defined within the environment, allowing our software to dynamically adjust scripts on the fly without introducing human error. Workloads can be defined, golden images for pave/repave can be specified, and the isolation is inherently built-in and unmodifiable. The result includes a faster time to recovery with less manual effort, facilitating the combination of reduced manual efforts for more frequent testing opportunity and lower business impact from downtime through quicker recovery and data access.

Capability	Commvault Cleanroom Recovery	DIY Scripting
Same resources require multiple runbooks for different use cases (cyber, DR, ops, testing)	✓ Supported natively with shared groups	✗ Requires separate scripts per use case
Automatic inclusion of newly added resources based on rules	✓ Dynamic groups update all runbooks automatically	✗ Must manually update every script
Centralized configuration: All recovery configuration and runbooks are available in a single place – Commvault Command Center.	✓ Update once, all runbooks inherit changes	✗ Must modify every script for infra/network changes
Automatic on-demand cleanroom deployment	✓ Fully automated, isolated	✗ Extremely complex, error-prone
Recovery order & priority definition	✓ Built-in, intuitive	✗ Must be manually coded; brittle
Distributed app / multi-hypervisor orchestration	✓ Works across VMware, Azure, AWS, GCP	✗ Requires multiple script stacks
Cross-cloud workload conversion	✓ Automatic (driver injection, metadata mapping)	✗ Very difficult, breaks often
Post-recovery threat scanning	✓ Automated malware/ anomaly detection	✗ Must build entire scanning pipeline
Golden image repave	✓ Native	✗ Hard to script securely
Autoscaling recovery infrastructure	✓ Automatic scaling of access nodes/MA	✗ Must build this from scratch
Automatic cleanup of environment	✓ Full lifecycle cleanup	✗ Leads to leftover resources/ costs
Real-time operator interaction (pause/ approve/skip)	✓ Native (Roadmap)	✗ No equivalent
Audit & compliance reporting	✓ Exportable, structured	✗ Must custom-build
Cyber event readiness	✓ Designed for ransomware response	✗ Scripts fail under degraded systems
Maintenance overhead	✓ Low ongoing overhead	✗ High overhead, high fragility

RECOVERY SCRIPTS

Following a recovery, various actions may need to be taken to deliver data integrity and identify potential threats. This often involves executing pre-defined scripts to validate data or using third-party tools to scan for Indicators of Compromise (IoCs: evidence that a system was breached, such as malicious file hashes or unauthorized registry changes), Indicators of Attack (IoAs: signs of active attack techniques, such as suspicious process behaviors or lateral movement patterns), or malware.

To mitigate the risk of executing compromised scripts, Cleanroom Recovery groups and individual entities should store scripts in a secure, isolated repository. This prevents accidental access to infected servers and reduces the likelihood of encountering encrypted or malicious scripts.

In a cleanroom environment, safe, protected scripts can be uploaded directly to the isolated recovery environment for the entire group or individual entities. Once uploaded, these scripts can be reordered to execute in the desired sequence, providing flexibility and control over the recovery process.

CLEANROOM TO PRODUCTION

Commvault builds Cleanroom Recovery in the cloud and on-demand, allowing for instances to be used to isolate recovery for forensics by teams working separately. This affords users the ability to leverage a dedicated cleanroom to recover clean data that can then be promoted to production.

As these verified clean instances come online in the cleanroom, Commvault can facilitate the protection of those cloud instances and use those backups to migrate the cleaned and validated workloads back to the production environment, reducing the time of production outage and the possibility of reintroducing malicious software back into production.

GENERAL REQUIREMENTS

Beyond the environmental requirements, there are some general recommendations to make Cleanroom Recovery successful.

1. Do not tie Commvault privileged users to Active Directory
2. Perform at least one full backup for each virtual machine to be recovered using Air Gap Protect
3. There must be a control plane (CommServe) database backup that is newer than the required recovery date.
4. Install Hyper-V drivers on any Linux servers that may need Cleanroom Recovery. Refer to Commvault Documentation for details.
5. Enable Remote Desktop Protocol (RDP) or SSH on the source VM.
6. For Linux VMs, enable integration services on the source VMs if they will be powered on automatically after conversion.
7. For Windows VMs, enable SAN policy for the source VM.
8. VMs that are encrypted on AWS are created as VMs with no encryption on Azure.

CLOUD INFRASTRUCTURE REQUIREMENTS AND RESOURCE CREATION

During the Cleanroom Recovery process, Commvault creates and configures resources in your cloud environment. This information defines the infrastructure changes made during recovery operations.

Express Configuration for Recovery Groups (Azure Only):

When using the Express Configuration option for the recovery groups, Commvault makes API calls into the recovery target to configure some of the environment. A list of the deployed resources and configurations can be found in Commvault Documentation.

CLEANROOM RECOVERY PROCEDURE SUMMARY

- **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.
- **Prepare the recovery environment:** Create a separate Azure or AWS cloud tenant or subscription.
- **Add target hypervisor:** Log into the newly recovered Commvault UI and add the Azure or AWS hypervisor as a destination for recovery.
- **Add a cleanroom recovery target:** Log into the Commvault UI and create the recovery target that points to the Azure or AWS environment created in step 2.
- **Create a recovery group:** Create a recovery group, add the workloads you want to recover, or choose an already existing recovery group and initiate the recovery.

SUPPORT MATRIX

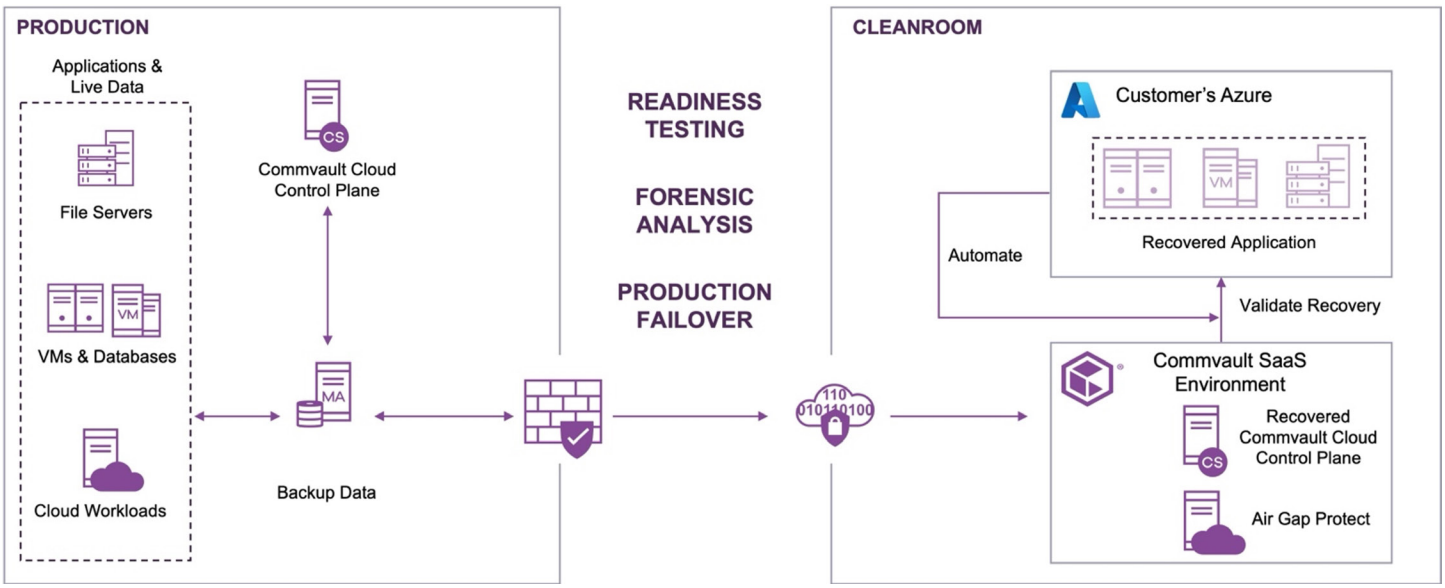
This list shows the tested any-to-any cross hypervisor restore into Cleanroom Recovery. Commvault supports a broader range of sources and targets; as those workloads are tested, they will be supported in Cleanroom Recovery.

Source	Destination: Cleanroom Recovery Azure	Destination: Cleanroom Recovery AWS
On Premises VMware	Yes	Yes
AWS VMC	Yes	Yes
Azure VMware Solution	Yes	Yes
Google Cloud VMware Engine	Yes	Yes
Oracle Cloud VMware Solution	Yes	Yes
Azure VMs	Yes	Yes
AWS EC2	Yes	Yes
Hyper-V	Yes	Yes
Standalone MS-SQL in Windows VM*	Yes	Yes
Standalone DB2 in Linux VM**	Yes	Yes

*MS-SQL backed up in a Windows VM must be a VM application consistent backup
**DB2 backed up in a Linux VM in a crash consistent VM backup

EXAMPLE CUSTOMER ENVIRONMENT AND RECOVERY PROCESS

This illustration shows what an environment would look like today for a Commvault software customer. The recovered control plane will be in the same region as the Air Gap Protect storage (e.g., US Central). The target environment should be in the same region.



BUY VS BUILD

While creating a custom cleanroom target on-premises or in the cloud is feasible, replicating the comprehensive functionality and ongoing development of Cleanroom Recovery presents a significant challenge. This situation reflects a classic "buy vs. build" decision with trade-offs to consider. While building a custom solution offers initial flexibility, the effort required to maintain feature parity with Cleanroom Recovery (including evolving workloads, security enhancements, automation tools, and integrations) can quickly become resource-intensive and unsustainable. As Cleanroom Recovery adds new features and capabilities, the gap between a custom solution and its offerings will widen. Organizations considering this path should carefully evaluate the long-term development and maintenance costs compared to the immediate benefits of a custom-built solution.

AVAILABLE CONSULTING SERVICES

While setting up Commvault's Cleanroom Recovery is straightforward, the challenge lies in navigating the complexities of cyber recovery. This includes understanding the process, planning effectively, testing rigorously, and ensuring your overall data protection is cyber-ready.

That is where Commvault Cyber Resilience Services come in. Our team of experts combines deep Commvault knowledge with proven cyber recovery experience. This unique blend empowers us to guide you through every step of your cyber recovery journey, helping you achieve true cyber resilience.

Commvault offers a comprehensive suite of Cleanroom services tailored to your specific needs. We help you plan, test, and even execute cyber recovery when necessary.

By partnering with Commvault, you gain access to years of expertise in Commvault Cloud and cyber resilience. We work collaboratively to develop a robust recovery strategy, giving you the confidence to face cyber threats. Commvault Cyber Resilience Services include:

- **Cyber Resilience Index:** Understand current state of the data protection environment measured against best practices for cyber resilience
- **Cyber Resilience Remediation:** Remediation of all recommendations found during the Cyber Resilience Index engagement.
- **Cyber Response Planning:** Detailed Commvault plan for responding to a cyber incident.
- **Cyber Resilience Tabletop:** Practice running through a recovery scenario that simulates a cyber recovery.
- **Cleanroom Planning:** Assistance creating a detailed plan for testing and executing based on response plan and tabletop exercise.
- **Cleanroom Setup:** Assistance setting up and configuring Cleanroom Recovery.
- **Cleanroom Testing:** Assistance performing cyber recovery testing leveraging Cleanroom Recovery.
- **Cleanroom Execution:** Assistance executing the cyber recovery plan when a cyber event occurs.

COMMON MISCONCEPTIONS

Many organizations conflate disaster recovery with cyber recovery. It's important to understand the difference between basic disaster recovery (DR) preparedness and being truly ready for malicious attacks. While traditional disasters offer a degree of predictability, cyberattacks are chaotic and unpredictable.

The pervasive and adaptable nature of attackers creates a fundamental uncertainty: we can never be confident to the true extent of the compromise. This inherent ambiguity demands a proactive approach beyond static plans. Continuous testing is the cornerstone of building cyber resiliency.

Traditional DR exercises, often scripted and predictable, fall short in simulating the complexities of cyberattacks. Tabletop exercises run through realistic attack scenarios more effectively, mimicking the chaos and pressure of a real-world incident. This helps you identify weaknesses in your plan and response procedures before an actual attack occurs. The challenge is that performing a true real-world recovery requires a place to recover, which is complex and cost

prohibitive. Commvault Cleanroom Recovery offers a cost-effective and flexible solution to bridge this gap by providing a secure, isolated environment for realistic cyber recovery testing.

Your organization can navigate the ever-evolving cyber landscape by embracing continuous testing within a secure, controlled environment. Commvault Cleanroom Recovery empowers you to build cyber resilience, supporting business continuity and data protection in the face of sophisticated attacks.

Summary

EXECUTIVE SUMMARY

Cyberattacks have evolved into a pervasive and sophisticated threat, posing a significant danger to organizations of all sizes. The ever-changing nature of cyber threats necessitates a robust and adaptable approach to cyber recovery. Commvault Cloud's Cleanroom Recovery addresses this critical need by providing a comprehensive testing and failover solution that enables organizations to mitigate cyber risk effectively.

THE LIMITATIONS OF TRADITIONAL CYBER RECOVERY TESTING

Traditional cyber recovery testing methods, such as tabletop exercises, often fail to adequately prepare organizations for the complexities and chaos of real cyber recovery scenarios. These exercises typically involve discussions and simulations that lack the realism and urgency of an actual attack.

Moreover, testing cyber recovery plans in hybrid environments can be time-consuming, complex, and expensive. With workloads spread across multiple clouds, on-premises hypervisors, and physical servers, organizations must perform testing within each environment separately.

THE NEED FOR CLEANROOM RECOVERY

Cleanroom Recovery provides a safe and isolated environment where organizations can test their cyber recovery plans without disrupting production systems. This environment allows organizations to identify and address gaps in their plans before an actual attack occurs.

In addition to testing, cleanroom environments can be used for forensic analysis of known infected systems. This analysis can help organizations understand the root cause of an attack and take steps to prevent future incidents.

COMMVAULT CLOUD'S CLEANROOM RECOVERY: A COMPREHENSIVE SOLUTION

Commvault Cloud's Cleanroom Recovery is a comprehensive testing and failover solution enabling organizations to mitigate cyber risk effectively. It provides a safe and isolated environment for testing cyber recovery plans, conducting forensic analysis, and supporting business continuity in case of a breach.

Key Features of Commvault Cloud's Cleanroom Recovery

- Comprehensive testing environment: Cleanroom Recovery provides a safe and isolated 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.
- Faster recovery times: Cleanroom Recovery can help organizations recover from cyberattacks more quickly by providing a streamlined recovery process.
- Reduced downtime: Cleanroom Recovery can help organizations minimize downtime by providing a production failover solution.

BENEFITS OF COMMVAULT CLOUD'S CLEANROOM RECOVERY

- Improved cyber resilience: Cleanroom Recovery can help organizations improve their cyber resilience by providing a comprehensive testing, analysis, and failover solution.
- Reduced risk of re-infection: Cleanroom Recovery provides a safe and isolated environment where workloads can be recovered without re-infection risk.
- Enhanced security: Cleanroom Recovery can be used to identify and address security vulnerabilities in cyber recovery plans.
- Simplified failover: Cleanroom Recovery can serve as a production failover solution in the event of a breach, so that production operation recovery is conducted within a sanitized environment.

DEEP DIVE INTO CLEANROOM RECOVERY

Testing Cyber Recovery Plans in a Hybrid Environment: Commvault Cloud's Cleanroom Recovery simplifies and streamlines the process of testing cyber recovery plans in hybrid environments. With its any-to-any portability feature, Cleanroom Recovery allows organizations to recover workloads from multiple clouds, on-premises hypervisors, and physical servers to a common environment within the cleanroom. This eliminates the need to perform testing within each environment separately, saving time and resources. Forensic Analysis of Known Infected Systems: In addition to cyber recovery testing, Commvault Cloud's Cleanroom Recovery provides a secure environment for conducting forensic analysis of known infected systems. This analysis can help organizations identify the root cause of an attack, understand how the attackers gained access to their systems, and take steps to prevent future incidents. Production Failover in the Event of a Breach: Cleanroom Recovery can serve as a production failover solution in the event of a breach. If a cyberattack disrupts an organization's production systems, they can recover their workloads to a clean environment within the cleanroom. This can help organizations minimize downtime and get their business back up and running.

CONCLUSION

In today's dynamic cybersecurity landscape, organizations must proactively address the ever-increasing threat of cyberattacks. Commvault Cloud's Cleanroom Recovery is a powerful tool for organizations to enhance their cyber resilience by providing a comprehensive testing environment, secure forensic analysis capabilities, and a production failover solution. By adopting Cleanroom Recovery, organizations can test their cyber recovery plans, identify and remediate vulnerabilities, and deliver business continuity in the face of cyberattacks.

Works Cited

Liu, Side, et al. "A Survey on the Evolution of Fileless Attacks and Detection Techniques." Computers & Security, vol. 137, 2024, doi:10.1016/j.cose.2023.103653. Accessed 8 Jan. 2026.

Prakash, Ravi. "Active Directory Under Siege: Why Critical Infrastructure Needs Stronger Security." The Hacker News, 16 Nov. 2025, thehackernews.com/2025/11/active-directory-under-siege-why.html. Accessed 8 Jan. 2026.