Commvault | PRESIDIO

CLEANROOM CLASH

Evaluating the Best Solutions for Optimal Performance

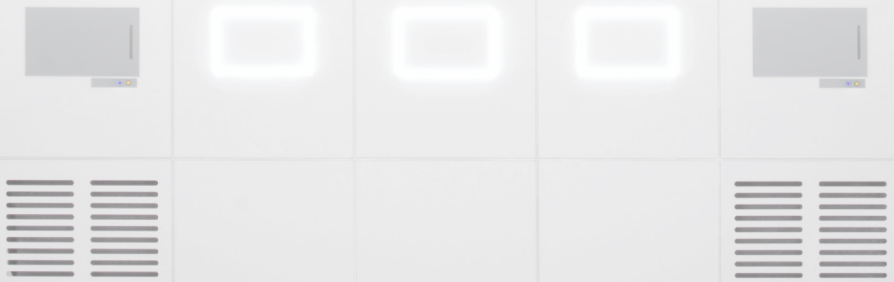
Cleanroom Comparison Guide

This guide provides a detailed comparison between traditional cybersecurity measures and modern cleanroom solutions, emphasizing the advanced capabilities of Isolated Recovery Environments (IRE) in the context of increasing cyber threats. All too often the limitations are hidden in the fine print of the solution.

Traditional cybersecurity approaches often rely on secure locations that, while necessary, are no longer sufficient in the face of sophisticated cyberattacks. These legacy systems typically focus on perimeter defense and after-the-fact threat mitigation, which may not effectively prevent or recover from modern cyber threats that bypass initial defenses. Many of these "cleanrooms" are cobbled together leveraging legacy platforms.

In contrast, modern cleanrooms offer a holistic approach to cyber recovery. They are not just physically secure spaces but are comprehensive systems that leverage the robust scalability and isolation that comes as part of the public cloud. These modern offerings are separated from the production network with meticulous planning, leverage established processes, best practices, rigorous testing, and precise procedures. This integration creates a robust defense mechanism that not only protects data but also helps provide operational continuity in the aftermath of a cyber incident. The strength of a cleanroom solution lies in its proactive stance—preparing organizations to handle and quickly recover from cyber disruptions rather than merely responding to them.

In Summary – This guide showcases the critical advantages of modern cleanroom approaches in mitigating the risks associated with cyberattacks, which have grown in frequency and severity, affecting organizations across all sectors. Strategic approach not only helps safeguards information, but also reinforces an organization's trustworthiness and reliability in an increasingly digital world.



Commvault | PRESIDIO

Business Value of Cleanrooms/IRE

In the realm of cyber recovery, a cleanroom, or Isolated Recovery Environment (IRE), is recognized for its security and pristine condition.

Yet, the essence of a genuine and validated cleanroom concept extends beyond mere physical characteristics. It represents an all-encompassing strategy for cyber recovery that integrates a secure, autonomous environment with meticulous planning, proven processes, rigorous testing, and clear procedures.

Cleanroom Recovery offers a unique test bed to validate the effectiveness of cyber-recovery plans, technologies, and processes. It provides a secure environment where data and critical assets are isolated and safeguarded from attacks. Different from other data security offerings that have cleanroom offerings which are limited to disaster recovery and constrained by a minimal set of workloads and recovery options. Security and IT leaders can obtain valuable insights into unfamiliar threat actors, fortify their strategies, and effectively deliver uninterrupted business continuity. Commvault instills confidence with a proven approach for recovering systems and data from an encrypted source and provides clean recoveries.

As cyber threats continue to escalate, affecting not just major Fortune 500 companies but businesses of all sizes, it's essential to embrace the concept of an Isolated Recovery Environment (IRE) universally. Commvault Cleanroom Recovery makes the benefits of cleanrooms accessible to all, enhancing cyber recovery readiness and resilience without the need for costly dark site locations or elaborate infrastructure expansion.

Challenges With Ransomware Attacks

It is no longer a question of if your organization will be hit by a cyber-attack, only a matter of **when**. Why are organizations challenged with securing and recovering their IT systems? **There are many reasons, including:**

Siloed Organizations

Many companies segment IT services, which handles data recovery, from security, tasked with securing systems and preventing bad actors from accessing systems. Many threat actors exploit those gaps. **Key considerations are listed below.**

IT and Operations

- Providing system reliability and uptime
- Planning for future IT projects
- Allowing optimal use of staff time

Security

- Preventing unauthorized access to corporate systems
- Reducing risk for data exfiltration
- Minimizing insider threats

False Sense of Readiness

Many organizations believe their disaster recovery plans are adequate for a cyberattack, but during actual incidents, they find the data unreliable. This leads to prolonged recovery times as they identify the last known good copies of data, often resulting in reinfection during the recovery process.

Meeting Security and Compliance Requirements

Compliance standards are continually changing, making it challenging to keep IT systems secure and compliant. Compliance often requires labor-intensive, repetitive manual tasks, with few opportunities for automation or customization.

High Cost

Cyber vaults and similar legacy solutions typically involve costly hardware and require custom professional services that need ongoing updates, further increasing expenses.

Limitations of Traditional Approaches

Reactive to Threats

Many solutions suffer from a lack of bidirectional integration with security platforms, resulting in **slow responses to ransomware and other threats**. This delay can cause chaos and lead to prolonged downtime, which is costly for any business.

Limited Workload Support

Often, support is **restricted to just virtual machines or on-premises workloads**. This limitation hampers workload portability, making migrations difficult and costly, including the maintenance of platforms and management tools. This reliance on outdated methods increases both costs and risks.

Technical Debt

IT and security departments frequently acquire products on an ad-hoc basis to meet immediate or specific project demands. Over time, these **piecemeal, incompatible toolsets** become obstacles to adopting a unified management approach, complicating IT strategies.

Complex Manual Processes

Traditional solutions fail to provide comprehensive orchestration for on-demand recovery. As a result, customers are **forced to depend on manual, intricate, and costly testing and recovery processes**.

Insufficient Scale

Many solutions are built around an **appliance-based model that has limited scalability and requires advance planning**. This limitation restricts the speed and scope of large-scale recoveries, leading to slower recovery times and reduced effectiveness.

Susceptible to Threats

On-premises and DIY approaches to creating a cleanroom can be affected by outages caused by power, cooling, or other attacks caused during a cyber incident. Organizations typically get one chance to recover successfully with on-prem hardware, else you risk reinfecting your environment.

Top 6 Solution Requirements

Proactive Approach

SEE TROUBLE COMING AND WARD IT OFF

The solution should help you transition from reactive to proactive with **recovery readiness and testing**, which are essential to cyber resiliency. This should include:

- Any-to-any workload portability.
- Continuous, automated testing capabilities.

Increased Flexibility

LEVERAGE THE CLOUD FOR VIRTUALLY LIMITLESS SCALE

Effective recovery solutions give you options, not constraints. Look for freedom of choice in multiple dimensions, including:

- SaaS or on-premises deployment options.
- Massive scalability.
- Support for multiple use cases.
- Leveraging extensive automation capabilities.

Ease of Recovery

CLEAN BY DESIGN

Modern cloud-based cleanrooms that are **purpose built for recovery** allow organizations to test recoveries and perform failovers seamlessly. In the event of reinfection in the isolated cloud cleanroom, administrators can simply wipe it clean and start again with limited to no impact on other running production systems.

Simplified Management

BENEFITS FOR A SINGLE PANE OF GLASS

Safe, isolated environment for testing cyber recovery plans on-demand and without the risk of disrupting production systems.

- Supports your applications including, legacy, hybrid, and modern cloud native apps.
- Conduct an analysis of known infected systems and identify the root cause of an attack.
- Provide a unified, efficient, and streamlined recovery process to minimize downtime.

Get Back to Business

ACCELERATE TIME TO VALUE

Leverage a vendor with a proven track record of stability that can be a partner with your staff. Vendors should provide a **wide range of service capabilities** to support your team immediately and over time, including:

- Continuous testing to help with preparedness.
- Consulting to plan and deploy the optimal solution.
- Consulting on every aspect of implementation and success metrics.
- Training, education, and ongoing support.

Zero Trust & Immutability

ARCHITECTURE MATTERS

Separate control and data storage planes are critical for a securely designed cleanroom. This design incorporates **strong controls to defend against various threats**, including accidental deletions or malicious attacks, keeping your backup operations secure and highly recoverable. You should look for a solution that:

- Includes virtually air-gapped locations, to provide isolation of backup copies.
- Integrates bidirectionally with your security suite.
- Boosts security and the ability to test recoverability without the risk of contaminating your production data.

Delivering Clean Recoveries

For security and IT leaders whose businesses are at risk due to the complex and costly process of testing their readiness and recovering from cyberattacks, Cleanroom Recovery provides a clean, isolated recovery environment, on demand, for data availability and clean recovery.

Unlike traditional, prohibitively expensive cleanroom methods, Commvault provides simple, on-demand cleanroom recovery for testing, conducting forensic analysis, and business continuity. Put your resilience to the test. Commvault Cloud Cleanroom Recovery is the only offering that makes reliable cyber recovery testing and readiness possible for any enterprise.

Cleanroom Recovery Combines Key Capabilities

- **Commvault Cloud**, helps enable customers to seamlessly secure, manage, recover, and rebuild data across diverse environments with our game-changing cyber resilience platform.
- **Public Clouds**, bringing virtually limitless scale, speed of recovery, security, and flexibility to recover applications & workloads.

Outcomes

- **Comprehensive testing environment:** Cleanroom Recovery provides a safe and isolated environment where organizations can test their cyber recovery plans without 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 faster by providing a streamlined recovery process.
- **Reduced downtime:** Cleanroom Recovery can help organizations minimize downtime by providing a production failover solution.

KEY FEATURES

- Secure, isolated, and immutable vault backups with Commvault Air Gap Protect
- Early detection of suspicious behaviors and patterns
- Cyber analysis and data sanitization
- Automated recovery validation
- Planned, rapid recovery in the cloud

Commvault | PRESIDIO

Building Muscle Memory

Traditional methods of cyber recovery testing, like tabletop exercises, frequently fall short in fully preparing organizations for the intricate and turbulent nature of actual cyber recovery situations. While tabletop exercises provide valuable insight into cyber recovery planning, they often fall short in fully simulating the complex and unpredictable dynamics of real-world cyber incidents.

Testing cyber recovery plans in hybrid environments is often a lengthy, complicated, and costly process. With workloads distributed across various clouds, on-premises hypervisors, and physical servers, it is necessary for organizations to conduct tests within each distinct environment. Achieving true cyber resilience goes beyond merely reaching a technological benchmark; it also requires a deep understanding of its significance in fostering genuine resilience.

The effort to achieve cyber resilience is as crucial from a business perspective as it is from a technological standpoint. Historically, IT domains functioned independently, but achieving robust cyber resilience necessitates a collaborative approach between technology teams and business units. It is essential for senior executives to lead the charge in fostering a cybersecurity-aware culture and implementing best practices that facilitate swift recovery.

Enterprises need a safe and isolated environment where organizations can test their cyber recovery plans without the risk of disrupting production systems.

Continuous Enhancements Add New Value

Commvault Cloud Cleanroom Recovery adds new capabilities, updates, and upgrades to Commvault Cloud.
Key enhancements are summarized below:

Feature	Business Value/Benefit
Cleanroom Recovery for SaaS	SaaS customers can be recovery-ready by conducting cyber recovery testing
Cleanroom Recovery of SQL, DB2, and Oracle DB (using VM backups)	SQL, DB2, and Oracle databases running on VMs can be recovered to VMs in the cleanroom
Automatic scaling of Commvault Cloud services	Improved scalability during a recovery
Validate and Recovery Active Directory	Cleanroom Recovery support for Active Directory streamlines the entire recovery and recovery validation process
Pave + Repave +VMs from a template for clean point recovery	Rebuild corrupt or infected applications / data from a the last know clean point
Automate clean recovery points using Palo Alto XSOAR integration	Enables customers to investigate security incidents by utilizing XSOAR to enrich incidents with the latest threat intelligence data, streamlining the recovery of compromised assets into a cleanroom for forensic analysis and rapid, secure cyber recovery

> "Cleanroom Recovery is a game-changer for Commvault Cloud. It enables **comprehensive testing and retesting on the fly**, which traditional cleanroom solutions don't provide. It also is designed to help organizations rapidly recover from a cyber incident. The level of confidence and security this innovative solution can provide is invaluable."
>
> Michelle Buschman
> CIO, American Pacific Mortgage

Cleanroom Use Cases

A cleanroom environment, also known as an "isolated recovery environment" or "sandbox," plays a crucial role in cyber recovery strategies by providing a cost-effective and flexible place for testing, as well as a safe and secure space to analyze, restore, and remediate systems affected by cyberattacks. **Here are some key use cases for a cleanroom in cyber recovery:**

Continuous Cyber Recovery Plan Testing

- Organizations can use the cleanroom to simulate cyberattacks and test their 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 completely compromised environments, a cleanroom allows 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.

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.

"We are excited about the advent of Cleanroom technology in our services. This approach allows us to **test our recoverability and create a meticulous checklist for system recovery**, utilizing a fully segmented Cleanroom to restore critical infrastructure rapidly."

Kevin Cronin
CEO Co-Founder, Kelyn Technologies US

5x lower OPEX

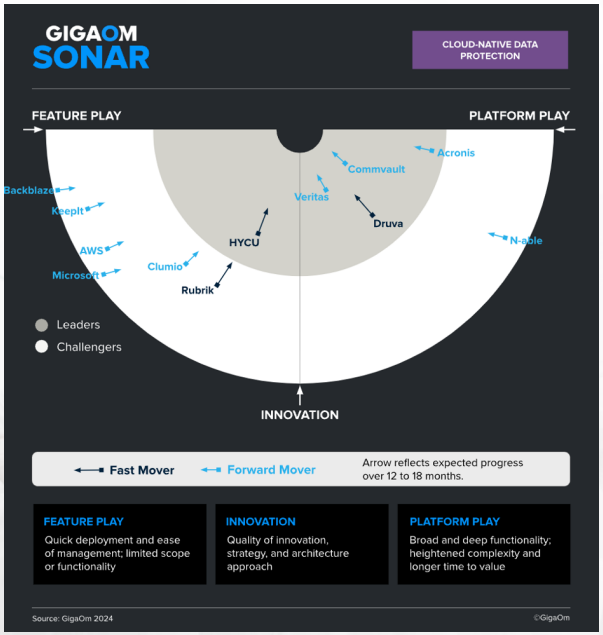
compared to DIY estimate

Commvault | PRESIDIO

SUMMARY

Commvault® Cloud Cleanroom™ Recovery

WHERE THE BEST GO TO TEST.



GigaOm Sonar Report

A GigaOm Sonar report analyzes emerging technology trends and sectors, providing decision-makers with the information they need to build forward-looking, rewarding IT strategies. Sonar reports provide an analysis of the risks posed by the adoption of products that are not yet fully validated by the market or available from established players.

In exploring bleeding-edge technology and addressing market segments still lacking clear categorization, Sonar reports aim to eliminate hype, educate about technology, and equip readers with insight that allows them to navigate different product implementations. The analysis highlights core technologies, use cases, and differentiating features, rather than drawing feature comparisons. This approach is taken mostly because the overlap among solutions in nascent technology sectors can be minimal. In fact, product implementations based on the same core technology tend to take unique approaches and focus on narrow use cases.

"A notable feature of Commvault Cloud Platform is its Cleanroom Recovery technology and Air Gap Protect, which pairs immutable SaaS storage with access to a Commvault-managed Azure tenant for business continuity. **This technology creates a secure, isolated environment for cyber recovery testing, forensic analysis, and data recovery**, automating the recovery process and ensuring quick, secure recovery from cyber incidents without reinfection. The ability to automate and prioritize recovery workflows, including restoring accounts, permissions, and credentials, enhances the platform's resilience and operational efficiency."

Source: GigaOm Sonar for Cloud-Native Data Protection v2.0 by Chester Conforte

August 7, 2024

Preparing for the inevitable need not be a daunting task.

Today, there are smarter, more straightforward solutions that transcend the constraints of traditional methods, enhancing your security measures effectively.

Commvault® Cloud Cleanroom™ Recovery equips your organization to effortlessly test and recover from threats on a large scale. This enables your IT and security teams to protect vital resources efficiently, confidently, and economically, benefiting your entire organization.

- ☐ Does the cleanroom support all of our workloads (Virtual, physical, cloud, etc...)?
- ☐ Is the cleanroom physically isolated from my existing infrastructure (network, location, power, cooling, etc...)?
- ☐ Does the cleanroom have limited admin access, physically and/or remotely for people to access?
- ☐ Can the cleanroom offer bi-directional integration with existing security platforms?
- ☐ Does it offer built-in threat hunting & malware scanning?
- ☐ Can I perform multiple regular testing scenarios in the cleanroom?
- ☐ In the case of reinfection in the cleanroom, can you easily rebuild a new instance of a cleanroom?
- ☐ Does the cleanroom solution fit into our budget?

If the answer is yes to all of these, you must be looking at Commvault Cloud Cleanroom Recovery.

To learn more about Commvault Cloud or for detailed specifications and system requirements, contact us today or visit www.commvault.com.

To learn more about Cleanroom Recovery Performance & TCO Analysis refer here.

Commvault®

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