SALES PLAYBOOK

Cleanroom Recovery

Deliver total resilience with Commvault Cloud

Commvault

Table of Contents

Account Targeting

IDEAL ACCOUNTS TO TARGET

Goal: Develop an understanding of the characteristics of ideal accounts to target, things to look for, discovery questions to qualify an opportunity in or out, etc.

Midsize and Enterprise organizations (44-65% cloud workloads)

Organizations with a technology environment that includes:

- Air Gap Protect, over 50 TB, or planning to buy soon
- Workloads focused on VMs

Regulated industries, industries with sensitive data:

- Technology
- IT Services
- Finance & Insurance
- Healthcare
- Government

Adhere to best practices around NIST, DORA

QUALIFYING A CLEANROOM RECOVERY OPPORTUNITY

What to ask	What does it tell you	What to do next
Do you have a tertiary, immutable, air-gapped copy of your data?	In addition to being a pre-requisite for Cleanroom Recovery, this will tell you how mature they are from a backup & recovery perspective.	If they are not doing this, note that it's an Air Gap Protect opportunity.
Describe your target cyber recovery environments. Are they different than recovery environments used for operational and disaster recovery?	You want to learn how well-defined their target recovery environments are for cyber recovery — and if they treat it differently than operational and disaster recovery.	Find out if they plan on using the recovery environments for production recovery, forensics, and testing.
Does your incident response plan include testing for operational recovery? Disaster recovery? Cyber recovery?	This helps you determine if they have an incident response plan and if it's documented. It also gives you a sense of how mature their approach to recovery is.	Dig deeper into the differences between the plans, incredibly how confident they are in each.
Do you have established RTOs and RPOs?	This tells you how they think about recovery and gives you a sense of how fast/capable they are of recovering.	If they have established RTOs/ RPOs, find out who they share this with to determine the broad expectations. Do they share only within IT? With the business? Officers of the company?
Have you established any expectations on the recovery process and timing with the business for recovering from cyber incidents?	You want to find out if they use their RTOs and RPOs for cyber recovery too? If so, they may not be particularly mature in cyber recovery.	If they use RTOs/RPOs for cyber recovery, are they the same as for DR? How do they account for the unpredictability of a cyber attack?
How often do you test your cyber recovery plan? If you test, how do you test?	You want to determine how prepared they are for a cyberattack. And by "how," you want to know if they review a checklist or perform some simulation (like a tabletop exercise) or if they test — i.e., they perform a full recovery from backup. It is essential to determine which methods they use to set up Commvault's offering properly.	If they perform some simulation or test, determine how broad it is. Who is included? How much of their estate is covered? Do they tier applications into critical apps and test those differently/ more frequently than non-critical ones?
Do they follow frameworks (e.g., NIST) or legislation (e.g., DORA) that guides their cyber recovery requirements or practices?	You want to learn what drives their readiness. Fear? Striving for operational excellence? Audit requirements?	Explain how we can help them abide by the DORA risk assessment framework and adhere to NIST recommendations on testing of recovery plans.

Buyer Personas

ENTERPRISE DECISION-MAKING PROCESS

Commvault Customer Personas →

"Cyber attacks are increasing. What's your Cyber Response strategy?"

CEO ← **BoD**

"I promised the board we would complete and test our Cyber Response Strategy by xx date. Go figure that out."

CISO

"Go figure out how to complete and test our Cyber Response Strategy by XX date. And do it without impacting business operations and incurring additional cost."

ITDM

"I've been looking at how we can create and maintain a cohesive and reliable cyber recovery practice. Go validate problems and take a look at some solutions."

TECHNICAL MANAGER

BUYER PROFILES

Persona	Common Titles	Role in buying process	What they care about
Primary: Security Chief	• Chief Information Security Officer (CISO) • Director of Global Information Security • VP of Information and Cybersecurity	• The level of involvement can vary, with some spearheading the recovery readiness solution evaluation. • Others play a more consultative role and evaluate solutions from a cybersecurity perspective. • Typically, stakeholders and/or final decision-makers in these decisions. • They lead their department and create data security and retention policies, while the Head of Infrastructure implements and oversees the cyber recovery solutions.	• Concerned with protecting data from cybersecurity threats with zero trust principles. • See data protection as being resilient, securing and controlling access to data, ensuring data is protected at rest, in transit, and rapidly recoverable. And creating a virtual or real airgap. • Security Chiefs in EMEA also view data protection as related to data privacy and compliance, such as ensuring compliance with GDPR.
Secondary: ITDM	• Chief Information Officer (CIO) • Chief Information Technology Officer (CITO) • Chief Technology Officer (CTO) • VP of Cloud • VP of Cloud Infrastructure	• Typically involved in the final decision when evaluating recovery readiness solutions. • May be involved in evaluations or POCs (esp. SMB) • Usually, one of the executive sponsors for all data backup and recovery-related projects. Sometimes, the executive sponsor may be the Security Chief instead of the Technology Leader. • Less involved in daily oversight of recovery readiness solutions than the Head of Infrastructure.	• View data protection as a robust set of policies and strategies encompassing data governance. • Think about TCO, ease of backing up, and rapid recovery • Concerned with data security and ensuring consolidated solutions are in place, leveraging AI-driven technologies to prevent data loss, capturing the right type of data, proactively protecting the data from cybersecurity threats, and ensuring compliance with regulations like GDPR.

Commvault

PROBLEM IDENTIFICATION

CISO	ITDM	Technical Manager
The Decision Maker	The Driver	The Influencer

SOLUTION EXPLORATION

“People like me... Companies like us”	“Cross-functional challenges”	“Day in my life”	“WHAT exactly do you do... HOW does it work?”

REQUIREMENTS BUILDING

POC	**Feature List**	**Top of mind** “Problems I see”

SUPPLIER SELECTION

Business Transformation	**Solution**	**Tool**

POST-PURCHASE

“Make our business successful”	“Make my team successful”	“Make me successful”

Market Landscape

THE WORLD HAS CHANGED

Ransomware everywhere — including the backup

99%

99% of ransomware tampers with security and backup infrastructure

Breaches are becoming the norm

66%

66% of organizations surveyed were breached in 2023

Average time to recover is devastating

24

24 days is the average reported time to recover from a cyberattack

CURRENT RECOVERY READINESS APPROACHES FALL SHORT

Recovery testing is expensive and complex

Building out physical or virtual recovery environments with all the required infrastructure to test critical application recovery is untenable for most.

Delta between plans and readiness is massive

Many organizations have cyber response plans, but cannot reliably test cyber recovery readiness.

Organizations rely on DR plans, checklists, or simulations

Because testing cyber recovery plans is complex and expensive, most rely on simulations, tabletop exercises, and checklists.

NEW THREAT LANDSCAPE DEMANDS TOTAL RESILIENCE

Due to a lack of testing, many organizations are unaware of the gaps in their cyber recovery plans. As cyber-attacks become more pervasive and sophisticated, it's critical to have a robust, adaptable approach to true resilience.

- Cybersecurity breaches are inevitable
- Ransomware attacks backup environments, too
- People confuse cyber testing with disaster recovery
- Recovery readiness is critical to cyber recovery

Commvault can help reliably recover clean applications into a cleanroom, especially for:

- Recovery testing
- Performing forensic analysis
- Production failover

Sales Messaging

CLEANROOM RECOVERY POSITIONING

POSITIONING	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, we provide simple, on-demand cleanroom recovery for testing, conducting forensic analysis, and business continuity.
VALUE PROP	Cleanroom recovery is no longer an ideal reserved just for the largest F500 companies — Commvault is democratizing cleanrooms. With Commvault's unique offering, any enterprise can have cyber recovery readiness and resilience without the cost of dark site locations and complex infrastructure proliferation.
THE HOOK	**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.

Messaging Pillars		
Simple Readiness within reach, for any organization	**Secure** Clean recovery. Clean locations. Isolated testing	**Intelligent** AI-enhanced for reliable testing
Evidence for Pillar 1 • On-demand cleanroom avoids costly, dedicated infrastructure. • Broad workload support avoids managing duplicate environments for every critical application across every location. • Built-in automation simplifies critical but complex workflows like Active Directory recovery.	**Evidence for Pillar 2** • On-demand cleanroom provides a clean, secure, and isolated environment. • Built-in integrations with MSFT Defender for threat scanning and Palo Alto XSOAR for forensics. • Modern pave/re-pave automation which rapidly restores clean application images from a pre-approved, secure location.	**Evidence for Pillar 3** • New integration with Palo Alto XSOAR2 to automatically look for suspicious patterns and unusual events and pinpoint vulnerabilities • Intelligent and automated Cleanpoint™ Validation includes AI-driven orchestration and post-validation for more efficient and reliable recovery. • Organizations can optimize cloud costs with intelligently scaled application group recovery.

CLEANROOM RECOVERY QUICK PITCH

One-liner: Cleanroom Recovery is designed for cyber recovery with the rapid and reliable recovery of applications into a secure, on-demand cleanroom.

FOR	security and IT decision-makers responsible for cyber recovery
WHOSE	businesses are at risk due to the complex and costly process of testing and recovery from cyber attacks
AND WANT	the ability to continually test cyber response plans so when it matters most, they are ready to go and can experience rapid, frictionless, and reliable recovery
Commvault Cloud Cleanroom Recovery	
IS	a revolutionary offering to help deliver cyber recovery readiness and resilience
THAT	provides an affordable, clean, secure, isolated recovery environment for testing cyber recovery plans, conducting secure forensic analysis, and helping deliver uninterrupted business continuity
UNLIKE	• **traditional cleanroom methods**, which are too expensive and complex for most organizations • **other data security solutions** with cleanroom offerings that are limited to disaster recovery and are constrained by a very limited set of workloads and recovery options
ONLY COMMVAULT	offers the ability to recover workloads from ANY location to a safe, cloud-isolated cleanroom for the strongest and most reliable cyber recovery and readiness

TALKING POINTS — BY AUDIENCE

CISO	Demonstrate readiness to company officers that adhere to best practices around NIST, DORA, and any other relevant compliance regulations. With comprehensive testing and the ability to perform forensic analysis, business leaders can stay compliant and secure to meet the demands of the evolving hybrid world.
ITDM	They have the same key messages as the CISO but also want to feel confident without building or creating their own cleanroom. Cleanroom Recovery delivers comprehensive testing, the ability to perform secure forensic analysis, and production failover. To stay resilient, ITDM's need a safe and isolated environment for: • Testing cyber recovery plans • Conducting forensic analysis • Delivering business continuity in the event of a breach, all of which are provided by Cleanroom Recovery
Existing Customers (land/expand)	In the face of constant breaches, testing your cyber recovery plan is crucial for success. Ransomware attacks targeting backup environments pose a significant risk during recovery. Enter Commvault Cloud's revolutionary Cleanroom Recovery. This game-changing solution allows organizations to confidently test cyber-resilient recovery plans, conduct secure forensic analysis, and have uninterrupted business continuity. Experience reliable, faster recovery times, reduced downtime, and a streamlined process.
Partners	Cleanroom Recovery empowers partners to initiate meaningful conversations with customers regarding their cyber recovery strategy. By offering Cleanroom Recovery as a solution, partners can position themselves as trusted advisors, sell additional services and networking solutions, and bring all Cleanroom Recovery data back on-premises. Partners can also seize the opportunity to establish Cleanroom Recovery as the new data center, providing a comprehensive and secure environment for customers' critical data. With Cleanroom Recovery, partners can unlock new avenues for growth and strengthen their position as strategic partners in cyber recovery.

TALKING POINTS – NIST & DORA

NIST recommends regular testing for recovery plans

- Empower customers to adhere to NIST recommendations on testing of recovery plans

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recovery
Security is blind to unknowns.			Recovery readiness and testing enable the business to be **cyber resilient**.	

DORA Risk Framework

- Enable customers to abide by the DORA risk assessment framework

Risk Management

Business continuity and disaster recovery plans a must

Incident Reporting

Cybersecurity and reporting processes a requirement

Digital Operational Resiliency Testing

Annually including remediation plans

ICT Third-party Risk

ICT third-parties subject to EU oversight

Information & Intelligence Sharing

Encouraged to share threat information and intelligence

CLEANROOM RECOVERY USE CASES

Cyber Recovery Readiness & testing
Provide a safe and isolated environment where organizations can test cyber recovery plans on-demand and without the risk of disrupting production systems.

Forensic Investigation & Analysis
Cleanroom Recovery can be used to conduct forensic analysis of known infected systems and identify the root cause of an attack.

Production Failover for Business Continuity
Recover from cyberattacks faster with a streamlined recovery process and minimize downtime with a production failover solution.

Rapid, reliable application recovery into a secure, on-demand cleanroom

CLEANROOM RECOVERY CAPABILITIES

Features

- Automated recovery workflows (from initial clean point validation to final verification).
- AI-enhanced cloud scaling for mass recovery.
- Any-to-any portability to enable recovery from diverse environments to a common environment.

Current CRR version supports

- VMware Solutions: VMware, VMware on AWS, VMware on Oracle, VMware on Azure.
- Hyper-V, Azure VMs, and AWS EC2.

Strengths

Take VM data and recover it dynamically to an isolated cloud testing environment.

- No other platform can take diverse workloads to a cleanroom in the cloud.
- We are the only solution to do anomaly detection-based machines in flight and after the backup.
- We're the only platform with pre-, during, and post-detection.
- We can dynamically convert source data to the target, allowing us to facilitate cost-effective cyber recovery testing.
- We not only help with recovering in the event of an attack, but we also enable the ability to test and go through the exercises so you can regularly test to understand the state of your cyber recovery plan.
- We go beyond immutable cloud storage and offer the cleanroom recovery process that automates recovery into a cleanroom.

CLEANROOM RECOVERY FEATURES

1H 2024

Feature	Value
Cleanroom validation and recovery as a SaaS service for software customers.	End to end automated cyber recovery solution for software customers.
Microsoft Defender to scan data in the Cleanroom during cyber recovery/validation.	Data validation and sanitization leveraging trusted malware scanning tools.
SaaS service delivery automation through SRE.	Self service automation for customers.
Auto scale of access nodes for recovery group operations.	Automated recovery at scale and across regions while optimizing recovery costs.
Integrate Cleanroom Recovery with XSOAR (Palo Alto).	Automatic discovery of compromised assets and timeline for cyber recovery or forensic analysis.
Cleanroom Recovery for MSSQL (VM recovery + post recovery scripts).	Validated recovery of databases.

2H 2024

Feature	Value
Cleanroom Recovery for AD servers (single domain controller).	Validated recovery of AD domain controllers.
Deliver Cleanroom Recovery for SaaS tenants.	Cyber Recovery solution for SaaS customers.
Cleanroom Recovery for physical servers.	Cyber recovery for hybrid workloads.
Cyber Resiliency dashboard.	Central index and dashboard to monitor cyber resiliency.
Integrate Threat Scan into Cleanroom Recovery.	AI enabled intelligence for scanning threats in virtual machines.
Integrate Agentless Defender into recovery validation.	Advanced cloud native security tools for Cleanroom validation and sanitization.
Predict recovery times to measure RTO.	Better incident response planning through predictive RTO.
Extend Cleanroom Recovery to support HSX and VMware as recovery target.	Cleanroom for critical on-prem workloads.

CLEANROOM RECOVERY IS AI-ENHANCED

By combining powerful AI techniques with smooth integration capabilities, our AI-enhanced solution empowers organizations to leverage the power of AI to solve real-world problems and achieve significant business benefits.

- **Plug-and-play Ready:** They can be easily deployed and connected to a company's existing network without requiring major modifications or overhauls. This allows for quicker adoption and reduces implementation costs.
- **Security-Focused:** Enterprise-grade AI prioritizes data security and adheres to strict compliance standards to provide safe handling of sensitive information within the organization's network.
- **Scalable:** These AI solutions can handle large volumes of data and adapt to the growing needs of the business.

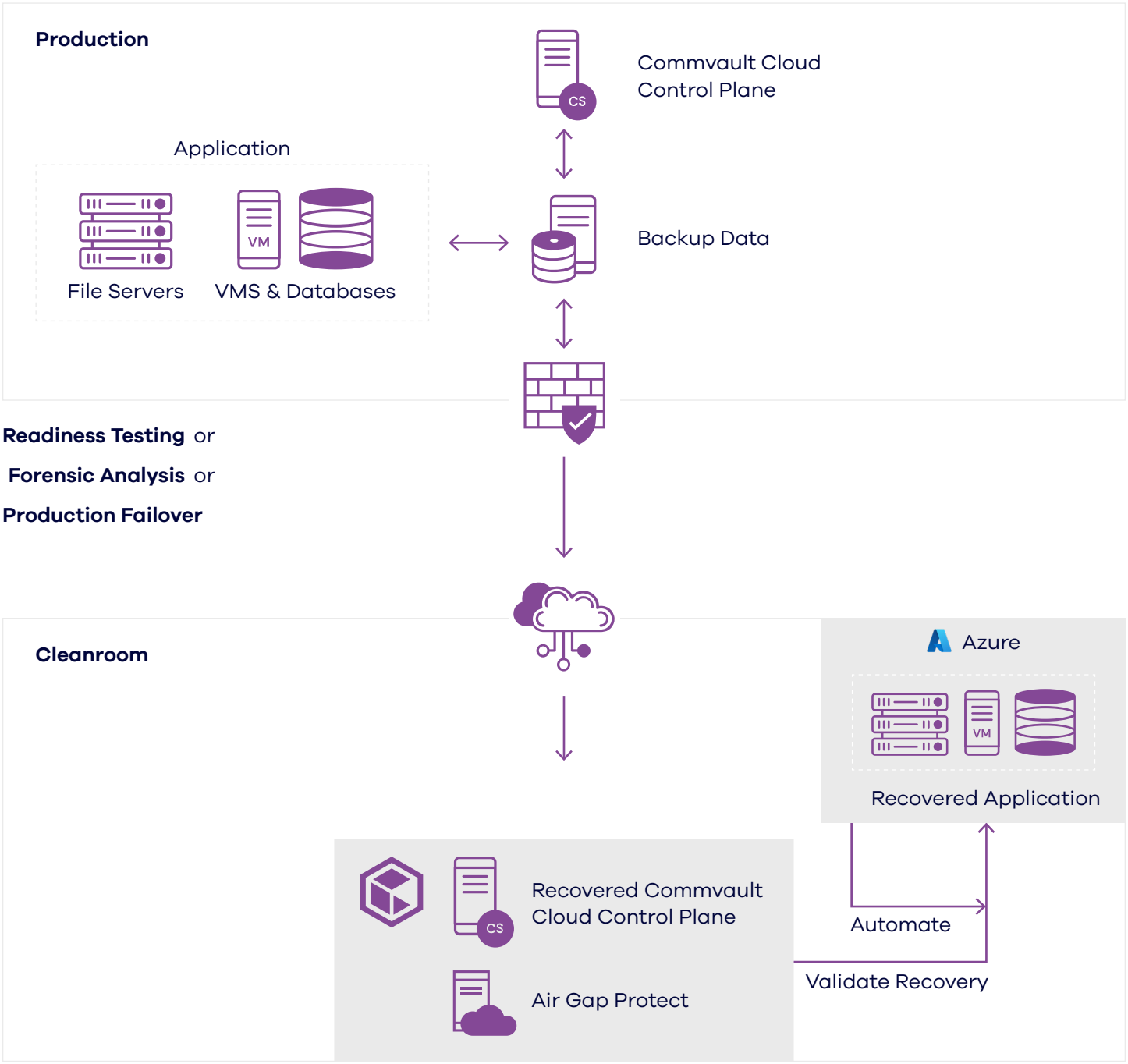
Cleanroom Recovery Benefits

- Reduce the complexity and time required for recovery operations with an automated, efficient process for restoring critical systems
- Gain peace of mind by minimizing the risk of malware reinfection and data breaches, leveraging a recovery process powered by a solution designed to address sophisticated cyber threats.
- Discover gaps in your recovery plan and strengthen your resilience and readiness with regular recovery plan testing.
- Reduce recovery times and avoid operational downtime to minimize the financial impact of disasters.
- Gain potential cost savings through intelligent resource allocation and downsizing recommendations.

What makes Cleanroom Recovery unique

- Any-to-any portability to recover workloads from anywhere to anywhere. Traditionally, apps and data from various systems would require duplicating all environments to rest and recover.
- Able to leverage a flexible dissimilar Cleanroom target, reducing cost and complexity. Pay for what you need when you need it.
- We start off a cleanroom recovery with a read-only control plane. Even if the production environment is compromised, the cleanroom environment can not be accessed.
- Automated hooks into AI/ML to assist in deciding known good recovery point.

HOW CLEANROOM RECOVERY WORKS



THE DEMO

DELIVERING TOTAL RESILIENCE WITH COMMVAULT CLOUD

OPERATIONAL RECOVERY

Challenge:

Operational recovery to support business operations, accidental deletions, unexpected data corruption, etc.

Solution:

Commvault Cloud Backup & Recovery is the most advanced and intelligent data recovery platform.

- Comprehensive data protection support
- Convert data to destination format at run time
- Scale up services to boost recovery time objectives
- Scale down services when not in use
- Privacy controls to control access to data

DISASTER RECOVERY

Challenge:

Disaster recovery for business continuity and site recovery upon natural disasters or outage.

Solution:

Commvault Cloud Auto Recovery is the most flexible and cost-efficient data replication platform.

- Sub-minute RPO capabilities
- Near-zero RTO recovering data instantly
- Transform data during replication
- Simple orchestration production to DR, and vice versa.
- DR Fire drills for recovery readiness validation

CYBER RECOVERY

Challenge:

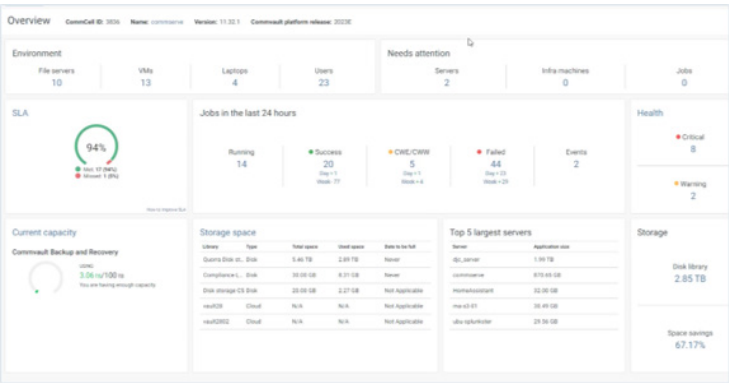
Cyber recovery to recover data and malware-affected applications after a cyber incident.

Solution:

Commvault Cloud Cleanroom Recovery for a simple, secure, and rapid recovery of applications.

- Establish and automate cleanrooms for recovery
- Logical grouping of heterogeneous workloads
- Secure scanning with built-in and customizable tools
- Recovery dependency and custom actions
- Commvault control plane accessible in clean site
- Recovery-centric monitoring, reporting, auditing

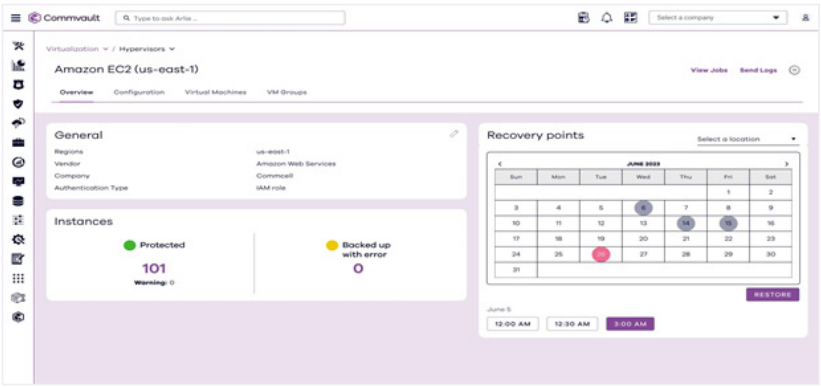
FOR TOTAL CYBER RECOVERY, ALSO CONSIDER...



OPERATIONAL RECOVERY

Commvault Cloud Backup & Recovery

- Role-based access control for self-service while restricting unauthorized access
- Eliminate data sprawl and reduce the burden on database administrators
- Increase efficiency and allow focus on critical business activities
- Extract more business value from data to facilitate business planning and improve business outcomes



DISASTER RECOVERY

Commvault Cloud Auto Recovery

- Secure cyber threat recovery across your entire data landscape
- Execute proven recovery readiness in the event of a ransomware incident
- Reduce recovery time with sub-minute RPOs and near-zero RTOs
- Facilitate cost-effective cloud data mobility

Sales Play

CLEANROOM RECOVERY FAST START SPIFF!

Supercharge your earnings!

Close the first 100 opportunities and earn:

- **4x BCR:** Opportunities 1-25
- **3x BCR:** Opportunities 26-50
- **2x BCR:** Opportunities 51-100

Who is eligible?

- Account Executives
- Sales Engineers
- Partner Business Managers
- 1st and 2nd Line Managers in Sales, Sales Engineering, and Channel organizations

Duration

- Runs through the earlier of June 30, 2024 or the first 100 closed Clean Room Recovery opportunities.

Terms and Conditions:

- Stacking SPIFFs and accelerators is prohibited
- GSI, Alliance, and Hyperscalers roles: Max payout is 2x BCR
- New and existing customers are eligible
- All VAR, Alliance, and GSI sales channels are eligible
- Payouts based solely on Cleanroom Recovery SKU ACV
- Deal Desk and Sales Ops approval required
- Only locations offering Air Gap Protect are eligible
- MSPs are ineligible as a route-to-market
- Sell-through opportunities prohibited
- Contractors are ineligible for SPIFF payout
- C-suite reserves the right to adjust eligibility and payout for any opportunity

PROBLEM IDENTIFICATION

Learn the basics. Identify trends and thought leaders.

- Conduct a discovery call to understand goals and objectives. Understand how they manage incident response planning today and whether certain frameworks they adhere to exist. (NIST, DORA)
- Qualify in or out based on meeting the targeting criteria outlined in Ideal Accounts to Target.
- Understand who is part of the buying group.

Recommended next steps:

- A deeper analysis of the current environment, challenges, and objectives.
- Loop additional stakeholders into the conversation.

Resources:

- **IDC:** The Cyber-Resilient Organization
- **Gartner:** 2023 Magic Quadrant and Critical Capabilities Report
- **ESG:** The Economics of Cyber Recovery
- **Guide:** The Ransomware Solution Your CISO Will Love

SOLUTION EXPLORATION

Identify the benefits of solving the problem. Understand how others are doing it.

- Dig into pains and challenges experienced (sales messaging).
- Map implications of pain/challenges to critical issues.
- Identify key use cases – cyber recovery readiness & testing, forensic investigation & analysis, and production failover for business continuity.
- Describe traditional approaches companies have taken to solve these challenges and why they fall short.
- Proactively set competitive land mines and traps to help guide preference for Cleanroom Recovery.

Recommended next steps:

- Map Cleanroom Recovery capabilities with goals, needs, and desired use cases.
- Overview and demo of Cleanroom Recovery mapped to desired use cases.

Resources:

- **eBook:** Understanding Team Roles and Responsibilities
- **Webinar:** Ensure Business Continuity with Cleanroom Recovery
- **Sales Deck:** Cleanroom Recovery

1 Problem Identification

2 Solution Exploration

3 Requirements Building

4 Supplier Selection

REQUIREMENTS BUILDING

Evaluate vendors. Explore key features and functionality.

- Pull in a Sales Engineer to help drive conversations.
- Reiterate understanding of the customer's environment, goals, key challenges, ideal state, and desired use cases.
- Demo how Cleanroom Recovery can achieve desired use cases and address key challenges.
- Share a project timeline for the solution that is mutually agreed upon.
- Share solution briefs to help sell internally where necessary.

Recommended next steps:

- Develop a proposal to show how Cleanroom Recovery fits within the customer's environment.
- Analyze the TCO & ROI.

Resources:

- **Buyers Guide:** Aligning Ransomware Protection and Recovery with Critical Capabilities
- **Solution Brief:** Cleanroom Recovery
- **Solution Brief:** Air Gap Protect

1 Problem Identification

2 Solution Exploration

3 Requirements Building

4 Supplier Selection

SUPPLIER SELECTION

Pitch to your team and make a selection.

- Determine what is needed to prove economic and technical value.
- Review the implementation process based on desired use cases.

Recommended next steps:

- Secure approvals from decision makers and stakeholders.
- Develop a success plan for implementation.
- Share best practices.

Resources:

- **Guide:** Essential Guide to Cleanroom Recovery

1 Problem Identification

2 Solution Exploration

3 Requirements Building

4 Supplier Selection

The Competition

COMPETITIVE OVERVIEW

Centered around recovery, rather than testing

Many competitors are focused on recovering quicker and faster. In reality, they need to focus on the attack and have a clean location to recover to.

Commvault looks at the issue of ransomware end to end, not just the part of the process that recovers data. Many say, "We can recover into a cleanroom," which differs from end-to-end orchestration. No matter the source environment, we can recover it in your target cleanroom destination (any-to-any).

- We're the only vendor doing any-to-any portability.
- VMware and AWS, Azure solutions as well as any Azure VMs.

CLAIMS VS. REALITY

Competitor	Competitive Approach	Reality
Rubrik	You can recover within 24 hours.	Rubrik is aggressive with cyber recovery and data security and will say they can do the same thing as Commvault with a cleanroom. Rubrik requires a cloud cluster to facilitate its limited cross-platform restores. Their any-to-any cross-platform support matrix is far more limited than Commvault's supported matrix. Also, look for their cloud clusters to change soon as the cost and complexity of running them are prohibitive.
Cohesity	Claiming AI/ML for Zero trust, Recovery at scale, singular platform.	Focus on Fort Knox, which is equivalent to our Air Gap Protect. While they have limited capabilities beyond Fort Knox, these are not discussed, with many relying on third-party applications. Additionally, the recent announcement of their intent to acquire parts of Veritas calls into question their cloud readiness.
Veeam	"Radical resilience", recovery to anywhere from anywhere — Zero data loss.	Veeam will say they are hyper-resilient. The reality is that they offload all aspects of security onto the client. They still "require" Active Directory integration and still suffer from frequent high-profile exploits. Veeam has developed services to help clients accomplish this, but it is a new offering and a paid engagement. Additionally, leveraging service providers is necessary for Veeam to provide the same experience we can with running the Control Plane in the Commvault Cloud.
Dell	Dual offering — Cyber Recovery vault (specially replicating to PPDD), CyberSense (index engines) works with CRV but scans the environment.	Dell will lead with Cybervault coupled with CyberSense. At the surface, this is a compelling technology but does not have the same any-to-any capability we have and is built heavily on Data Domain. This is a high-cost/high-complexity solution built on Data Domains and third-party software. Due to the cost and complexity, Dell only recommends that 10% of a client's environment resides in the Cybervault.

Pricing & Packaging

PRICING & PACKAGING OVERVIEW

Packaging	Cleanroom Recovery is currently packaged as a standalone add-on, similar to Air Gap Protect. We are evaluating models that include it in a packaged offering, like Cyber Recovery.
Pricing	Cleanroom Recovery is sold in increments of 10TB. The 10TB measurement is based on the amount of data the customer configures into a Recovery Group, which is based on front-end terabytes. For example, suppose the customer configures 100TB of data into the recovery groups (based on the data size at the time of configuration). In that case, they must purchase ten units of the CV-CLNRM-10TB SKU units. If the client needs to configure 104TB of data, they must purchase 11 units of the CV-CLNRM-10TB SKU. • CV-CLNRM-10TB Commvault Cloud Cleanroom Recovery, $1,590 USD It's important to note that if a customer configures a recovery group within their licensed limits and the data set grows to exceed what they have purchased, they will be notified of the overage. In such cases, no further systems or data can be added to the recovery groups until the license overage is remedied.
Prerequisites	• Cleanroom Recovery SKU • Air Gap Protect • Backup & Recovery (from any of the packages) • Any of the Commvault Cloud tiers (i.e., Operational Recovery, Autonomous Recovery, Cyber Recovery, Platinum Resilience)

Additional Resources

TOOLS TO HELP YOU SELL

	Problem Identification Learn the basics. Identify trends and thought leaders.	**Solution Exploration** Identify the benefits of solving the problem. Understand how others are doing it.	**Requirements Building** Evaluate vendors. Explore key features and functionality.	**Supplier Selection** Pitch to your team and make a selection.
CISO The Decision Maker **ITDM** The Driver **Technical Manager** The Influencer	**External** • **IDC:** The Cyber-Resilient Organization • **Gartner:** 2023 Magic Quadrant and Critical Capabilities Report • **ESG:** The Economics of Cyber Recovery • **Guide:** The Ransomware Solution Your CISO Will Love • **Blog:** DORA Compliance	**External** • **Webinar:** Ensure Business Continuity with Cleanroom Recovery • **Sales deck:** Cleanroom Recovery • **eBook:** Understanding Team Roles and Responsibilities • **Blog:** Why Cleanroom Recovery and Cyber Testing are Critical for Cyber Recovery • **Blog:** How Cleanroom Recovery Helps Ensure Business Continuity	**External** • **Buyers Guide:** Aligning Ransomware Protection and Recovery with Critical Capabilities **Solution Brief/ Datasheet** • Cleanroom Recovery • Air Gap Protect • Backup & Recovery • **Video:** Cleanroom Recovery explainer • **Demo**	**External** • TCO Calculator • Customer references • Sales Proposal

QUESTIONS

For questions regarding marketing materials, please reach out to PartnerCampaigns@commvault.com.

Place partner contact info here
and delete this text box