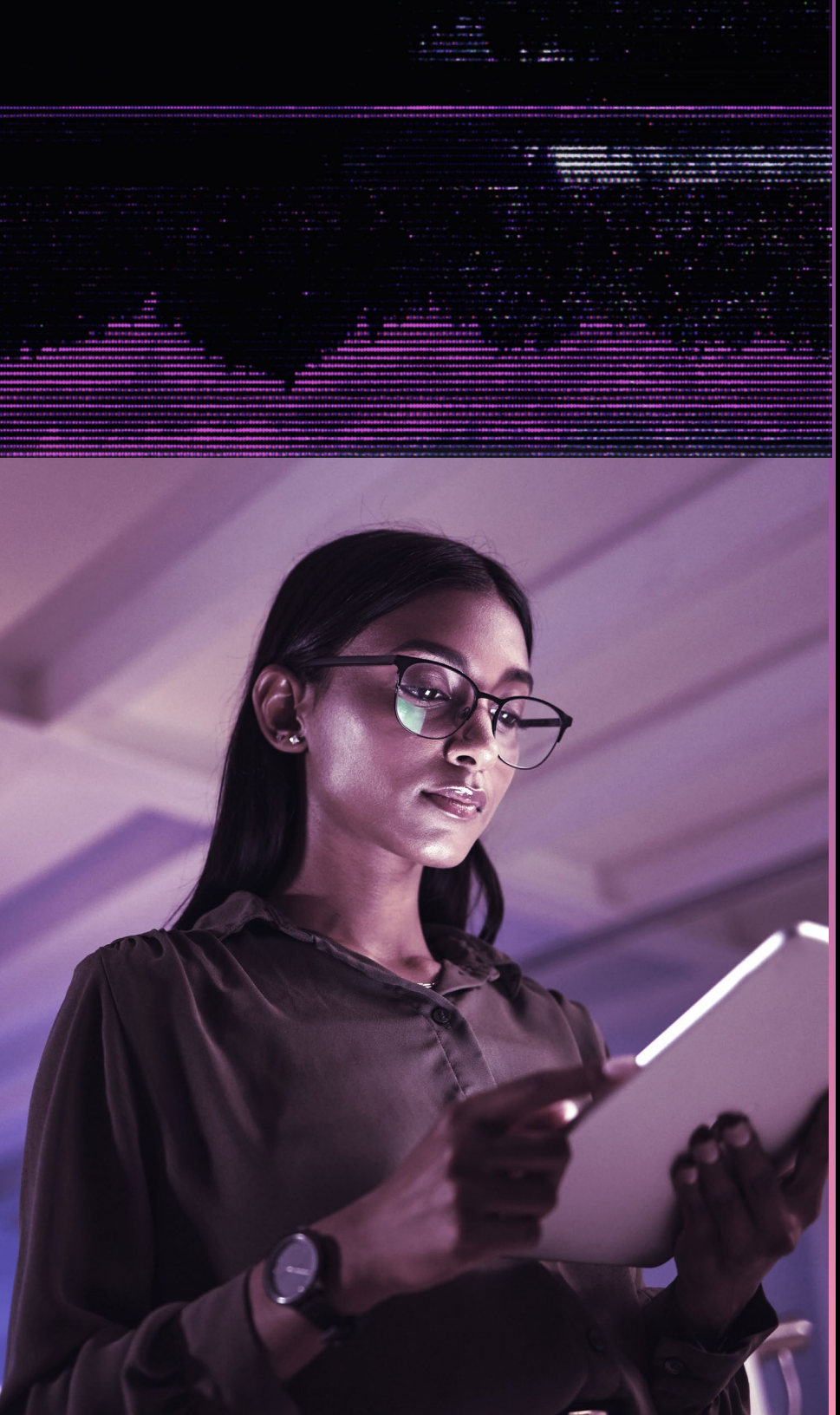


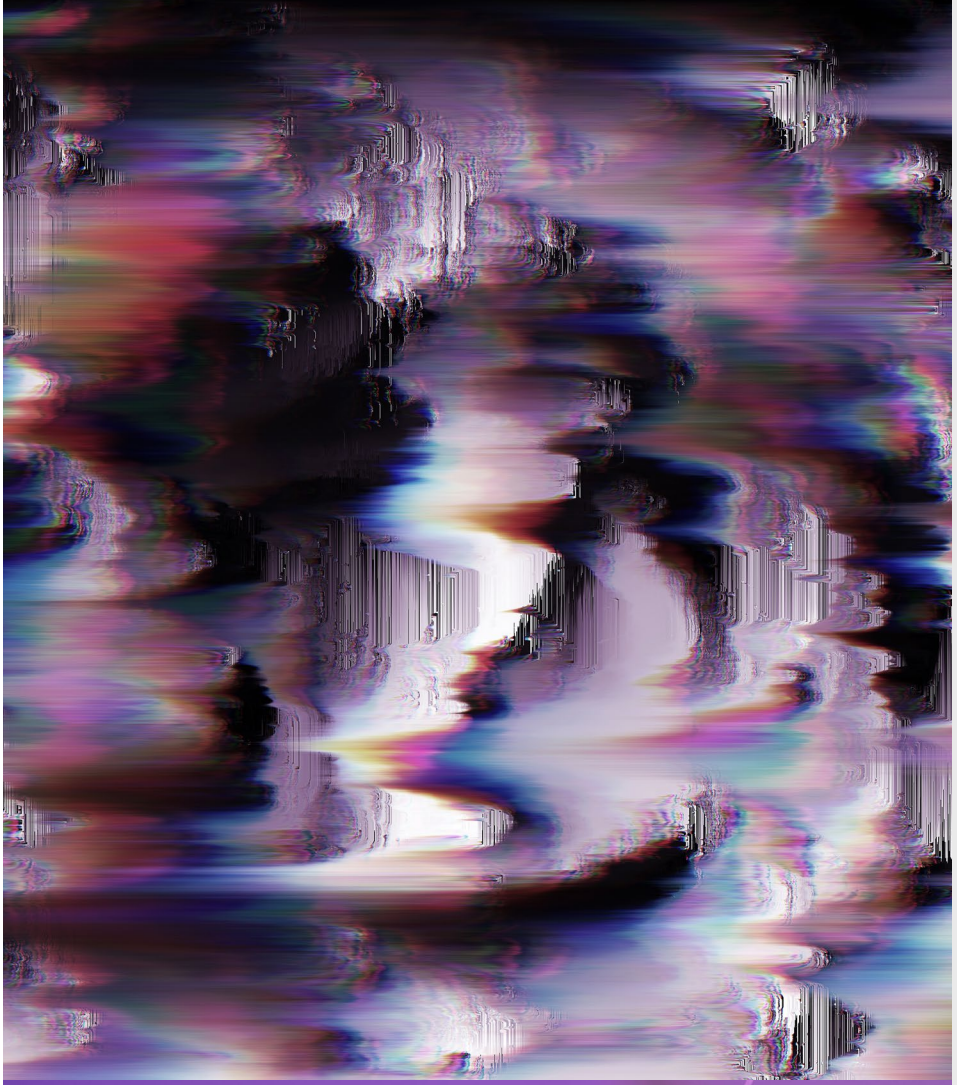
Commvault

eBOOK

Your Step-by-Step Guide to Cleanroom Recovery

FOR IT PROFESSIONALS

CONTENTS



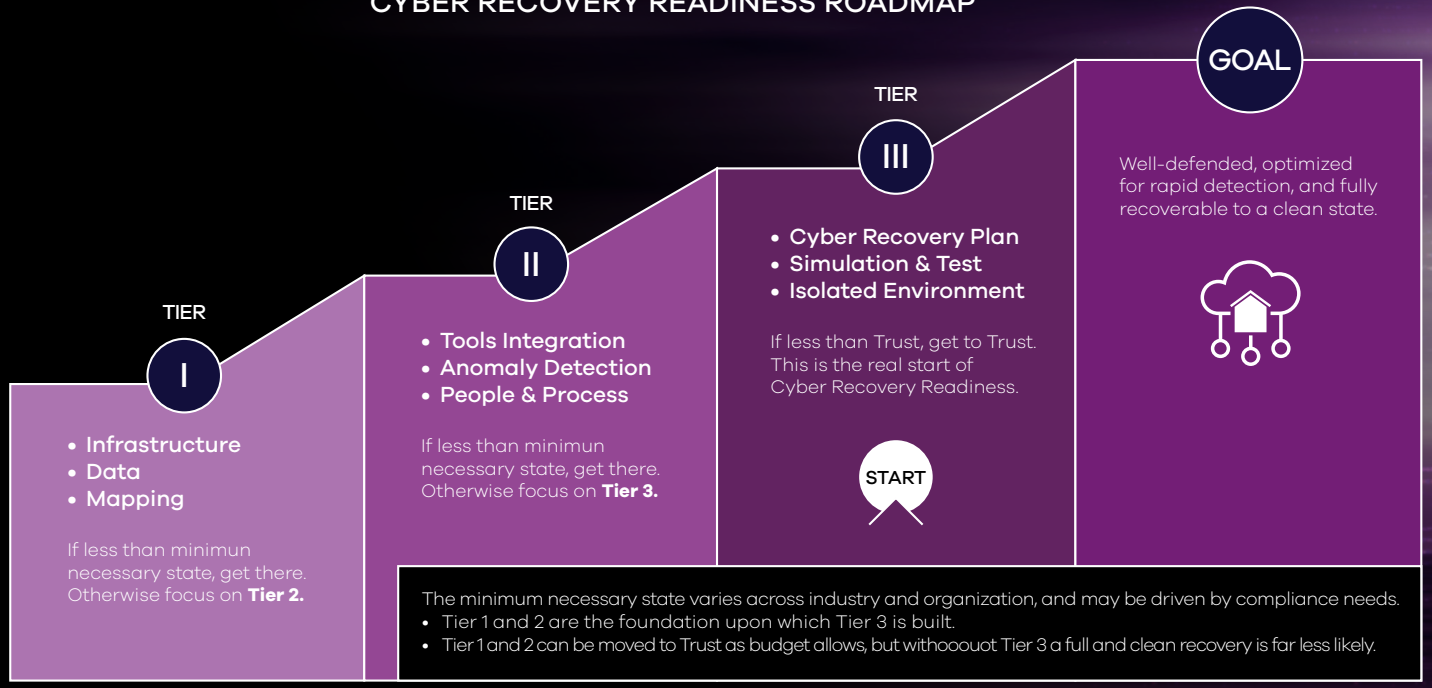
INTRODUCTION

Traditional disaster recovery (DR) drills, which are often scripted and predictable, do not adequately replicate the complexities of cyberattacks. Tabletop exercises, on the other hand, present more realistic attack scenarios, effectively capturing the chaos, variability, and pressure of an actual incident. This approach is valuable for pinpointing vulnerabilities in your response plans and procedures before a real attack takes place. However, the challenge lies in executing a true real-world recovery, which can be complex and expensive. Commvault Cleanroom Recovery addresses this issue by offering a cost-effective and flexible solution, providing a secure, isolated environment for realistic cyber-recovery testing.

HOW TO PLAN YOUR RECOVERY?

Commvault Cloud Cleanroom Recovery Solution epitomizes the strategic evolution from traditional data protection and recovery strategies to a holistic cyber resilience framework. This shift is essential in today's threat landscape, emphasizing data recovery as well as its protection and integrity throughout the cyber incident lifecycle.

CYBER RECOVERY READINESS ROADMAP



HOW TO PLAN YOUR RECOVERY?

PLAN

- **Initial assessment:** Begin with a comprehensive evaluation of current data protection and recovery strategies to identify critical assets, data, applications, and associated vulnerabilities that should be continually tested for cyber recovery readiness.
- **Integration planning:** Develop a detailed plan for integrating Commvault Cloud Cleanroom Recovery into existing IT and security frameworks, providing alignment with organizational cyber resilience goals.

TEST

- **Simulation drills:** Conduct simulated cyberattack scenarios to test the effectiveness of the cleanroom recovery process.
- **Operational testing:** Conduct actual operational testing before an incident occurs to find operational errors in the recovery process before the chaos of a cyber incident threatens an organization's ability to operate.
- **Process refinement:** Analyze test outcomes to refine recovery protocols and enhance the way the solution is used for testing and forensics use cases measures.

DEPLOY

- **Implementation:** Roll out Commvault Cloud Cleanroom Recovery for a seamless integration with minimal disruption to operations.
- **Ongoing optimization:** Establish a continuous improvement cycle, leveraging insights from testing and real-world operations to optimize the recovery strategy.

GET STARTED WITH

THE CYBER RECOVERY READINESS SELF-ASSESSMENT

TIER	ELEMENT	DESCRIPTION	Need it, don't have it	Have it, don't use it	Use it, don't test it	Test it, don't trust it	Trust it
I INFRASTRUCTURE	**Resillient Infrastructure**	Designed, built, operated, and maintained in a way that can withstand, adapt to, and rapidly recover from disruptions.					
	Data Discovery	The process of identifying and locating sensitive data within an organization's various systems and storage locations.					
	Data & Application Mapping	A holistic understanding of the information flow within an organization's IT infrastructure.					
II SECURITY	**Tool Integrations & Monitoring**	Combines and coordinates various security tools to create a comprehensive and synchronized defense system.					
	Anomalous Activity Detection	Identifies unusual patterns, events, or data points that deviate significantiy from what's considered normal behavior.					
	People & Process	Governs an organization's strategies and procedures for detecting and communicating concerns.					
II CYBER RECOVERY	**Cyber Recovery Plan**	Governs an organization's strategies and procedures for responding to and recovering from a cybersecurity incident.					
	Event Simulation	Tests an organization's plan in a controlled environment, allowing participants to practice response procedures and refine.					
	Isolated Recovery Environment	A specifically designed isolated and secure infrastructure, separate from the organization's production environment					

HOW DO YOU ADDRESS GAPS IDENTIFIED IN CYBER RECOVERY ASSESSMENT?

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.

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 wheworkloads 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, ensuring that production operation recovery is conducted within a sanitized environment.ent.

TIPS TO GET SECURITY BUY-IN

Effective collaboration and communication between IT and security teams are essential for ensuring a secure and resilient IT infrastructure.

Although the objective for all parties involved in cyber resilience is to safeguard the business, IT and SecOps might approach this with different methods that could potentially expose the business to external threats. It's crucial to find a mutual understanding.

1. **Shared goals:** Both IT and security teams aim to protect the organization's assets, systems, and data. They work towards maintaining the confidentiality, integrity, and availability of information.
2. **Collaboration:** IT and security teams often collaborate closely to implement and maintain security measures. They work together to identify vulnerabilities, implement security controls, and respond to incidents.
3. **Risk management:** Both teams are involved in assessing and managing risks. IT teams focus on operational risks related to system availability and performance, while security teams focus on mitigating risks associated with unauthorized access, data breaches, and other security incidents.
4. **Compliance:** IT and security teams work together to comply with relevant regulations and standards. They collaborate to implement controls and processes that meet legal and industry requirements.
5. **Incident response:** In the event of a security incident, IT and security teams collaborate to investigate, contain, and remediate the issue. They work together to minimize the impact, restore normal operations, and investigate its root cause post-incident
6. **Awareness and training:** Both teams play a role in promoting security awareness and providing training to employees. IT teams educate users on safe computing practices, while security teams provide guidance on identifying and reporting potential security threats.
7. **Stress testing:** A team that trains together builds bonds and achieves more. Stress testing your plans, policies, and ability to interact finds areas for potential improvement. Better to have it all worked out under ideal conditions, without the stress of an attack.

eBOOK

Learn more about how Commvault can help protect your organization, and get a demo of Commvault® Cloud Cleanroom™ Recovery.

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

Commvault®