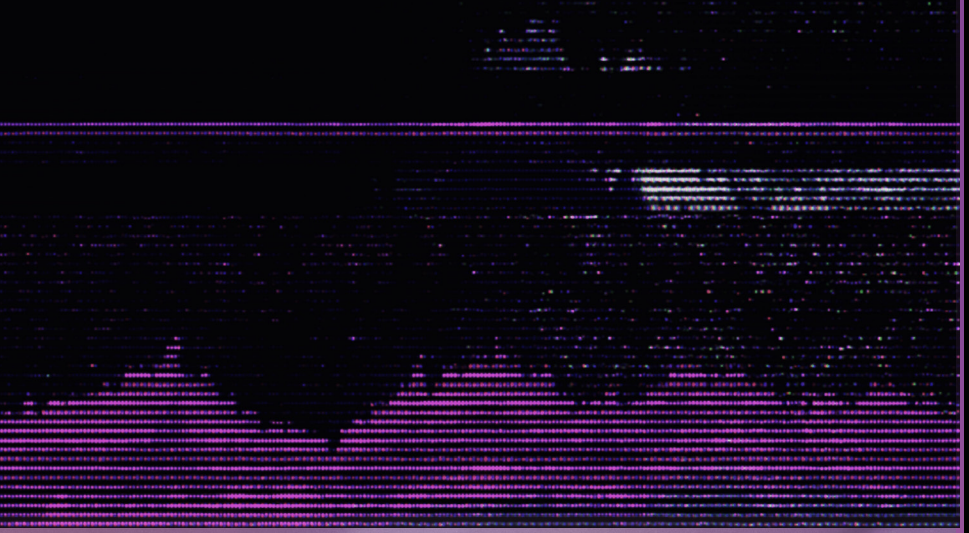


Commvault

eBOOK

Beyond Disaster Recovery

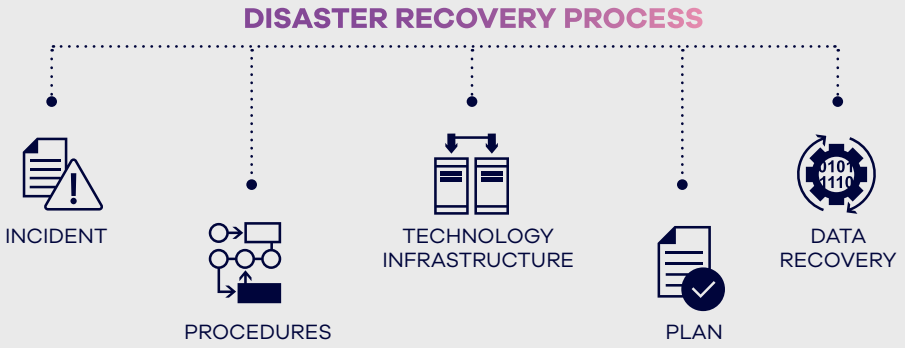
WHY YOU NEED A DIFFERENT STRATEGY WHEN CYBERATTACKS STRIKE

CONTENTS

DISASTER RECOVERY

You need a disaster recovery plan to handle predictable events like hardware failures or natural disasters like fires and floods. In general, these incidents aren't intentional and do not actively target your data.

Disaster recovery usually follows a pre-defined plan with established steps to restore systems quickly. Restoring from backups helps you get back online even if some data is lost. This process aims to ensure business continuity, minimize long-term impact, and protect critical data.



CYBER RECOVERY

In contrast, cyber recovery tackles malicious attacks like ransomware or data breaches, where attackers actively try to harm your systems and corrupt your data. This could be a subset of data or the entire infrastructure, including a disaster recovery failover site.

Cyberattacks often involve investigation and remediation before recovery, which can extend the timeline. You need to contain the attack and ensure no exploits remain. Every element of your environment, from hardware to data and backups, must be scrutinized for infection before restoring, as attackers might have hidden malware or altered backup files. You will need to minimize the damage, prevent data loss, and maintain security posture.

CYBER RECOVERY–READY DESIGN SCOPE

SCENARIOS

Cyber recovery generally drives a different set of needs vs. disaster recovery/business continuity plans

ELEMENTS	DISASTER RECOVERY/ BUSINESS CONTINUITY	CYBER RECOVERY
COMPROMISE	Full-site loss of operations	Data, networks, security
RECOVERY	Failover/back RTO, rebuild	Selective restore to repair
RESOURCES	Full availability stack	Validation, restore, rebuild
PLANNING	Persistent	Elastic

These strategies can be blended to converge resources and processes.

ORGANIZATION

Cyber recovery involves collaborative shared responsibility outcomes across the organization (people, process)

Integrating and automating notifications, informed actions, and seamless workflows across the teams can accelerate the outcomes.

CAPABILITIES

Cyber recovery requirements depend on the goals of the organization

- Secure, isolated, and immutable vault backups
- Early detection of suspicious patterns
- Cyber analysis and data sanitization
- Automated recovery validation
- Planned, rapid recovery

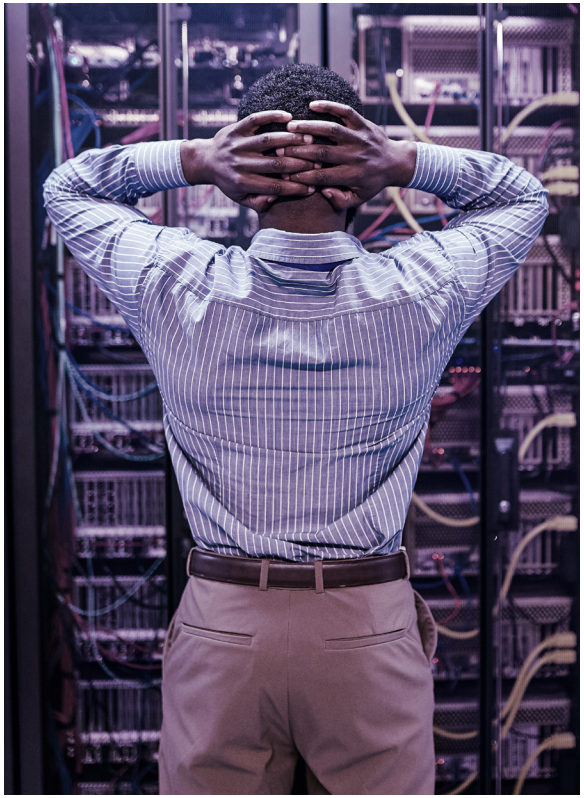
DISASTER RECOVERY TESTING IS NOT ENOUGH

Disaster recovery testing is important, but cyber recovery is much more comprehensive. While both aim to restore operational functionality after disruptions, fundamental differences necessitate distinct responses. Traditional disaster recovery plans struggle to effectively address the nuanced threats and complexities cyberattacks pose.

Here is why:

- Nature of the threat
- Scope and focus
- Methods and tools
- Data integrity and vulnerability

Therefore, while disaster recovery plans provide a valuable foundation for incident response, relying on them in the face of a cyberattack can be perilous. A dedicated cyber recovery plan, backed by specialized tools, personnel, and frequent testing, is essential for mitigating these malicious attacks' specific risks and complexities.



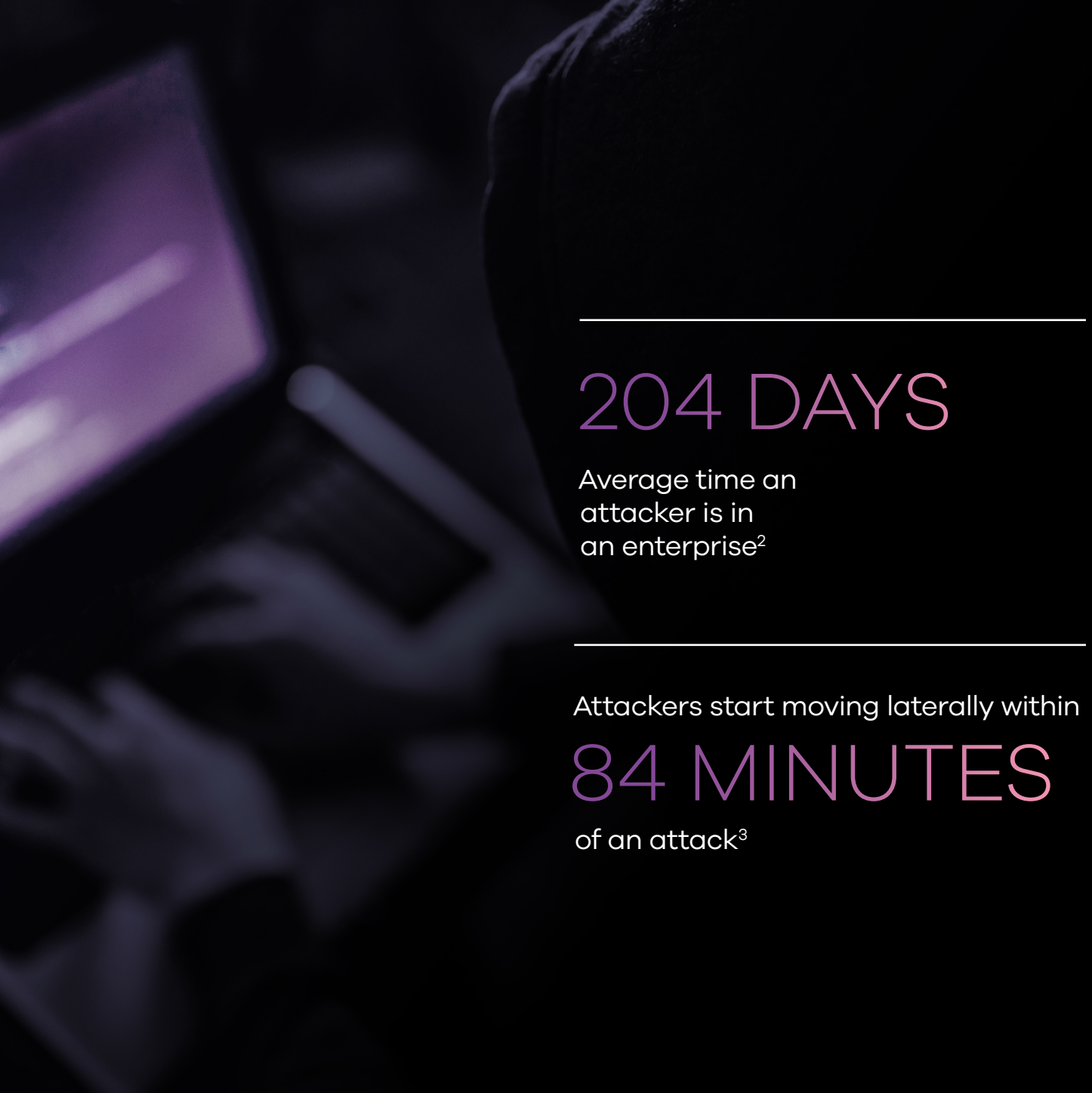
CYBER RECOVERY TESTING IS CRITICAL

Cyber recovery testing is an actual practice run (or operational test) of restoring an application and its data from a backup. This is the kind of restoration process that will happen in a cyber incident, and it is the process that NIST recommends. Disaster recovery testing and cyber recovery testing[1] each have their place for applicable scenarios, but cyber recovery is much more comprehensive.

Cyber recovery testing enables resilience for your systems and data, as well as business continuity. Recovering critical applications and data is fraught with complexity and issues. Testing cyber recovery helps uncover and resolve errors when the stakes are low.

Testing will give your teams practice and confidence to recover critical applications and data when a cyber incident occurs. In fact, NIST recommends "backups of data are conducted, protected, maintained and tested" because "it is better to identify an unexpected issue during testing than during an actual cyber event."[1] But the reality is that very few organizations test fully, frequently, and successfully.

[1] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-84.pdf



204 DAYS

Average time an attacker is in an enterprise[2]

92%

of companies that pay the ransom don't get all their data back[4]

Attackers start moving laterally within

84 MINUTES

of an attack[3]

[2] https://www.ibm.com/reports/data-breach
[3] https://www.crowdstrike.com/resources/reports/threat-hunting-report/
[4] https://www.sophos.com/en-us/content/state-of-ransomware

HOW COMMVAULT CLOUD HELPS

You can get proactive cyber resiliency with **Commvault® Cloud Auto Recovery**, minimizing the impact of data threats across all workloads and promoting business continuity. Auto Recovery delivers automated proactive cyber recovery through multi-layered data protection to reduce recovery time during cyberattacks and other disasters. With potential near real-time recovery time objective (RTO) and sub-minute recovery point objectives (RPO), Auto Recovery minimizes the impact of data threats broadly across cloud, on-premises, and SaaS workloads for business continuity.

Commvault® Cloud Cleanroom™ Recovery provides an affordable, clean, secure, isolated recovery environment on demand for testing cyber recovery plans, conducting secure forensic analysis, and uninterrupted business continuity.

Ongoing cyber threats and ransomware introduce existential risk and create organizational confusion and anxiety. Cleanroom Recovery offers a unique test bed to validate the effectiveness of cyber recovery plans, technologies, and processes.

Cleanroom Recovery provides a secure environment where data and critical assets are isolated and safeguarded from attacks. Security and IT leaders can obtain valuable insights into unfamiliar threat actors, fortify their strategies, and help enable uninterrupted business continuity.

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 possible for recovering data instantly
- Transform data during replication
- One-click orchestration production to disaster recovery, and vice versa
- Disaster recovery 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 provides 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

While a disaster recovery plan is essential to protect your company's infrastructure, you won't be fully protected unless you also have a cyber recovery plan and testing strategy in place, too. This is critical to keeping both your data and your reputation safe in the face of nefarious attacks.

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®