eBOOK

HOW REAL RESILIENCE IS PROVEN UNDER PRESSURE

CYBERATTACKS ARE FASTER, SMARTER, AND HARDER TO DETECT. TO STAY READY, YOU NEED MORE THAN A PLAN – YOU NEED REAL RESILIENCE.

Commvault®

Contents

Preparedness vs. Real Resilience

Every vendor claims resilience, and most organizations believe they're prepared.

However, when a real attack occurs, gaps in preparedness begin to surface.

Many recovery strategies were designed for predictable disruptions – not the intelligent, adaptive threats of modern cyber attackers and frontier AI. Advanced AI models can autonomously map an entire enterprise attack surface in hours, discover vulnerabilities that have gone undetected for decades, and enable attackers to move and adapt faster than any patch cycle can keep up with.

Today's cyberattacks move faster, remain hidden longer, and increasingly target the very systems organizations depend on for recovery. As a result, several challenges are becoming more difficult to manage:

- **Backups are no longer a guaranteed fallback:** Attackers are increasingly targeting backup systems to weaken recovery options. In some cases, backup data may be encrypted, deleted, or compromised – making it harder to identify a trusted recovery point.
- **Attackers can persist undetected:** Threat actors may remain inside environments for extended periods, moving laterally and establishing persistence. This can make it difficult to determine when an attack began, what identities may have been compromised, and which data can be safely restored.
- **Recovery may reintroduce risk:** Without proper validation, restoring systems can unintentionally reintroduce malware or compromised configurations, extending the impact of an incident.

Preparedness assumes recovery will be clean, fast, and reliable – but the reality is becoming more complex. With frontier AI accelerating the pace and scale of attacks, organizations need stronger visibility and faster response across their environments.

92%

of IT security leaders say AI-enabled cyber threats are forcing them to significantly upgrade their defenses.[1]

[1] The State of AI Cybersecurity 2026, Darktrace

Resilience for a New Reality

Cyberattacks don't just disrupt systems – they corrupt data, compromise identities, and erode trust. Attackers often move quietly through environments, establishing persistence and spreading across systems before detection. By the time an incident is identified, it can be difficult to determine what data is unaffected and what can be safely restored.

Frontier AI is making this challenge more immediate. The same AI capabilities that can support defenders are also being used to create and accelerate attacks across the lifecycle, from reconnaissance to exploitation. As the time between vulnerability discovery and exploitation continues to shrink, organizations need stronger cyber resilience strategies that go beyond patching alone.

Today's new reality:

- **AI is accelerating attack speed and scale:** Automated techniques allow attackers to move faster and adapt in real time.
- **Hybrid and multi-cloud environments increase complexity:** Data, applications, and identities are distributed across environments, making it harder to maintain visibility and control during recovery.
- **Recovery must happen under extreme time pressure:** Organizations are expected to restore operations quickly, even when the scope and impact of an attack are still unfolding.

Resilience is no longer an aspirational program for high-achieving teams – it's a required capability for every organization. To keep up in the frontier AI era, organizations need resilience that is:

- **Continuous:** Always tested and ready
- **Validated:** Built on trusted, clean data
- **Unified:** Across data, identity, and workloads

Without these capabilities, recovery becomes uncertain – slowed by complexity, risk, and a lack of confidence in the outcome. Real resilience requires a more disciplined, operational approach to verify recovery is not only possible, but trusted.

What Is Real Resilience?

If your recovery strategy can't meet today's demands, it's not real resilience.

AI demands a new approach that's capable of actively monitoring the state of your data and instantly restoring it. Commvault Cloud is the only unified platform that combines coverage of cloud, on-prem, and SaaS workloads with identity protection, risk analytics and cyber recovery – helping automate resilience and making it operational.

Here's what real resilience looks like:

Real Clean

Recoveries that don't need a recovery.

THAT WAS THEN

Rolling back to before the attack – and losing everything good that came after.

THIS IS REAL

Commvault Threat Scan can help identify compromised data and support rebuilding a clean version of your files, reducing the risk of reinfection.

Real Complete

Recover clean. Recover fast. Recover more.

THAT WAS THEN

Your data comes back – but your apps, configurations, and cloud infrastructure still have to be rebuilt from scratch. Data recovery and business recovery are not the same thing.

THIS IS REAL

Commvault can help recover your business across workloads, clouds and identities – from a single platform designed for the scale of today's attacks.

Real Fast

Test continuously. Recovery with confidence.

THAT WAS THEN

Everyone has a recovery plan ... that no one ever tests. It's a guess you're making at the worst possible moment.

THIS IS REAL

With Commvault, you can easily spin up an on-demand, isolated Cleanroom that helps you validate recovery continuously.

From Recovery Plans to ResOps

(Resilience Operations)

Traditional recovery focuses on isolated events.
Modern resilience requires a continuous lifecycle as frontier AI increases the pace of cyber threats.

ResOps includes:

01 **DISCOVER**
Understand your critical data, systems, and identities.

02 **PROTECT**
Safeguard and isolate data with strong controls.

03 **DETECT**
Identify threats, anomalies, and compromised assets.

04 **RECOVER**
Restore clean data and rebuild systems.

05 **VALIDATE**
Test recovery readiness continuously.

06 **IMPROVE**
Strengthen processes based on real-world outcomes.

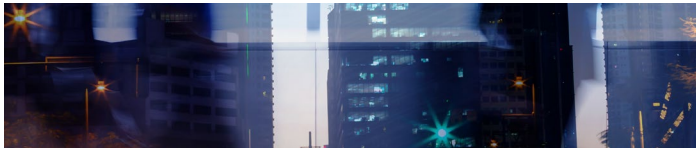
This lifecycle transforms recovery from a reactive process into a proactive, operational discipline designed to support resilience in a fast-moving threat environment.

Start Recovery with Minimum Viability

In a real resilience model, recovery doesn't begin with everything – it begins with what matters most. Minimum viability is a foundational concept for resilience that prioritizes restoration of the most critical systems, data, and processes required to keep your business running.

When an attack occurs, minimum viability helps you:

- **Prioritize critical operations first:** Identify the systems and data essential to business continuity, so recovery efforts are focused where they have the greatest impact.
- **Restore trusted, clean data:** Focus on recovering validated data to help reduce the risk of reinfection and avoid restoring compromised systems.
- **Resume operations under pressure:** Bring key services back online quickly while broader recovery efforts continue in parallel.
- **Reduce complexity during recovery:** Limit scope in the initial phase of recovery, helping teams make faster, more confident decisions.



Minimum viability is not the end state of recovery – it's how recovery begins. It provides a controlled, practical starting point for restoring operations while maintaining trust in your data.

Learn more about the steps to restore your business operations and our recommended practices in **The Ultimate Guide to Minimum Viability**.

How Commvault Delivers Real Resilience

Commvault helps you achieve real resilience by unifying protection, recovery, and validation across your environment.

Commvault® Cloud

Commvault Cloud brings together data, applications, and infrastructure across cloud, SaaS, hybrid, and on-prem environments into a single platform. This unified approach helps reduce fragmentation and enables consistent protection and recovery operations across your entire data estate.

Commvault Cloud Threat Scan

AI-enabled threat detection helps identify anomalies and flag potentially compromised data within backup environments, helping reduce the risk of reinfection during recovery. By improving visibility into threats, teams can make more informed decisions about what data is safe to recover. Automated workflows coordinate response and recovery actions across systems and applications, helping reduce manual effort and helping teams recover more efficiently.

Commvault Cleanroom™

Cleanroom provides a secure, isolated environment to test recovery scenarios, validate data integrity, and conduct forensic analysis. This allows organizations to continuously test their recovery plans and improve confidence in real-world outcomes. And it can help organizations can **increase recovery testing frequency by up to 30x**.

Commvault Cloud Rewind™

Cloud Rewind helps enable organizations to recover clean, trusted data and rebuild applications quickly after an incident. By orchestrating recovery processes, it helps reduce downtime and supports faster restoration of critical services. Organizations have recovered **800+ cloud resources and 200+ TB of data in under 10 hours**, averaging minutes per object.

eBOOK

Test Your Resilience Before an Attack Does

As cyber threats continue to evolve, recovery is no longer just about getting systems back online. It's about restoring trusted data quickly and confidently, even when backups and environments may be compromised.

The question isn't whether you can recover. It's whether you can recover clean, fast, and with confidence.

TAKE THE ASSESSMENT

www.commvault.com/cyber-resilience

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

Commvault®