Commvault

WHITE PAPER

Cyber Resilience needs Confidence: Recover Clean Data, Fast.

THE NEW HORIZON OF CLEAN AND FAST RECOVERY

In an age of artificial intelligence (AI) further driving relentless cyber threats, **speed and confidence** in recovery are no longer luxuries—they are operational imperatives. The Commvault-exclusive **Synthetic Recovery™** redefines the clean recovery process by automating how organizations identify and assemble last known good versions of files enabling rapid restoration of operations while minimizing data rollback and reinfection risks.

Through **AI-enabled, multi-engine threat detection and response capabilities,** Commvault can intelligently use Cleanpoint™ identification and can remove malware and encrypted files from backup datasets. The result: **faster, cleaner recoveries** and **unified, resilient operations** across the enterprise.

THE CHALLENGE: RISK OF HIDDEN THREATS IN PROTECTED DATA

94%

of ransomware attacks attempt to compromise backups[1]

Cyber threats, both known and zero-day threats, are increasingly stealthy, often lying dormant for days—or even months—before activating. Attackers use this **"dwell time"** to spread laterally, implanting malware, installing backdoors, and preparing ransomware payloads. By the time the threat is detected, backups may already contain compromised data.

Industry dwell time benchmarks illustrate the problem and foreshadow a solution:

1–2 weeks median dwell time globally[2] **or** **1–3 days** median dwell time in continuously monitored environments[3]

Can you keep up with the speed of modern adversaries?

≤10 minutes to detection

≤60 minutes to containment[4]

vs today's reality

241 days average from breach identification to containment[5]

48 minutes average Adversary breakout time[6]

COMMVAULT'S CONTINUOUS BUSINESS PRINCIPLE: INNOVATING "PROTECT FIRST, SCAN LATER"

For years, data protection practices operate under a guiding principle: protect first, scan later. The idea of the approach is to back up data immediately, without challenging its integrity. It prioritizes availability and continuity – a foundation of cyber resilience that Commvault remains committed to upholding.

- **Continuous Protection:** Data is captured without delay, so restore points can constantly be available.
- **Forensic Staging:** Even potentially compromised backups are preserved for investigation in isolated, quarantined environments.
- **Deferred AI Scanning:** Advanced threat analytics inspect protected data post-backup to surface hidden malware and encryption artifacts.

While this model has served organizations well, the growing sophistication and speed of modern cyber threats demand an evolution. Commvault is advancing this principal – exploring ways to bring threat detection and data protection closer together, integrating threat detection mechanism earlier in the process.

This evolution aims to help organizations **identify potential risks sooner**, alert on anomalies before they become full-blown incidents, and continue to innovate so every recovery can become **fast, clean, and complete**.

1 Sophos, "The impact of compromised backups on ransomware outcomes", 2024
2 Google Cloud Security, Mandiant M-Trends 2025 Report, 2025
3 Sophos, "Active Adversaries Report", 2025
4 CrowdStrike, Global Threat Report, 2025
5 IBM, 2025 Cost of a Data Breach Report, 2025
6 CrowdStrike, Global Threat Report, 2025

WHY TRADITIONAL DATA RECOVERY FALLS SHORT

Organizations that depend on conventional recovery strategies typically rely on manual steps:

- Creating **Isolated Recovery Environments (IREs)**
- Manually restoring and scanning data
- Guessing a single last known good recovery point without tools for restore testing and validation

These methods are slow, labor-intensive, and often unreliable— introducing **data loss, reinfection risks, and operational inefficiencies.** The absence of automation leads to longer downtime, room for human error, and uncertainty during the most critical phase: recovery.

INTRODUCING SYNTHETIC RECOVERY: AUTOMATING CLEAN, CONFIDENT RESTORATION

Synthetic Recovery is Commvault's new, automated method for **assembling the last known clean version** of data across all backups to eliminate guesswork. By leveraging AI-enabled **threat detection**, it identifies and excludes compromised files while reconstructing the cleanest, most current dataset possible.

Key Outcomes

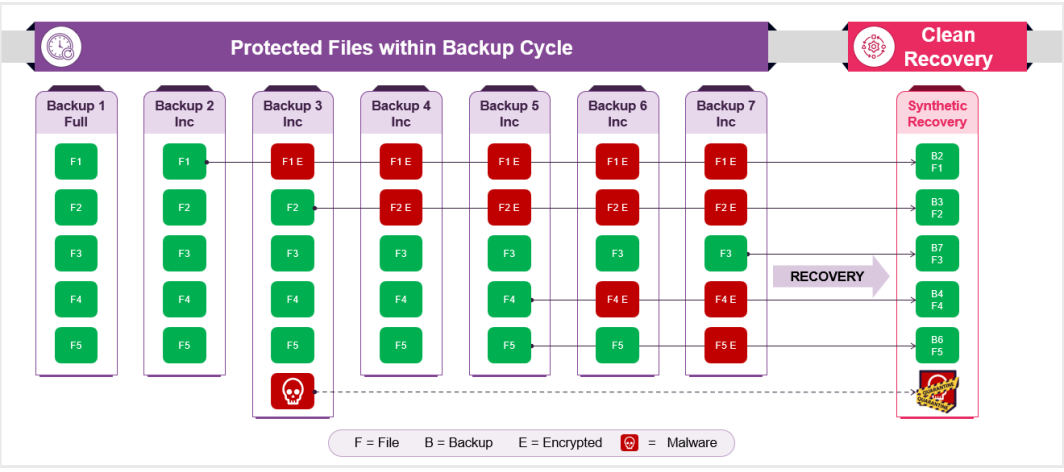
- **Recover faster:** Automation shrinks recovery time from hours to minutes.
- **Recover cleanly:** Automatically replaces corrupted files with verified clean versions.
- **Reduce rollback:** Only excludes affected files from earlier backups—no single point in time across instances.
- **Avoid reinfection:** Confidently recover without re-introducing dormant malware.

HOW SYNTHETIC RECOVERY WORKS

Synthetic Recovery functions at the index layer of the Commvault platform.

1. **Backup and Indexing**:
   Commvault can build an index of every full and incremental backup, recording file metadata (including name, size, path, and type).
2. **AI-Enabled Threat Scanning:**
   Commvault's multi-engine threat detection flags encrypted or malicious files.
3. **Curated Recovery Point Creation:**
   For restoration, the platform can automatically select the most recent clean file versions across backups.
4. **Automated Clean Recovery:**
   Corrupted or encrypted files are excluded, resulting in a clean, verified dataset ready for production.

Synthetic Recovery Workflow



The diagram to the left visually demonstrates how Synthetic Recovery assembles clean data from multiple backups while quarantining malware and infected versions. Visual of how Synthetic Recovery pinpoints and removes compromised data (patent-pending).

PRECISION AND AI: THE POWER BEHIND THE PLATFORM

Commvault's **detection mechanism** utilizes:

- Anomaly detection
- Signature-based scanning
- Heuristics malware analysis
- Machine-learning threat & encryption identification
- YARA-rule detection
- Hash scanning
- Security partner signals

This fusion drives **unparalleled accuracy** in identifying both known and emerging threats. Synthetic Recovery then applies these insights to recovery workflows, enabling **data integrity and operational continuity**.

UNIFIED RESILIENCE: FASTER, CLEANER, SMARTER

Synthetic Recovery aligns backup, recovery, and threat intelligence into one cohesive resilience model.

The result: **confidence at scale**—for IT and security operations alike.

BUSINESS OUTCOME	BENEFIT
Faster Recovery	Automated clean restoration
Reduced Reinfection Risk	AI driven mechanism removes infected data
Operational Efficiency	No manual scanning needed or rollback guesswork
Data Integrity	Preserves latest known clean versions
Unified Resilience Operations	Seamless integration of protection, detection, and recovery

CONCLUSION: CYBER RESILIENCE REQUIRES CONFIDENCE

In a world where the next ransomware attack is inevitable, confidence is everything. Commvault's Synthetic Recovery orchestration is the enabler for enterprises that their **recovery will be both fast and clean**, powered by **AI precision** and **automated procedures.**

With Commvault, cyber resilience isn't just about surviving the attack—it's about **recovering with certainty, speed, and strength**.