BACKUPS DON'T MATTER.

If they can't bring your business back. A field guide to recovering cleanly after ransomware, not just restoring files.

WHAT CLEAN RECOVERY TAKES

Known-clean points · Isolated recovery · Identity-first sequencing · Tested runbooks · Minimum viable operations

THE ASSUMPTION

A backup is not a recovery plan.

A green checkmark proves a backup job completed. It does not prove your business can come back. Those are different questions, and ransomware makes the difference existential.

Backup thinking asks: did the job run? Recovery thinking asks: can we operate again, cleanly, before the damage is permanent? The first is a storage problem. The second is operational, spanning clean data, identity, infrastructure, dependencies, runbooks and people, all under pressure.

BACKUP THINKING	RECOVERY THINKING
Did the job complete?	Can the business operate?
Files and workloads	Critical services
Assume the copy is clean	Prove the copy is clean

54%

of enterprises lack confidence in their ability to recover from a major disruption.

41%

faster recovery among organizations with higher cyber-recovery maturity.

70%

of cyber-mature organizations test their recovery plans quarterly.

THE THREAT

Ransomware targets your recovery, not just your data.

Modern ransomware is not a smash and grab. Attackers dwell for weeks, escalate privileges and quietly disable defenses before they encrypt a file. By the time you notice, your recent backups may already be compromised.

Long dwell time

Attackers are often inside for weeks before they encrypt. Your most recent backup may already contain their foothold.

Backups are a target

Snapshots are deleted, repositories encrypted and retention revoked, on purpose, to remove your safety net first.

Identity is compromised

Active Directory and Entra are prime targets. If identity is dirty, everything that depends on it is suspect.

Reinfection risk

Restore a compromised point into production and you can reinfect the very environment you are trying to rebuild.

ANATOMY OF AN INCIDENT

INITIAL ACCESS	Phishing, stolen credentials or an exposed service. Usually quiet and unremarkable.
SPREAD & PERSISTENCE	Privilege escalation, lateral movement and disabling of defenses. Dwell time measured in weeks.
TARGETING BACKUPS	Snapshots deleted, repositories encrypted, retention revoked. The safety net is removed first.
EXFILTRATION	Data stolen for double extortion, before anything is locked.
ENCRYPTION	Systems locked, often on a Friday or a holiday. Operations stop.
DISCOVERY & DECISION	Now the questions begin: which point is clean, where to restore, what comes online first, who can log in.

The questions a backup report cannot answer.

When an incident hits, these decide whether you come back. A backup report answers none of them.

01 Which recovery point is clean?

02 Where will you restore it?

03 What comes online first?

04 Can anyone authenticate?

05 Who has authority to make the call?

06 Has this ever been tested for real?

Recovery readiness answers all of them, before the day it counts.

THE ANATOMY OF RECOVERY

It takes more than a copy.

Clean recovery is the sum of six things working together, in order and under pressure.

01 **Clean data**

A verified, known-clean recovery point. Not simply the latest copy, which may already be compromised.

02 **Identity**

Authentication restored before the systems that depend on it. Nothing logs in until identity is back.

03 **Infrastructure**

Compute, network, DNS, storage and configuration, ready in a place you control.

04 **Dependencies**

Applications returned in the order the business actually needs, not alphabetically.

05 **Tested runbooks**

Current procedures with named owners, clear authority and proof they have been run.

06 **Prepared people**

Teams that know their role before pressure arrives, not during the incident.

= A business that comes back.

THE METHOD

Test. Isolate. Validate. Recover clean.

Clean recovery is a repeatable discipline, not a lucky restore. Four moves, and three things they depend on.

01 **Test**

Rehearse recovery before you need it. A plan that has never been run is a hypothesis, not a capability.

02 **Isolate**

Recover into a clean, isolated environment, separate from the compromised one, so you never reinfect production.

03 **Validate**

Prove the recovery point is clean and the restored systems are healthy before you trust them with real traffic.

04 **Recover clean**

Bring the business back on a known-clean foundation, in the order operations actually need.

Find a known-clean point

The latest backup is not automatically clean. Immutable, air-gapped copies plus anomaly scanning prove a point predates the intrusion.

Recover in a clean room

Restore into an isolated environment, apart from production and the attacker. Validate there, then promote only what is proven.

Sequence identity first

Nothing authenticates until identity is back. Restore AD, Entra and DNS first, then apps in dependency order.

READY WHEN IT COUNTS

Your next backup will run. Will your business come back?

Commvault delivers clean, immutable, isolated cyber recovery. KELYN makes it operational: architected around your critical operations, tested until the gaps are gone, and run by experienced, 100% U.S.-based engineering.

ARCHITECT · OPTIMIZE · PROVE · OPERATE

TALK TO A RECOVERY ENGINEER →

KELYN

Recovery, operational. Powered by Commvault.

KELYNTECH.com

COMMVAULT FEDERAL PARTNER OF THE YEAR

FIRST MSP FOR COMMVAULT GOVCLOUD

ENTERPRISE + GOVERNMENT