halcyon

An Executive Guide to Ransomware Resilience

5 Reasons Backup and Recovery Is Not a Ransomware Strategy

WHY BACKUP FALLS SHORT

Practitioners who have been around security long enough know that backup and recovery solutions were never designed for ransomware. They were built for hardware failure, accidental deletion, and natural disasters.

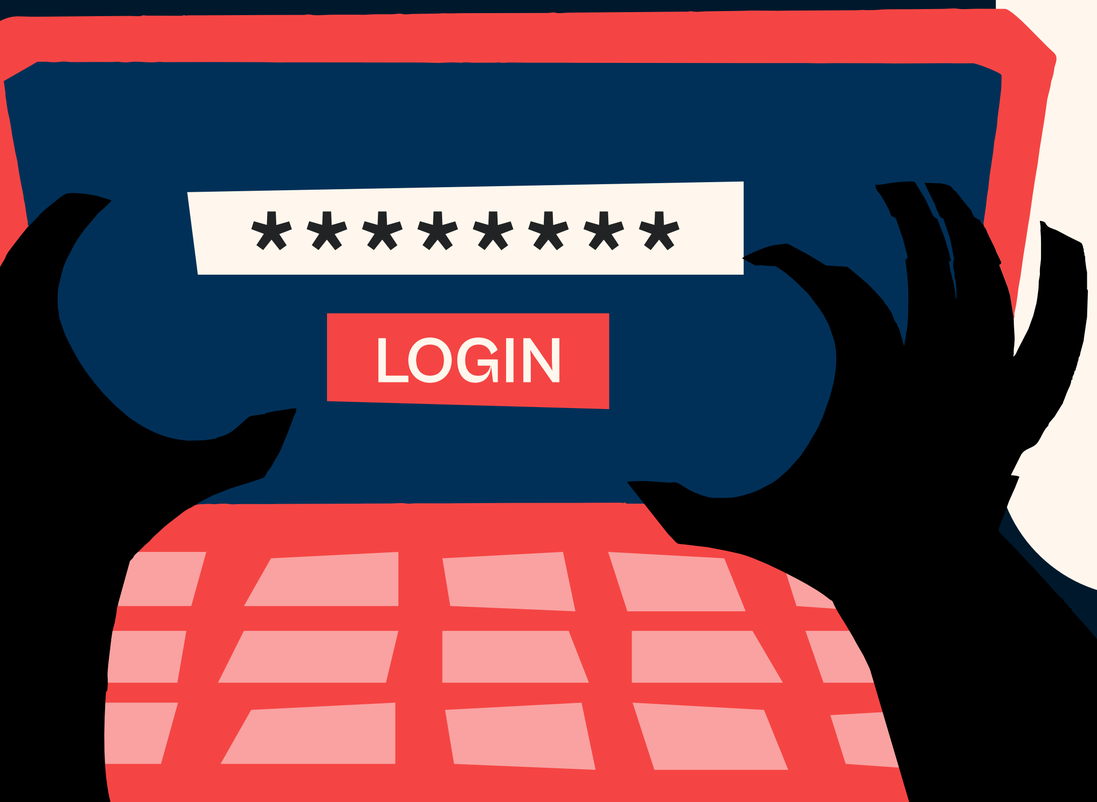
Backup answers one question: can we get the data back? This is theoretical. In reality, ransomware forces organizations to answer a dozen other questions that backup is not equipped to address.

Modern ransomware groups operate like professional criminal enterprises. They research targets, exfiltrate data before encrypting, destroy recovery options, and time their attacks for maximum disruption. By the time most organizations realize what is happening, their backup strategy has already been rendered useless. Read on to discover the most important five reasons why.

1 Attackers Spend Weeks Inside Your Environment Poisoning or Deleting Your Backups

Ransomware is the final step of a process that began weeks or months earlier. Attackers had unrestricted access to victim environments for an average of **70+ days between 2022 and 2024**. During that time, they are conducting reconnaissance, escalating privileges, exfiltrating data, and systematically neutralizing backup infrastructure. Veeam, one of the largest backup and recovery solutions, found that in **96% of attacks, threat actors targeted backup repositories directly, succeeding 76% of the time**. By the time encryption triggers, the recovery option is already gone.

With weeks or months of undetected access, attackers locate administrator credentials, access the management console with legitimate permissions, and work around every protection before a single alert fires.



Here is what that process looks like:

- Identify and map backup repositories, storage locations, and retention policies.
- Manipulate retention policies to trigger automatic purge of all prior backup generations.
- Delete the backup catalog, making immutable data impossible to locate and restore.
- Manipulate time synchronization to trick systems into releasing immutable retention locks.
- Terminate backup services entirely immediately before triggering encryption.

While backup vendors have built features specifically to counter these tactics, including immutable storage, quorum controls, air-gapped vaults, and anomaly detection, ransomware attackers use dwell time to bypass all of them. With weeks or months of undetected access, attackers locate administrator credentials, access the management console with legitimate permissions, and work around every protection before a single alert fires. Immutability protects data from direct modification but not the management plane from a trusted account. Quorum controls depend entirely on consistent enforcement and proper configuration.

Ransomware attackers have adapted by deliberately remaining dormant to defeat backup protections through two methods: **outlasting retention windows so that every available restore point contains compromised data before encryption triggers** or **disabling backup jobs entirely and waiting for existing snapshots to auto-delete on schedule**, leaving nothing to restore to when the attack finally executes.

When encryption finally triggers, the backups are gone or poisoned, the recovery window has closed, and the only option left is to pay or rebuild from scratch.

2 Recovery Takes Weeks. Your Business Cannot Afford It.

Organizations treat having backups as a risk mitigation strategy. The logic makes sense on paper: if you can recover your data, you can survive a ransomware attack. What that framing misses is that recovery is not the same as continuity. Even a successful restore still means days or weeks of systems being down, operations running on manual processes or not at all, employees unable to do their jobs, customers unable to reach you, and revenue stopping while the recovery clock runs. Backups mitigate the risk of permanent data loss. It does not mitigate the business disruption that happens while you are getting there.

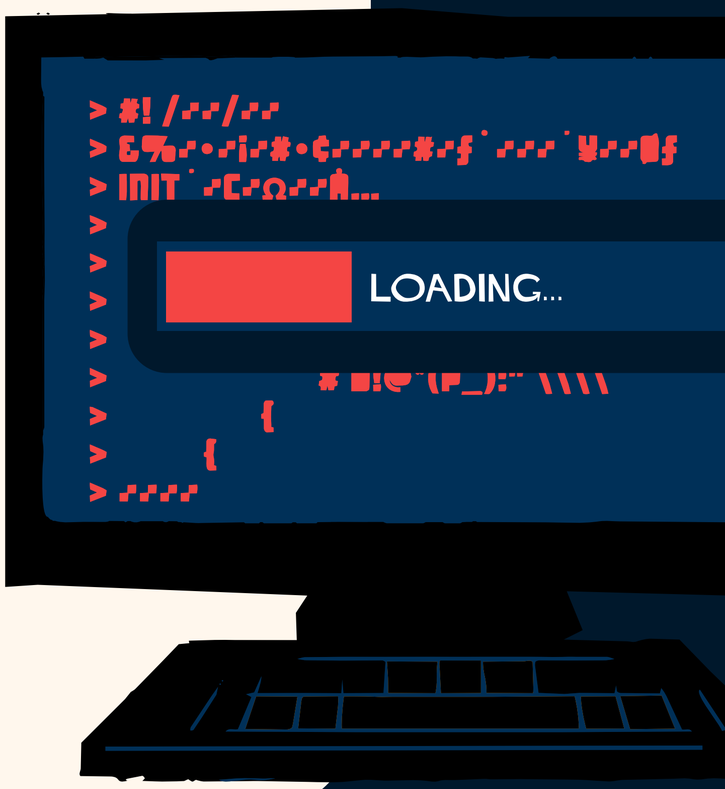
According to Gartner, the average organization spends 22 days recovering from ransomware, with enterprise environments averaging 38 days.

At $14,000 per minute in downtime costs, that disruption alone approaches $48 million before counting ransom, legal, or recovery expenses.

The recovery time can be so high due to any variety of reasons:

1. Restoration cannot start immediately

Before any system can come back online, the organization must contain the attack, isolate infected systems, and stand up out-of-band communications because email and collaboration tools are potentially compromised. Containment speed is directly tied to how prepared an organization is before the attack happens. Cybersecurity Time has the estimated containment time breakdown as follows:



6 to 12 hours in highly mature enterprise environments, 12 to 36 hours in mid-sized organizations, and 48 to 96 hours or longer in under-resourced environments. For every hour containment is delayed, the attack spreads further, more systems require restoration, and the recovery timeline extends accordingly.

2. Forensics must come before recovery. Insurance carriers require documented forensic investigation before processing claims, and law enforcement requires preserved evidence. No system can be wiped or rebuilt until forensic images are captured. **Incident response practitioners** describe the first 1 to 4 hours after containment as scope assessment: determining which systems are encrypted, which credentials are compromised, whether data was exfiltrated, and critically, when the attack actually began. **Organizations that skip forensics** to accelerate restoration frequently discover weeks later that the attack vector was never closed and attackers re-enter, extending the total recovery timeline far beyond what the shortcut saved.

3. Backup verification is its own phase. Every candidate restore point must be scanned for malware in an isolated environment before it is used. This includes running antivirus and YARA rule scans against mounted backup data, validating database integrity, and documenting each restore point as clean or infected. **Veeam's own documentation** notes that when multiple machines share a single repository, orchestrators must process them sequentially, which can significantly affect recovery time objectives. **Microsoft's guidance for Azure Backup** recommends restoring to an isolated network first, verifying healthy recovery points on smaller data sets, and scanning restored data for infection before connecting to production. In large environments with multiple candidate restore points that span weeks of dwell time, this process alone can add significant time to the overall recovery window.

4. Restoration happens in tiers, not all at once. **Microsoft's own guidance** has identity systems, including Active Directory and domain controllers, as the first priority for restoration because nothing else in the environment can authenticate until they are back online. Core business systems follow, then line-of-business applications, integrations, and workstations last. Each system must be validated in isolation before returning to the network. **Active Directory recovery alone involves 40 high-level steps** and can take days or weeks yet only 27% of organizations have dedicated identity recovery solutions in place. Every credential in the environment must be treated as compromised and rotated before systems return to production. At enterprise scale, with systems validated sequentially and thousands of accounts rotated, this phase alone drives the 38-day average recovery window.

According to Gartner, the average organization spends 22 days recovering from ransomware, with enterprise environments averaging 38 days.

3 Ransomware Is No Longer Just Encryption.

Modern ransomware attacks are multi-extortion operations by design. Attackers steal data before encrypting it, threaten to publish it publicly, and collect leverage regardless of whether the victim restores from backup.

- **Arctic Wolf** found that in 96% of ransomware cases analyzed, threat actors exfiltrated data before or alongside encryption.
- The **Halcyon Ransomware and Data Extortion Business Risk Report** found that 60% of respondents said that sensitive or regulated data was exfiltrated from their organization during the attack.

The **ClOp ransomware group's 2023 MOVEit campaign** is one of the clearest examples of how far the threat has moved beyond encryption. ClOp exploited a zero-day vulnerability in Progress Software's MOVEit file transfer product to steal data from over 2,700 organizations affecting an estimated 95 million individuals, without deploying a single encryption payload. There were no encrypted files to restore, and no backup strategy that could have changed the outcome. The leverage was the stolen data alone. **Over 90% of victims did not pay**, yet the data had already left their environment, exposing millions of individuals to ongoing breach risk regardless of what any organization did next. **ClOp still earned an estimated $75 to $100 million** from the small number who paid.

Backup cannot un-expose data. It cannot prevent regulatory notification obligations, litigation exposure, or secondary extortion. Once data leaves the environment, no restore operation addresses those consequences.

4 Recovery Does Not Mean You Got Everything Back.

Restoring from backup may feel like the finish line, but often it is not. Even in a best-case recovery scenario, organizations routinely discover that what came back is a fraction of what was lost, and that the business consequences of the attack are still running long after the last system is restored.

That confidence gap is well documented. **Veeam's 2026 Data Trust and Resilience Report**, based on responses from more than 900 senior IT, security, and risk leaders, found that 90% of organizations are confident they can recover quickly and meet their recovery time objectives, but only 28% of ransomware victims fully restored all affected data. The belief that backup equals recovery and the reality of what actually comes back are fundamentally different things.

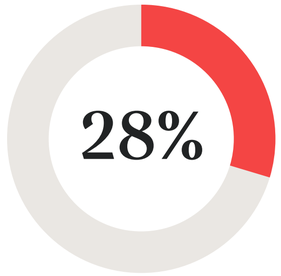
On the data side, **only 57% of affected data is recovered on average** in a ransomware attack, even when backups are in place. The remaining 43% is simply gone. The gap between the last clean restore point and the moment of the attack represents everything that happened during the attacker's dwell period that was never cleanly captured. For organizations with daily or weekly backup schedules, that can mean days or weeks of transactions, records, communications, and work product that no restore operation can retrieve.

Backup restores data and systems. It does not restore what the attack cost the business while those systems were down. Customers who could not be served found alternatives. Contracts subject to SLA penalties have already been breached. Reputational damage from public disclosure has already landed. Revenue lost during 22 to 38 days of downtime does not come back when the servers do. These are permanent business consequences that exist entirely outside the scope of what any backup platform is designed to address.

Recovery also does not make the organization safer. **Varonis found** that 60% of organizations that paid a ransom experienced a repeat attack. Restoring systems from backup does not close the initial access vector, revoke credentials harvested during dwell time or remove the organization from the attacker's target list. Without addressing those underlying exposures, recovery is just a reset to a state where the same attack is possible again.

THE REALITY GAP

of organizations are confident they can recover



of victims actually made a full recovery

5 Backup Vendors Are Building Security Features. They Still Don't Stop the Attack.

Gartner's 2025 Magic Quadrant for Backup and Data Protection Platforms found that only 55% of backup platforms have embedded cyberthreat detection of any kind today, with ransomware detection scores across the 12 evaluated vendors averaging 3.45 out of 5.

But even as those scores improve, the detection capabilities being built share a fundamental flaw that no score reflects: every one of them applies to backup copies and backup telemetry, not the live production environment where the attack is progressing. In the backup industry, breach is assumed, and recovery is the product. Here is what that looks like in practice:

Append-only immutable filesystems that write backup data in a format that cannot be overwritten or deleted at the storage level:

- Immutability protects data blocks but not the management plane. An attacker with stolen admin credentials simply changes the retention policy from years to hours and lets the automated purge do the rest.

Cyber deception technology that plants fake credentials, decoy files, and honeypot systems to detect attackers during reconnaissance before encryption triggers:

- The closest any backup vendor gets to detecting an active attack in progress. It still depends entirely on the attacker touching a honeypot, and sensors only cover environments the backup platform already manages. Legitimate credentials used against real assets generate no signal.

Inline entropy analysis and YARA rule scanning during the backup process to detect file-level anomalies suggesting encryption has already occurred:

- By definition, this fires after files have been encrypted in the production environment. It identifies which backup copies are clean. It does not stop the attack.

Ransomware recovery warranties offering financial coverage if backup data cannot be restored following an attack:

- These cover recovery costs when backup data cannot be restored. They do not cover exfiltrated data, regulatory fines, business interruption beyond sublimit thresholds, or reputational damage. They are financial instruments for the aftermath of a successful attack, not evidence that the attack was prevented.

Air-gapped vaults and cleanroom recovery environments that store an isolated copy with no network connectivity and validate data integrity before returning systems to production:

- Both are useful recovery tools, but neither addresses what happened in the production environment. If attackers spent weeks inside the environment before triggering encryption, vault copies may already contain compromised data or dormant malware captured during dwell time. Restoring from a poisoned vault copy reintroduces the attacker alongside the data.

While these investments represent meaningful progress in making backup recovery more reliable and trustworthy, none of these features address the weeks of downtime, the data already exfiltrated, or the business disruption already incurred. They make the backup safer. They do not make the business more resilient.

Halcyon: Recover in Minutes Not Weeks Without Relying on Backups

Backup is a necessary component of data protection, but it is not a ransomware strategy on its own. The organizations that recover fastest are not those with the fastest restore speeds. They are those who stopped encryption before it spread, protected backup infrastructure from tampering so a clean restore point is always available, preventing data exfiltration before it can be leveraged, and had expert-led response capability ready to manage recovery the moment an attack was detected.

Halcyon is built exclusively to defeat ransomware. It detects ransomware before it reaches backups, reverses encryption as it occurs, and captures key material to recover affected files in minutes.

When an attack does occur, the Halcyon Ransomware Operations Center (ROC) is the difference between recovery measured in minutes or hours and recovery measured in weeks or months. The ROC provides 24/7 expert-led detection, investigation, and recovery at no additional cost, meaning organizations have a dedicated team managing the response the moment an incident is detected through full restoration of operations. Attackers plan for your backups to fail. Halcyon ensures your business does not go down. Ready to see what ransomware resilience actually looks like?

Ransomware is a business problem.
Resilience is the answer.

See what that means for your organization.

halcyon