COHESITY

WHITE PAPER

# 5 steps to strengthen ransomware resilience for midsize businesses

A practical guide for lean IT and security teams to prepare for cyberattacks and recover from them quickly and securely.

# TABLE OF CONTENTS

# Executive summary

Midsize businesses are dealing with the same ransomware, data loss, and compliance risks as large enterprises, but with fewer people and tighter budgets. For these organizations, ransomware resilience isn't just about stopping attacks. It's about keeping the business running, recovering cleanly, and preventing one incident from turning into weeks of disruption.

A May 2026 Cohesity **report** presents survey results from nearly 1,000 IT and security operations decision makers at midsize organizations. The findings confirm what many security leaders already suspect: surviving ransomware today depends less on prevention and more on the ability to recover safely and rapidly.

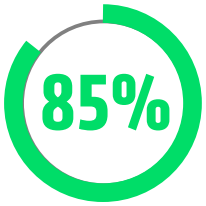

have experienced at least one material cyberattack


were hit within the past 12 months

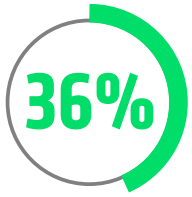

were hit more than once in that same period

Most midsize organizations don't have dedicated teams for backup, security, identity, compliance, and recovery planning. Often, one or two administrators often cover all of it. When those teams rely on disconnected tools across SaaS, on-premises, and cloud workloads, attackers gain the advantage through gaps, blind spots, and slow manual recovery processes.

And the damage is real. Among organizations that experienced a material attack:

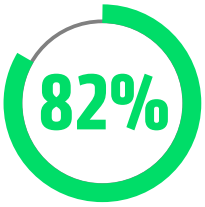



lost revenue




lost customers


faced legal or regulatory consequences




paid a ransom in the past 12 months (avg. $1.3M)

Part of the problem is where the budget goes. Most midsize organizations still weight their cyber spending toward prevention and detection: the **Identify, Protect, and Detect** functions of the NIST Cybersecurity Framework, while **Respond and Recover** consistently receive the least investment.

Prevention will never be perfect. The organizations that come out ahead treat response and recovery as seriously as they treat defense.

That's why we built the **Cohesity 5 Steps of Cyber Resilience**©, a practical framework that takes a midsize IT and security team from wherever they are today to a state where an attack is survivable, not an existential threat. Each step addresses a distinct challenge; together, they provide the highest levels of ransomware resilience.

1. Discover and protect all data
2. Ensure data is always recoverable
3. Detect and investigate threats
4. Practice application resilience
5. Optimize data risk posture

None of these steps require an enterprise-sized team or budget. What they require is a deliberate platform-and-process approach that reduces tool sprawl, removes manual guesswork, and helps a lean team recover with confidence when ransomware puts the business under pressure. Let's walk through each one.

*Ransomware recovery is not disaster recovery. In a fire or an outage, you know the root cause and can rely on your disaster recovery plan to get back online. In a ransomware attack, you need to investigate the root cause and the extent of the impact while an adversary is actively working against your recovery, and the systems you'd normally use to investigate or recover may be compromised themselves.*

# Step 1
# Discover and protect all data

The first problem many midsize businesses face is simple: they don't have one clear view of where their data lives. It may sit across Microsoft 365, Salesforce, virtual machines, NAS shares, cloud workloads, and identity systems. With lean teams and limited governance resources, data sprawl quickly turns into ransomware exposure. Every unprotected workload, forgotten file share, or unmanaged identity system is another place where an attacker can gain a foothold.

The first step is to discover and protect all data. For a midsize business, that means consolidating protection across the environments the organization actually runs on, then identifying sensitive data before attackers do. It also means protecting identity systems, such as Active Directory or Entra ID, because recovery breaks down fast if users, admins, and access controls can't be restored reliably.

## What good looks like

- A single data platform that can protect virtual machines, SaaS applications, databases, and unstructured file data, instead of five different tools for five different environments. This lets a small team operate a large data estate without hiring to match its size.
- Data Security Posture Management (DSPM) that automatically discovers and classifies sensitive data wherever it lives, so you find the risk before an attacker does, not after.
- The same protection discipline extended to identity infrastructure like Active Directory, often the first thing attackers target and among the last to be fully restored.
- Protection that keeps pace as new data sources appear, including business data that AI assistants create, summarize, or surface within Microsoft 365 and other SaaS applications. This way, newly generated or newly exposed information doesn't remain outside backup and governance policies by default.

### Why it matters

- Shrinks the attack surface instead of just monitoring it.
- Gives a lean IT team one place to manage data protection instead of many.
- Surfaces the sensitive data you didn't know you had, before it becomes a breach headline.
- Lowers total cost of ownership and improves ROI from existing IT resources.

## Step 2

# Ensure data is always recoverable

Having backups isn't the same as having recoverable backups. Many businesses assume that if backups exist, recovery is covered. But attackers increasingly target backup infrastructure itself. Your backup is your last line of defense. If it becomes compromised, you'd lose your leverage, and paying the ransom could become your only option.

Assuming "we back things up" means we're protected is a common mistake. Many businesses only discover the gaps mid-incident, when it's too late to fix them. Maybe the backup admin account had no multifactor authentication required for critical actions. Maybe the most recent clean recovery point was quietly compromised weeks before anyone noticed.

That's why the second step is to ensure data is always recoverable. For midsize organizations, this means hardening the platform with strong access controls and cyber vaulting so protected data can't be easily altered, encrypted, or deleted. It also means keeping enough recovery history to search for clean restore points when the most recent copies may already be affected.

## What good looks like

- Multifactor authentication, role-based access, and multi-person approval required for any sensitive backup or recovery action, no single compromised credential should be enough.
- Immutable backups secured with DataLock, our implementation of WORM (Write Once Read Many). Backup snapshots can't be altered or deleted, even by someone with admin credentials, until the WORM policy expires.
- A logically air-gapped cyber vault holding an isolated copy of your most critical data, completely separate from your production environment.
- A retention window long enough that you can find a verified clean recovery point from before the infection, not just your most recent, possibly compromised, backup.

### Why it matters

- Strengthens protection against attacks.
- Gives you a real choice for recovery instead of a forced one.
- Builds in the audit trail regulators and cyber insurers increasingly expect to see.

# Step 3
# Detect and investigate threats

Fast recovery without investigation is risky. If teams restore data without understanding what happened and without eradicating threats, they can reintroduce persistence mechanisms, vulnerable configurations, or infected files. This starts a cycle of attack, recovery, and reinfection. A smaller team can't do it all alone, and shouldn't try to. Knowing when to bring in outside incident response expertise is itself part of a mature incident response strategy, not an admission of weakness.

The third step is to detect and investigate threats. When production systems are compromised, backup data may be the safest source of truth for investigation and clean recovery. For midsize organizations, this means extending visibility beyond production systems and into backup data, where attackers often assume nobody is looking. At Cohesity, we recommend reviewing any abnormal changes in backups, scanning backup data for known threats, and using advanced investigation techniques when an incident is underway. Together, these steps strengthen incident investigation and confirm that backups are clean before they're restored.

## What good looks like

- Continuous, proactive scanning of backup data for anomalies and known malware, running in the background to support investigations when production systems or detection tools are unavailable. This ensures threats are identified and eradicated before clean data is restored to production.
- A safe way even for a generalist admin to identify a suspicious file and share it, along with other relevant metadata, with their SOC team for further investigation.
- Threat intelligence integrations that put IT and security teams on the same page, looking at the same data, without needing separate tools to reconcile.
- A relationship with expert incident responders established before an attack, so getting help doesn't mean starting from zero when the clock is already running.

### Why it matters

- Catches threats hiding in the one place most teams forget to look.
- Cuts investigation time. Every hour of downtime has a real dollar cost, so faster investigation means faster recovery.
- Aligns IT and security around one source of truth instead of two conflicting ones.

# Step 4
# Practice application resilience

One of the biggest mistakes organizations make is overestimating their readiness for a cyberattack, until a real one hits. Nearly half of cybersecurity leaders express confidence in their resilience strategies, but real-world incidents reveal a different reality. Under pressure, manual recovery steps, undocumented dependencies, and unclear priorities create chaos. The fourth step makes sure your response actually works under pressure. The first time your team executes the recovery plan should never be during a real attack, with the business down and leadership asking for hourly updates.

For a midsize team, this step is often the difference-maker. A lean team can't afford to spend resources on a chaotic recovery, which is exactly why rehearsed, automated recovery matters more, not less, when you have fewer hands on deck. Orchestration reduces manual recovery, validates dependencies, and helps lean teams repeatedly test without disrupting operations.

## What good looks like

- A defined Minimum Viable Company (MVC): the specific identity systems, infrastructure, data, and applications your business needs to function, and the exact order they need to come back online. All of this is worked out ahead of an incident, not improvised during one.
- A digital jump bag™: credentials, configurations, and trusted tools stored outside your primary environment, prepared ahead of an incident. Your jump bag is critical for initiating incident response, so your own responders aren't locked out of the recovery process by the same attack they're responding to.
- Recovery workflows that run on their own once triggered, so your team isn't hand-executing dozens of steps in the right order under pressure.
- `An isolated recovery environment or clean room where the investigation can take place safely, without touching production, and where systems can be verified as free of threats before returning them to production. This practice helps break the attack-recover-reinfect cycle that traps so many organizations.

### Why it matters

- Turns recovery time objectives from a hopeful estimate into a tested number.
- Removes single points of failure: recovery doesn't depend on one person's memory or availability.
- Cuts the risk of the single most demoralizing outcome: recovering, only to get reinfected.

# Step 5
# Optimize your data risk posture

Ransomware resilience isn't finished once backups are protected and recovery is rehearsed. Data keeps spreading across SaaS, cloud, edge, and on-prem environments. That makes it harder to know what data is sensitive, where it resides, and whether it's protected appropriately.

The fifth step is to optimize your data risk posture. For midsize organizations, this means continuously discovering and classifying data, aligning protection policies to the value and sensitivity of that data, and being able to answer urgent questions quickly after a breach.

This step is also where your response to a breach either holds up or falls apart. The first questions from a regulator, a customer, or your own board will be about exactly what data was involved.

## What good looks like

- Ongoing discovery and classification of data across your entire environment: what exists, where it lives, how sensitive it is, and what protection level it currently has.
- That same classification extended to your backup estate, not just production, so you have all sensitive data protected.
- The ability to answer, quickly and confidently, the questions that follow a breach: What data was impacted? How sensitive is it? Which customers or records were affected?

### Why it matters

- Finds hidden risk before it becomes an incident.
- Turns "we're not sure yet" into a fast, defensible answer when regulators, customers, or your board are asking.
- Makes compliance a byproduct of good data hygiene instead of a separate, manual scramble.

# Resilience is a system, not a single purchase.

No single step works well on its own. Protecting your data doesn't help much if it can't be recovered and you can't prove recoverability to your leadership, board, and regulators. Recoverable backups don't help if a threat re-enters the moment you restore. And none of it matters if you can't tell your board, your regulator, or your customers what actually happened. Taken together, though, the five steps do something money and headcount alone can't guarantee: they turn "we hope we're ready" into "we know we're ready."

Commercial organizations do not buy cyber resilience because the framework is elegant. They invest because downtime is expensive, recovery confidence is low, and one attack can disrupt revenue, customers, operations, and trust.

A strong cyber resilience strategy helps midsize businesses achieve four business outcomes:

1. Less operational complexity for lean teams through consolidation and centralized management.
2. Stronger protection across the full environment, including SaaS, cloud, on-prem, and identity systems.
3. Faster, more confident recovery with less risk of reinfection.
4. Better control over cost, risk, and business continuity.

For a security leader at a midsize business, the goal isn't to replicate an enterprise security operation. It's to get the outcomes that the Cohesity 5 steps of Cyber Resilience© framework produces: improved recoverability, reduced downtime, and continuous risk visibility. All of it comes through a platform sized and priced for the team you actually have, not the team you wish you had.

That's the thinking behind Cohesity Essentials: enterprise-grade ransomware resilience, built around the same Cohesity 5 Steps of Cyber Resilience© framework, without the enterprise complexity or overhead. It's available as M365, Virtual Edition, or Appliance, depending on how your environment is built. Whether your data lives on-prem, in the cloud, or across Microsoft 365, it gives a lean team one unified way to protect it, vault it, monitor it, and, if the day ever comes, recover from it with confidence.

**Learn more at Cohesity Essentials**



COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000105-001-EN 8-2026