COHESITY

HEALTHCARE

BUYERS GUIDE

AN IT LEADER'S GUIDE TO EVALUATING CYBER RESILIENCE SOLUTIONS FOR HEALTHCARE

Make the right choice to protect patient data, prove compliance, and recover to a trusted state—when, not if, an attacker gets in.



Why so much depends on your cyber resilience solution

When ransomware hits a hospital, the outage doesn't stay in the data center. Instead, surgeries slip, ambulances divert, and clinicians are forced to revert to pen and paper.

In healthcare, a cyberattack is a patient-safety event. Recovering data isn't the same as recovering care. Backups alone can't protect patients. And lean IT teams must manage these high stakes with auditors, insurers, and regulators already asking for proof.

The cost of cyberattacks in healthcare

78%	**healthcare organizations have experienced a material cyberattack in the past 12 months, up from 66% in 2025.[1]**
85%	**missed their recovery target.[1]**
16%	**have a tested plan to keep care running mid-attack.[1]**
97%	**faced legal or regulatory fallout after an attack.[2]**
2%	**view their current plans as equipped for AI driven attacks.[1]**
6.64M USD	**The global average cost of a data breach in healthcare.[3]**

> You can't stop every attack.
> But you can choose a solution that keeps care moving despite one.

The real question isn't whether a vendor can back up your data. It's whether they can bring care back fast after you're hit. This buyer's guide helps you tell the difference.

Learn what to demand, what to ask, and what to walk away from. Use the guide to choose a solution that protects patient care, not just data.



Beyond backup tools: 5 problems your solution needs to solve

Avoid this common mistake when evaluating a solution: treating cyber resilience as a backup problem. It's so much more than that. In healthcare, the job is to get care up and running after a destructive attack, a challenge that backup tools weren't built to handle.

Here are five problems your solution must solve—and why the wrong solution leaves them unaddressed.

The problem	Why it persists
"Attackers go after my backups first."	Modern ransomware targets the recovery layer on purpose. Encrypt or delete your last clean copy and paying looks like the only way out. That's why 94% of healthcare organizations pay a ransom when hit, averaging $1.3 million.1 Your last line of defense is now the front line.
"Restoring data isn't the same as restoring care."	You can restore a records system and still not resume care. After all, a care pathway includes records, connected devices, monitoring and alerting. Further, some EMR customers keep an isolated recovery environment that's live in minutes, but it's a bridge, not a destination.
"They break identity first, and it's the hardest workload to rebuild."	Most attacks run through Active Directory, Entra ID, or Okta. Bring identity back dirty and everything downstream comes back compromised. Active Directory Forest Recovery is specialist work, not "just another workload."
"I can't prove we'd actually recover."	The existence of backups is not proof of resilience. Only 16% of healthcare organizations1 have a documented and tested recovery baseline. Auditors, regulators, and cyber insurers now want evidence, not a signed attestation.
"My data is everywhere and my team is small."	Clinical and operational data sprawls across EHRs, imaging, databases, NAS, and SaaS, on-prem, and cloud. A lean IT team has to protect all of it, often with legacy tools.

Address all five problems and you have real resilience. Miss one and you have a false sense of it.

Define your Minimum Viable Company first

Before you choose a solution to protect your ealthcare organization, you must decide what essentials it can't go without: the core services, systems, and data that are critical to serving patients. Determine what's mission-critical to keep your organization up and running. Then, make this an operational capability that's the foundation of your resilience strategy. We call this your Minimum Viable Company (MVC).

With an MVC properly defined and operationalized, a health system can restore its most important clinical services to a trusted state, even when systems, records, and identities have been compromised. Prioritize your MVC before a crisis, so you're ready to respond and recover quickly when a real attack hits.

What belongs in your Minimum Viable Company

Every organization defines its essentials differently. Start here, and ask which of these your solution can recover first, fast, and to a trusted state:

- **Communications:** Nurse call, code blue/secure messaging, paging, telephony, and the downtime communication plan are what keep care running while IT rebuilds.
- **Identity:** Active Directory, Entra ID, Okta. The keys to everything else, and the first thing attackers take.
- **Core infrastructure:** Networking configurations, operating systems. The foundation that keeps care running.
- **EHR platforms:** Epic, Oracle Health, MEDITECH. The patient records, orders, and medication lists clinicians can't treat without.
- **Clinical services:** Protect the data, configurations, and infrastructure that power imaging, labs, connected devices, monitoring and alerting, on-call paging. These essential services decide whether care resumes.
- **Proof and evidence:** Proof of incident response and service recovery. The evidence regulators, auditors, and cyber insurers expect.

How it changes the way you buy

Once you define your Minimum Viable Company, you stop grading vendors on how fast they boot one VM and start grading them on how fast they bring your MVC back—in a trusted state that keeps care running.

> Even when protection fails, care can't stop.

What "good" looks like in a solution

Before you compare vendors, determine what constitutes a "good" cyber resilience solution. In healthcare, the bar isn't a list of features. It's a recovery operating model decided and tested before a crisis hits, not during one. It's whether care resumes quickly while an attack is underway. Here are the eight marks of a solution built to bring patient care back to a trusted state fast.

1. Protection for your whole clinical estate, EMR included

Your data does not sit in one place. It lives in EHRs, medical imaging, databases, NAS, SaaS apps, and your identity systems, spread across on-prem and cloud. A solution built for healthcare protects all of it from one platform—and that starts with your EMR. Ask for named support, not a vague promise to "cover most workloads."

2. A bulletproof cyber vault

Attackers hunt your backups before anything else. They know if they encrypt, alter, or delete your last clean copy, you pay. A bulletproof cyber vault takes that power away. Look for immutable, air-gapped copies that hold even when an attacker owns your domain admin, with WORM storage, hard isolation from the rest of the backup tier, and cryptographic checks that prove the data is untouched. If your vault folds once the adversary gets inside, you don't have a vault. You have another target.

3. Breadth and depth of threat scanning

You can't recover care if you can't see the threat. Breadth means the solution scans across file types for every source it protects–VMs, databases, NAS, SaaS, identity. Depth is what it finds: anomalies, malware, hash-based hunting, threats that evade signature-based tools, and indicators of compromise—all based on the latest threat intelligence feeds. Shallow scanning misses the payload that reinfects you on day three. Demand both reach and rigor.

4. Clean room automation

When systems are down and the clock is running, you can't afford to hand-build a recovery environment. Clean room automation hands your team a trusted, isolated space in minutes—a place to conduct forensics and remediate threats before you restore anything back to production. Investigate first. Recover second. A recovery that skips this step restores the attacker along with the data.

5. Identity-first recovery with automated ADFR

Identity is the first domino. Nine of 10 attacks run through Active Directory, Entra ID, or Okta, and if you bring identity back dirty, everything downstream comes back compromised. "Good" means automated Active Directory Forest Recovery (ADFR), a full-forest restore, decoupled from the operating system so malware and backdoors stay out. Recover identity first, back to a trusted state, and the rest of your recovery stands on solid ground.

6. Speed of trusted recovery

Speed on its own is a trap. A quick recovery that drags the attacker back in triggers re-infection that costs you time and money. What you want is the speed of trusted recovery—orchestrated, parallel restores measured against the clock that matters: how fast patient care comes back, not how fast a single workload boots. Measure the recovery time of a full care pathway: records, connected devices, monitoring and alerting. That number is your real RTO.

Score every vendor against one question: When the worst day comes, does care come back fast?

7. Proof you can hand auditors, regulators, and insurers

Having backups no longer proves you can recover. Auditors, regulators, and insurers now want evidence, not a signed attestation. They test for two things. First, proof of incident response: The recovery stripped out the attack surface and the persistence the attacker left behind.
Second, proof of service recovery: The full care pathway came back, not just workloads. A "good" solution lets you rehearse an entire recovery on demand, without touching production, and hand over evidence. The rules behind this standard vary by region (see the sidebar, Which rules apply to you?), but the bar is the same. The right vendor provides proof, not promises.

8. A total cost of ownership you can carry

Most healthcare IT teams are small and stretched. Weigh total cost of ownership on two fronts: the cost of the solution, and the load on your people. A solution that needs a dozen specialists to run is a cost, not a control. One platform that covers data and identity, with global deduplication and compression to shrink your storage bill, beats a stack of point tools you can't staff. And keep in mind the biggest line item nobody puts in the spreadsheet: the cost of downtime while patients wait.

Which rules apply to you?

Two frameworks carry most of the weight. Everywhere else, the ground shifts by country.

Region	Rule	What it requires
United States	**HIPAA Security Rule**	Administrative, physical, and technical safeguards for protected health information, including risk analysis, contingency planning, and data backup standards.
Europe	**NIS2 Directive**	Mandatory incident notification and cyber risk management measures for essential entities, including healthcare providers.

Questions to ask every vendor

Bring these to every vendor on your shortlist. Push for live demos, references, and documentation—not roadmap promises. A strong answer shows you. A weak one talks around you.

Protection and the vault

- Do your backup copies stay immutable even after an attacker gains domain-admin rights?
- What keeps the vault air-gapped and walled off from production?
- Do you protect EMR systems, or do you "cover most workloads"?
- Can one platform protect EHRs, databases, NAS, SaaS, and identity across on-prem and cloud?

Identity

- Do you recover Active Directory, Entra ID, and Okta—and in what order?
- Do you run automated Active Directory Forest Recovery (ADFR), decoupled from the operating system?
- How do you prove the identity you brought back is in a trusted state?



Detection and trusted recovery

- Do you scan our backups for anomalies, malware, and indicators of compromise? And do you check them against file hashes and live threat intelligence?
- How do you help us investigate before we recover, so we don't restore the attacker?
- How fast can we stand up a clean room, and how much of it runs without hands on the keyboard?
- How do you help me quickly identify what data was exfiltrated during an attack?

Speed and orchestration

- Show me a full recovery of a care service—records, devices, monitoring, on-call—not a single VM.
- Can you recover our critical care pathway in under a day? What did that look like for a customer our size?
- Can you orchestrate parallel restores, or does my team run it step by step under pressure?

Proof and compliance

- Can we rehearse a full recovery on demand?
- Can you produce the evidence an auditor or cyber insurer will ask for—proof of response, not just a restore log?
- When an attacker gets in, can you tell us which records they touched, so we notify patients and regulators with the right facts, on time?
- How do you support a documented, complete risk analysis?
- How do you help me lower my cyber insurance premiums?

Cost and fit

- What does it take to run this with the team we have today?
- What is the three-year total cost of ownership—license, storage, and staff time?
- How much do deduplication and compression cut from our storage bill?

One test cuts through every pitch: make them show you, on your data, with your people in the room. Ask them about their 24x7 incident response team. The vendor who can't demonstrate it now won't deliver it at 3 a.m.

Red flags in a vendor

Some answers should end the conversation. Watch for these red flags:

No identity-first recovery

If Active Directory, Entra ID, and Okta don't come back with automation into a trusted state, everything you rebuild on top is suspect.

No digital jump bag™

Without an essential cache of mission-critical data and files as part of your Minimum Viable Company, you increase your risk and prolong your recovery times.

Limited threat scanning

If you can only scan for malware on certain data types or file sizes, you have blind spots that increase your risk.

No way to rehearse or prove recovery

If you can't test a full recovery on demand and hand an auditor or insurer the evidence, you don't have resilience. You have a hunch.

An emphasis on "clean" rather than "trusted"

Clean recovery refers to an absence of malware. If the attacker got in using a vulnerability or leaked credentials that are still available in restored systems, you haven't removed the source of the attack.

Spot one of these, ask harder questions. Spot two, keep walking.

Vendor scorecard

Use this scorecard to compare your shortlist side by side. Score each capability from 0 to 5. A high score means the capability is present and proven—automated, built for scale, and ready today. See **How to score** for details.

Score what a vendor can demonstrate now, not what sits on a roadmap. Validate each score with product demos, customer references, documentation, deployment requirements, and proof of integration depth.

Capability	Vendor 1	Vendor 2	Vendor 3	Notes
Bullet-proof cyber vault: immutable, air-gapped, survives domain-admin compromise				
Full clinical estate coverage, including Epic				
Breadth and depth of threat scanning				
Clean room automation—investigate before you recover				
Identity-first recovery with automated ADFR				
Speed of trusted recovery, measured by care-service RTO				
Proof and compliance evidence: rehearsal on demand, auditor-ready				
Total cost of ownership a lean team can carry				
Total				

Score	What it means
5	Best-in-class. Fully delivered, automated, proven at scale.
4	Strong. Solid capability with minor gaps.
3	Adequate. Meets core needs but limited in depth, scale, or ease of use.
2	Basic. Partial support, notable gaps, heavy manual effort.
1	Minimal. Early-stage or heavily constrained.
0	Not supported, or no real evidence provided.

Add up the columns but trust the demos. A number on this page is only as good as the proof behind it.

The bottom line

No healthcare organization is safe from every attack. That's the point of resilience—the ability to take a hit and keep care moving. So judge every vendor by the outcome that matters: When the worst day comes, does care come back fast? Everything in this guide rolls up to that one test.

Cohesity Data Cloud is built for that test

An air-gapped Cohesity FortKnox vault keeps clean copies out of an attacker's reach. A Cohesity Clean Room Solution lets your team investigate before they recover, so you don't restore the threat. Cohesity Identity Resilience brings Active Directory, Entra ID, and Okta back first. Cohesity Data Cloud rebuilds systems fast, and DSPM tells you which records the attack touched so you notify with confidence.

What success looks like

Healthcare organizations around the world trust Cohesity. Here's what it looks like when a cyber resilience solution does its job

- When ransomware encrypted **Sky Lakes Medical Center's** backups alongside production, its team recovered patient records from a Cohesity clean room—no ransom paid, no patient data compromised.
- Instead of running a 24-hour full restore on a 6 TB virtual machine, the **UK's Stockport NHS Foundation Trust** used Cohesity global search to find and recover the one critical file it needed.
- At **Japanese Red Cross Maebashi Hospital**, every Cisco XDR threat detection immediately triggers a Cohesity DataProtect backup, so its team can restore clean, immutable data and keep Gunma's only advanced emergency center treating patients.

Your next steps

1. **Put your team to the test before an attacker does. The Cohesity Ransomware Resilience Workshop is a live attack simulation that pressure-tests your executive readiness.**

2. **See where your organization stands. Read the Healthcare Cyber Resilience Report to benchmark your cyber resilience plan against your peers.**

3. **Understand your potential gaps: Meet with a healthcare resilience specialist to map your security gaps.**

© 2026 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity Logo, and other Cohesity Marks are trademarks of Cohesity, Inc. or its affiliates in the US and/or internationally. Other names may be trademarks of their respective owners. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

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

Nov 2026 - BHD

Sources: [1]Cohesity, Healthcare Cyber Resilience Report, 2026 [2]Cohesity, Risk-Exposed: The Cyber Resilience Divide in Healthcare, 2026. [3]IBM, Cost of a Data Breach Report, 2026