COHESITY

AN EXECUTIVE'S GUIDE TO EVALUATING CYBER VAULTS

Executive summary: Why cyber vaulting is essential to cyber resilience

No company is immune from cyberattacks, so effective response and recovery are essential for every organization. Attackers will go to great lengths to force you to pay a ransom, even targeting the very systems intended to protect your data. Traditional backup strategies, designed to protect against hardware failures and natural disasters, do little to protect your organization against targeted, multistage cyberattacks. When ransomware strikes, backup copies of data that are connected to production networks can be encrypted or deleted, making clean, fast recovery nearly impossible. For IT leaders, it isn't a matter of if an attack will happen, but when. Is your organization ready to recover confidently when that attack does come?

As organizations like yours rethink how to protect and recover data, cyber vaulting has become a foundational part of a modern cyber resilience strategy. A cyber vault ensures you'll have an untouched copy of your data to recover when all else fails. Vaulting provides the separation, verification, and control necessary to guarantee clean, recoverable data, even in the face of destructive cyberattacks. That's why your peers are adopting cyber vaulting as an imperative for resilience.

The challenge: Cyber recovery is far more complex than disaster recovery

For years, organizations designed backup systems to address hardware failures, accidental deletions, and natural disasters. These systems often served their purpose well. But they aren't sufficient to secure and protect data against the destructive cyberattacks that dominate today.

As a result, a critical risk factor has emerged: backup data can be just as vulnerable as production data. Threat actors no longer focus solely on encrypting production data. They infiltrate backup repositories, disable snapshot schedules, plant malware, and corrupt metadata to eliminate recovery paths.

These risks exist even if you have a modern data protection platform in place.

Why your data estate is at risk

You may be thinking, "I have a secure data platform for all my backups, with all security add-ons enabled. Isn't that enough?" Short answer: No.

Such a platform reduces your risk and your attack surface significantly. But on its own, it doesn't eliminate exposure.

Here's why:

- **Shared connectivity**: Most backup systems remain connected to the production network. If that production environment is compromised, attackers already have a path to backup data.
- **Credential overlap**: Administrative credentials are often shared across environments. Once an attacker gains privileged access, they can delete or encrypt backups just as easily as production data.
- **False immutability**: Some "immutable" backups are only software-locked. If the storage control plane or API is breached, the immutability flag can be reversed.
- **Latent threats can remain**: Many organizations restore from backups without validating data integrity or scanning for latent malware, increasing the risk of reinfection during recovery.

The business impact

The result is a confidence gap: the perceived integrity of backup data is far higher than the reality. The negative consequences cascade:

- **Prolonged downtime**: Unverified or compromised backups extend recovery from hours to days or weeks.
- **Operational strain**: Teams spend time re-creating systems or data sets instead of executing recovery plans.
- **Compounding costs**: Each hour of downtime increases revenue loss, regulatory exposure, and brand damage.
- **Eroding confidence**: When IT can't deliver a fast, clean recovery, executive and board confidence in organizational resilience declines.

Cyber vaulting: Your last line of defense when all else fails

A cyber vault addresses this confidence gap. A cyber vault is a secure, isolated, and immutable repository that stores clean copies of critical data. The vault is deliberately disconnected from production networks and primary backup systems.

Adopting a cyber vault refreshes the 3-2-1 backup rule: keep three copies of data on two different media types with one offsite copy that's isolated and immutable.

In practice, organizations implement this modern backup rule as follows:

- **3 copies of data must be immutable:** Copies should be protected using write-once, read-many (WORM) or object-level locking, and continuously validated using AI-based anomaly detection and regular threat scans to confirm data is clean.
- **2 different media means storing data on two different platforms or trust boundaries:** Copies should reside on distinct systems that don't share the same control plane or attack surface. This may include combinations of disk, tape, or cloud storage designed for data isolation.
- **1 offsite copy must be isolated:** The final copy should be separated by a logical or physical air gap and protected by an isolated security model and third-party custodianship. This copy should also be protected with multifactor authentication (MFA), quorum, and data integrity checks.

Together, these advances transform the 3-2-1 rule into a foundational pillar of cyber resilience. The cyber vault serves as the final, clean recovery point for critical data. By combining immutability, isolation, diverse storage domains, and rigorous integrity validation, the cyber vault enables organizations to securely recover from destructive cyberattack—even in the worst-case scenario where your backup estate has been compromised.

Evaluating cyber vaulting solutions

When selecting a cyber vaulting solution, IT leaders should evaluate both security architecture and operational readiness. Based on feedback from hundreds of IT leaders, the following five pillars are critical capabilities:

1. **Isolation and access control:** Vault data should be unreachable from production networks. Look for enforced air gaps, independent identity domains, MFA, and quorum-based administrative approvals.
2. **Immutability and integrity:** Data must be tamper-proof, with WORM storage and retention lock policies that prevent modification or deletion—even by administrators.
3. **Automation and orchestration:** Vault replication, validation, and recovery should be automated. Policy-based orchestration reduces human error and accelerates recovery.
4. **Threat protection:** AI-based anomaly detection and malware scanning flags potential threats in snapshots to help ensure that only clean, uncompromised data is stored and restored.
5. **Compliance and reporting:** Immutable audit logs, encryption, and retention management should align with frameworks like NIST SP 800-209, ISO 27040, and DORA, to prove recoverability and resilience readiness.

Evaluation scorecard - Use this scorecard during your vendor conversations.

Instructions:

1. For each category, assign a score from 1–5 for each vendor, where 1 does not meet the requirement and 5 fully meets the requirement.
2. Multiply each vendor's score by the **Weight** for that category, and record the result in the corresponding Weighted Score cell.
3. For each vendor, sum all **Weighted Scores** down the column and record the total in the **Weighted Total** row at the bottom of the table.
4. Use the **Weighted Total** to compare vendors overall, and capture any qualitative observations or risks separately.

		Vendor 1		Vendor 2		Vendor 3		Vendor 4	
Category	**Weight**	**Score**	**Weighted Score**	**Score**	**Weighted Score**	**Score**	**Weighted Score**	**Score**	**Weighted Score**
Isolation / Air Gap	10								
Immutability / WORM	10								
Separation of Access Controls	10								
Strong Authentication (MFA / Quorum)	8								
Threat Detection / Anomaly	8								
Block Infected Snapshot Recovery	8								
Recovery Orchestration	8								
Clean Room / Validation	8								
Compliance / Auditability	8								
SaaS Simplicity / TTV	7								
Hybrid / Multicloud Flex	8								
TCO / Operational Overhead	7								
Weighted Total									

Modern cyber vaulting delivers measurable business outcomes:

- **Resilience**: A physically or logically isolated recovery copy that remains intact even when backup platforms are compromised.
- **Continuity**: Vaulted backups ensure organizations have a copy of data to recover, regardless of the scope of the attack.
- **Compliance**: Immutable storage and retention enforcement provide auditable evidence of data protection and recovery readiness.
- **Trust**: Recovery points are preserved outside the operational blast radius and can be validated before use, ensuring restored data is clean and uncompromised.

Cyber vaulting connects IT operations, security, and compliance, so when a crisis occurs, clean recovery is guaranteed, not a gamble.

From backup reliance to resilient recovery: Bethany Children's Health Center

Many organizations are integrating cyber vaulting as a standard component of their data protection strategy. One example is Oklahoma's Bethany Children's Health Center, which provides care for children with complex medical needs. To support uninterrupted care, the center must protect sensitive health data and restore it quickly in the event of a cyberattack or disaster. Bethany meets these requirements by storing immutable backups both on-premises and in Cohesity FortKnox, an isolated cloud vault.

For added resilience, Bethany follows the 3-2-1 principle, maintaining three copies of data on two different media, with one copy stored offsite. Two immutable backups are kept on-prem, with the third stored in Cohesity FortKnox.

Cohesity FortKnox provides a managed cyber vaulting service available for DataProtect and NetBackup environments, delivered across AWS, Azure, and GCP, and as on-prem solutions for the most secure environments. FortKnox combines isolation, immutability, and automation to deliver fast, clean, and verified recovery at enterprise scale.

FortKnox adds a new layer of defense: a secure, air-gapped vault that ensures critical data remains safe, compliant, and recoverable.

Next steps to assess your cyber resilience

Your resilience plan can't rely on assumptions that no longer apply. As cyberattacks grow more aggressive, business continuity increasingly hinges on the strength of your last, most secure copy of data. Cyber vaulting represents a proactive approach that strengthens cyber recovery and reduces downtime.

Start by assessing:

- **Do you back up SaaS, on-prem, and cloud data from all your data sources on a single, modern platform?**
- **Have you hardened your platform with MFA, immutability, and role-based access control (RBAC)?**
- **Do you adhere to the 3-2-1 backup rule?**
- **What isolation measures separate your backup data from production networks?**
- **How often do you scan your backups for threats?**
- **How often do you test your cyber response plan?**
- **During your last cyber response test, how quickly did you recover?**

Now is the time to elevate cyber resilience from a technical objective to a strategic imperative. Readiness—not assumptions—is the ultimate competitive advantage.

See how modern cyber vaulting can protect your data, strengthen your recovery posture, and provide the confidence to operate securely, no matter the threat. Learn more at https://www.cohesity.com/platform/fortknox/

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

4500065-001-EN 2-2026