September 2025

EBOOK

The CISO's Guide to Cyber-Resilient Storage

wasabi
hot cloud storage

FOREWARD

By Rob Black, CISSP — Founder & CEO, Fractional CISO

Resilience has become one of the defining challenges of the modern CISO role. It's no longer just about keeping attackers out; it's about ensuring your organization can recover quickly, maintain compliance, and continue to operate under pressure.

We spend a lot of time on identity, on network defense, on detection and response. All critical areas. But storage, specifically cloud object storage, hasn't always been part of the conversation. It should be!

The way we store and protect data directly shapes our ability to bounce back from ransomware, outages, or mistakes. Features like immutability, multi-user approvals for critical actions, and predictable costs aren't nice-to-haves. They're core to building a resilient organization.

That's why I'm glad to see this guide shine a light on storage as a key tool in the CISO's toolkit. It's an area too many overlook, but one that can make the difference between a smooth recovery and a business crisis.

Rob Black, CISSP
Founder & CEO, ***Fractional CISO***

We know, data storage isn't something you generally think about

Let's face it, you're a CISO. You're juggling threat intelligence, BCDR, compliance audits, and incident response drills. Data storage? Not exactly the stuff of epic cybersecurity tales. But hear us out, because storage might just become your new favorite cybersecurity secret weapon. (No, seriously.)

As a cybersecurity leader, you're caught in a perpetual balancing act of managing risk and fostering innovation—all while managing the people, processes, and technologies necessary to thwart the next attack or bounce back quickly.

In our opinion, Gartner® captures your reality perfectly in their Leadership Vision for 2025 report, where they list the top three strategic imperatives for CISOs.

PRIORITY 01 **Optimize for performance**

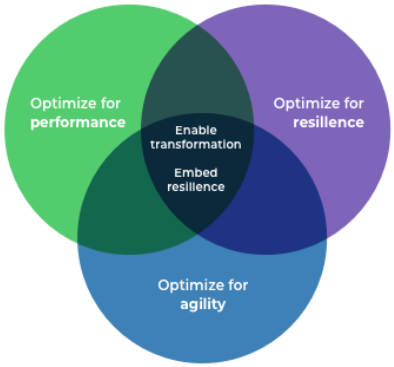
Performance is the ability to drive continuous improvement in the effectiveness and efficency of the cyber security program.

PRIORITY 02 **Optimize for resillence**

Resillence is the ability to resist, absorb, recover and adapt to business disruption in an ever-changing and increasingly complex environment and threat landscape to rebound and prosper.

PRIORITY 03 **Optimize for agility**

Agility is the ability to rapidly reprioritize the roadmaps and investments inherent in the cyber security strategy and program.



Source: Top 3 Strategic Priorities for Security and Risk Leaders – Gartner, Leadership Vision for 2025 report

While we believe we can also help you with numbers one and three, today we'd like to talk about resilience, the critical need for your organization to resist, absorb, and quickly recover from cyber attacks or other disruptions.

Because here's the thing: while most resilience plans focus on endpoints, identity and access management, network protections, and backup strategies, there's a critical yet often-overlooked piece of the puzzle—the storage your organization uses to house all its data.

Storage? Yes, really. More specifically, we're talking about cloud object storage, built from the ground up to be cyber-resilient.

The right storage can dramatically boost your ability to quickly bounce back and sustain operations after cyber incidents or data disasters. And, while storage itself might never be sexy, the security outcomes it delivers definitely are.

Intrigued? You should be. Because cyber-resilient storage has a direct impact on two things you care deeply about: incident response preparedness and regulatory compliance.

> *"Storage may not be exciting, but you know what is 'exciting'? A cyber attack! Great security practices minimize excitement."*
>
> - Rob Black, CISSP

What CISOs really care about

CISOs have a lot on their plate. While this list doesn't begin to cover the full scope of your responsibilities, these five priority areas probably take a good deal of your focus:

1. **Cyber resilience / Incident response preparedness**
   Resisting and absorbing attacks, responding quickly, and recovering faster to keep the enterprise running—whether facing ransomware, outages, or any other disruption

2. **Identity & access management / Zero Trust**
   Enforcing strict, continuous verification for every user and device, and eliminating implicit trust and minimizing opportunities for lateral movement

3. **Threat intelligence & detection**
   Staying ahead of adversaries by proactively identifying, monitoring, and responding to emerging threats—using credible intelligence before damage is done

4. **Regulatory compliance & governance**
   Navigating a complex and changing regulatory landscape while embedding audit readiness into everyday processes

5. **Endpoint protection (EDR/XDR)**
   Securing every device, workload, and application against compromise

While cloud object storage can't help with all of your priorities, the right provider can deliver meaningful advantage to three of them: cyber resilience, Zero Trust access, and compliance.

Cloud object storage. Yes, really.

Storage isn't usually the first thing CISOs think of when looking for quick wins in cyber resilience or compliance. If they think about storage at all. But that's exactly why it's worth a closer look.

When chosen wisely, cloud object storage can become a quiet force multiplier, shortening downtime after an incident, protecting the integrity of critical data, and making compliance audits far less painful.

Here's how cloud object storage stacks up against other storage types from a cyber-resilience standpoint:

- **File Storage** – Great for collaboration, not so great for immutable retention or massive scale.
- **Block Storage** – Fast for transactional workloads but lacks the built-in durability and cost-efficiency needed for large, long-term datasets.
- **LTO Tape** – A long-time staple for long-term retention and compliance archives, but too slow for rapid recovery and vulnerable to physical loss, damage, or theft.
- **On-Prem Object Storage** – Better durability, but still vulnerable to physical disasters, insider threats, and local network breaches.

So, why choose cloud object storage in particular? Because it eliminates many of these limitations, but only if it's designed with cyber-resilient features at its core: Zero Trust accessibility, virtual air-gapping, and a pricing model that encourages frequent testing and retrievals instead of punishing them.

Not every provider offers that combination. In fact, some hyperscalers make it cost-prohibitive to use the very features that strengthen resilience.

> ***"Storage is like the Clark Kent of cybersecurity. It may look ordinary, even boring. But in a cyber emergency, it suits up, steps out of the phone booth, and saves the day."***

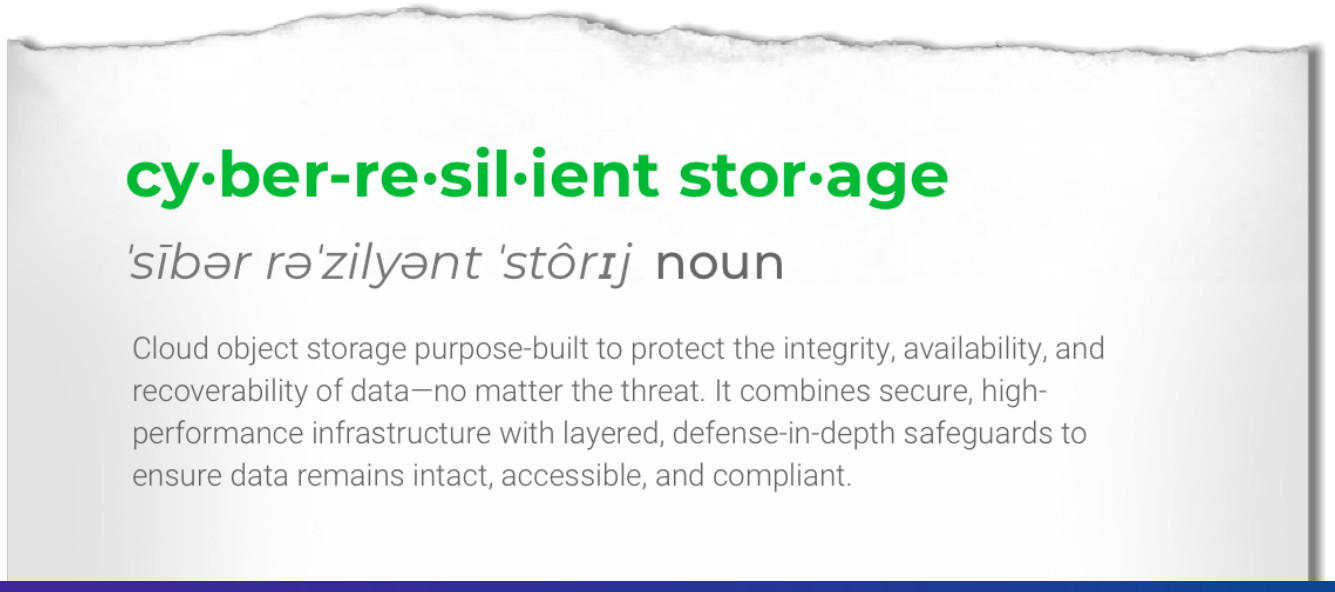
So what actually defines "cyber-resilient" storage? Let's break it down.

What is cyber-resilient cloud storage?

Your backup strategy is a critical part of your business continuity and resilience strategy. But here's the part that often gets overlooked: the storage target you choose is just as important as the backup up application or provider you determine best meets your objectives.

If your storage doesn't safeguard your data from tampering or loss, or is locked away when you need it most, then your resilience plan has a gaping hole in it.

That's why your storage target must be cyber-resilient storage.



The reality: Most cloud object storage solutions don't meet this standard, leaving critical security gaps.

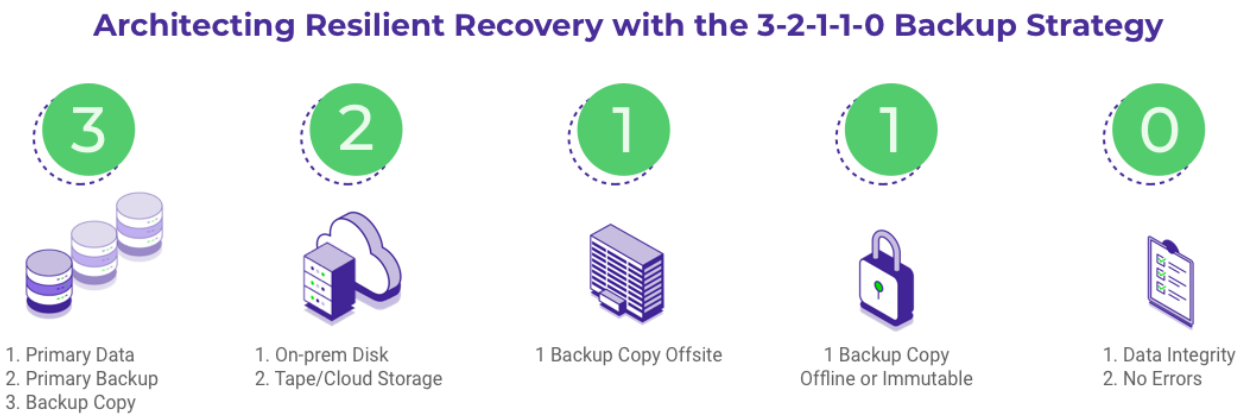
Key features of cyber-resilient storage

1. **Cloud object storage for 3-2-1-1-0 compliance** – Meets the gold standard for recoverability by keeping at least one copy safely offsite and immutable to changes, with zero errors after recovery verification.
2. **Zero Trust, defense-in-depth security** – Verifies every request for access and critical actions and locks data against tampering.
3. **High performance for fast recovery (RTO)** – Restores data quickly to minimize downtime.
4. **Cost-effectiveness for frequent backups (RPO)** – Enables more backups without budget strain.
5. **No fees for egress or API requests** – Frees you to test, access, and retrieve your data anytime without increasing total cost of ownership.

In the next sections, we'll break down each of these features and why they matter for your resilience strategy.

1. Cloud object storage for 3-2-1-1-0 compliance

As we already discussed, in order for storage to be cyber-resilient it must be offsite and separate from your primary storage or backups. One copy stored offsite is a key tenet of the 3-2-1-1-0 backup strategy, the "gold standard" for modern data protection best practices.



Cloud object storage is the ultimate offsite medium. It delivers the durability, scalability, and geographic separation needed, without the physical logistics and access tradeoffs of tape or offline drives. However, ransomware, insider risk, and reliance on an ever-growing SaaS ecosystem have made "offsite" backup alone insufficient. You also need immutability and automated recovery testing, which in turn validates data integrity.

This higher standard reflects the reality CISOs face today. Compliance, ransomware defense, and disaster recovery all hinge on backups that can be trusted to be both accessible and tamper-proof.

Not all cloud storage services meet this standard. Without immutability, multi-user approval for critical actions, and freedom from cost barriers that discourage testing, your offsite copy may not be as resilient as you think.

2. Zero Trust defense-in-depth security

CISOs have already embraced Zero Trust as a core security strategy. But too often, storage is left out of that equation. If data repositories aren't treated with the same level of scrutiny as networks or endpoints, they become a blind spot in an otherwise well-defended environment.

When it comes to cloud object storage, multi-factor authentication (MFA) should be considered a baseline requirement. Every provider should have it, and every organization should enforce it. But MFA alone only protects against unauthorized logins. It doesn't address the risk of a malicious insider or a compromised account with administrative privileges. That's where features like multi-user authorization (MUA) become critical.

Wasabi Multi-User Authorization requires approval from more than one authorized individual before sensitive actions like deleting storage buckets or even an entire cloud storage account can be executed. This ensures that no single set of credentials, no matter how privileged, can be exploited to cause catastrophic data loss.

Immutability adds an additional layer of security by ensuring that once data is written, it cannot be changed or deleted until its defined retention period has expired. This "write once, read many" safeguard creates a tamper-proof record of your backups. It also provides the kind of audit-ready assurance regulators increasingly expect. But not all providers make immutability practical to use. If cost or complexity prevents you from enabling it, your storage isn't truly resilient.

For organizations seeking a final layer of protection, cutting-edge security features enable them to create a hidden, "covert" copy of a storage bucket that remains invisible to everyone but the root user—and even then, only after multiple authorized security admins approve. It's the cloud equivalent of an **air gap**, without the delays or complexity of managing offline media.

It's important to note, while features like MFA and immutability have become common, advanced safeguards such as MUA and Covert Copy are not. Most providers don't offer simple ways to enforce multiple approvals for destructive actions or to hide critical copies of your data. These capabilities are offered exclusively by Wasabi and are designed to close the gap that Zero Trust, defense-in-depth principles are meant to address.

3. High performance for fast recovery (RTO)

How fast you can recover from an incident depends on the storage tier you choose. "Hot" object storage tiers such as Amazon S3 Standard, Azure Hot, Google Cloud Standard, and Wasabi Hot Cloud Storage are built for immediate access. Data stored here is always available, with no delays when you need to pull it back.

Cooler and archival tiers may look cheaper at first glance, but they trade performance for cost savings. Retrieval can take hours, not seconds, and in the middle of an incident, that delay is simply not acceptable.

And here's the kicker: those cooler tiers don't just slow you down, they typically charge much higher access and retrieval fees. So, what looked like a bargain on the front end becomes much more expensive—both in dollars and in downtime—when you need to recover your data.

For CISOs, the lesson is clear: cyber resilience demands hot storage. It ensures that your most critical backups can be restored quickly in order to minimize downtime, reduce exposure, and get back to business fast.

But...is it affordable?

4. Cost-effectiveness for frequent backups (RPO)

Resilience isn't just about speed; it's also about economics. If storage is expensive, it inevitably influences how much data you protect and how often you back it up. That trade-off directly impacts your Recovery Point Objective (RPO)—the amount of data you risk losing when systems go down.

The two biggest factors:

- Per-terabyte cost of your hot storage tier
- Ingress (PUT) fees for writing data into the cloud

Together, these determine whether frequent backups are affordable or cost pressures force you to stretch backup intervals and expose more data to loss.

> ***"Ingress and egress fees can get very complicated and expensive, especially if you need to restore objects across your organization."***
>
> - Scott Beven, Deputy Director of IT Delivery, Charles Darwin University

Put simply: cost-effective storage with no ingest fees makes it possible to capture more backups, more often, without blowing up your budget. That means less data exposure, stronger resilience, and better compliance with retention requirements.

5. No fees for egress or API requests that can weaken your cyber resilience

When most people think about cloud storage costs, they think in terms of dollars per terabyte. But with traditional cloud object storage, that's only part of the story. Every time you interact with your data, you may be triggering additional fees known as API request charges.

Here are some common examples:

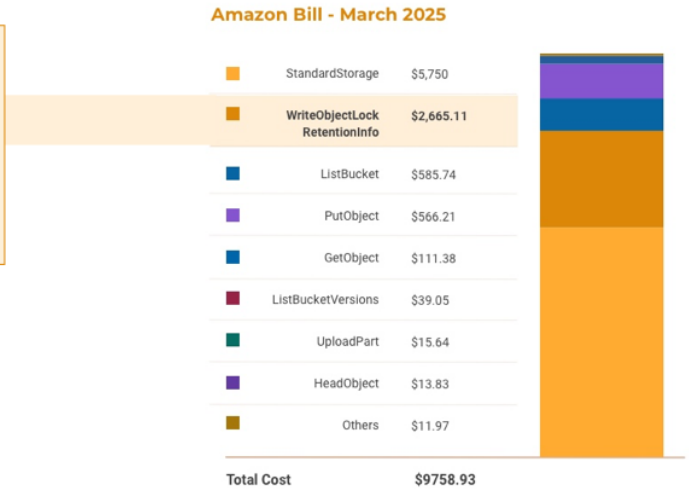
- **PUT Object –** Uploading an object into storage
- **GET Object –** Retrieving your stored data
- **COPY Object –** Duplicating data within or across buckets
- **LIST Objects –** Enumerating all the objects in a bucket (a routine step when verifying backups)
- **Upload Part –** Large files broken into smaller chunks for upload, with each part billed separately
- **HEAD Object –** Checking metadata or header information on an existing object

On the surface, these fees may look harmless—usually just a fraction of a cent per 1,000 requests. But in practice, they add up quickly. Backup software, for instance, may generate millions of these requests each month simply by verifying that data is intact. Multiply that across large datasets and frequent operations, and API request fees can account for nearly half of a cloud storage bill.

This real-world AWS bill illustrates the point: out of a $9,758 monthly charge for approximately 250 TB of data, more than $4,000 (41% of the total cost) came from API requests and retrieval fees, not storage capacity itself.

If fees discourage frequent backups, regular testing, or turning on essential security features, your resilience is compromised. That's why fee-free API requests and egress should be considered a core feature for any cyber-resilient cloud storage service.

Fees make setting retention periods for immutability cost prohibitive.



> *"Using Azure's cool and archive tiers gave us lower storage costs, but retrieval fees were much higher. We were getting hammered on that. Wasabi's flat rate with no fees eliminated that problem."*
>
> - Brian Supple, Technical Director, ProCloud

Storage outcomes that CISOs care about most

At the end of the day, cyber-resilient storage isn't about speeds, feeds, or individual features. It's about outcomes that support the priorities CISOs already care about.

- **Stronger resilience**
  Faster recovery times (Recovery Time Objectives, RTO) and more frequent backups (Recovery Point Objectives, RPO) mean less downtime, reduced financial impact or reputational damage, and fewer sleepless nights.
- **Compliance confidence**
  Immutable and audit-ready records simplify regulatory reporting and reduce the risk of penalties.
- **Reduced risk exposure**
  Storage designed for Zero Trust and defense-in-depth ensures critical data isn't the weak link in your security strategy.

Cyber-resilient storage doesn't just hold your backups. It is a core component of your organization's ability to withstand attacks, recover quickly, and adapt to new compliance demands.

Wasabi is cyber-resilient storage

The five key features of cyber-resilient storage that we've outlined aren't abstract. They're the foundation of how Wasabi is built.

1. Cloud object storage for 3-2-1-1-0 compliance

Wasabi cloud object storage is durable, scalable, and built for the 3-2-1-1-0 backup strategy by design. With full S3 compatibility and one of the industry's largest ecosystems of Technology Alliance Partners, Wasabi integrates seamlessly with every major backup provider. That makes it simple to implement best-practice frameworks without rewriting applications, reconfiguring workflows, or locking yourself into a proprietary stack.

2. Zero Trust and defense-in-depth security

Wasabi delivers the standard protections you'd expect—encryption in transit and at rest, SSO integration, and MFA—but goes further with its patented Multi-User Authorization (MUA) feature. Sensitive actions like bucket or account deletion require approvals from multiple admins, eliminating single-credential risk. Immutability is included at no extra cost, ensuring that once data is written, it cannot be altered or deleted during its retention period.

Covert Copy: Your last line of defense

Wasabi's new Covert Copy feature lets you create a hidden copy of a storage bucket that is virtually invisible and inaccessible to anyone except the root user. Functioning as an impenetrable copy of last resort, this unique feature requires immutability, MFA, and Multi-User Authorization to be enabled, so even the root user can't access a Covert Copy without full security admin team approval. It's like having an air-gapped backup that's available when needed, without the delays and costs of offline storage..

3. High performance for faster recovery

Wasabi Hot Cloud Storage delivers high performance on par with hyperscaler "standard" tiers but at a significantly lower cost. There's no need to compromise with colder tiers of service that delay recovery or add unpredictable and costly retrieval fees.

4. Cost-effectiveness for frequent backups

At a fraction of the cost of the hyperscalers, Wasabi makes it practical to back up more data, more often. That means less data at risk and stronger recovery points.

5. No fees for egress or API requests

With Wasabi, resilience isn't compromised by hidden costs. There are no charges for retrieving data, running DR drills, or turning on critical protections like immutability. Transparent, predictable pricing means you can back up, test, and access your data as often as needed without budgetary trade-offs.

Storage is no longer an operational afterthought. It's a strategic pillar of cybersecurity.

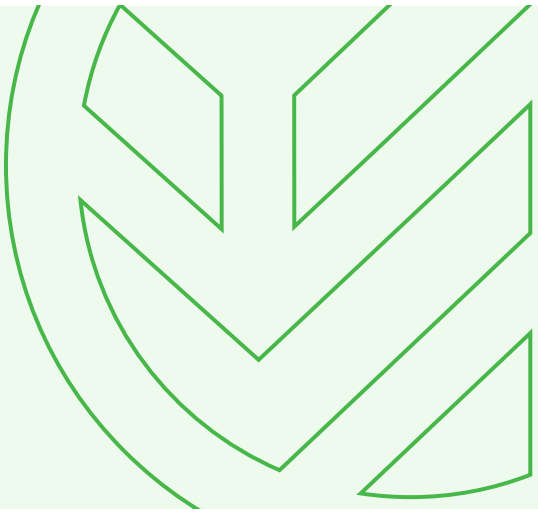
Cyber-resilient storage delivers the outcomes that CISOs care about most: faster recovery, less data loss, built-in compliance, and reduced risk exposure. When security leaders treat storage as a strategic business decision, the right choice can quickly become a core component of their cyber risk strategy—strengthening an organization's ability to withstand and adapt to disruption.

The bottom line: storage choices shape resilience. And resilience is exactly what CISOs are being asked to deliver.

Ready to strengthen your cyber resilience with a better storage strategy?

Your organization shouldn't have to choose between business resilience and your budget. With Wasabi, you don't have to.

Migrate 25 TB or more to Wasabi by December 31, 2025, and your migration is free. We'll even pay your hyperscaler egress fees! Visit **wasabi.com/migrate** to learn more.



ABOUT WASABI

Recognized as one of the technology industry's fastest growing companies, Wasabi is on a mission to store the world's data by making cloud storage affordable, predictable and secure. With Wasabi, visionary companies gain the freedom to use their data whenever they like without being hit with unpredictable fees or vendor lock-in. Instead, they're free to build best-of-breed solutions with the industry's fastest-growing ecosystem of independent cloud application partners. Customers and partners all over the world trust Wasabi to help them put their data to work so they can unlock their full potential. Visit wasabi.com to learn more.

Follow and connect with Wasabi on LinkedIn, X, Facebook, Instagram, and The Bucket.

wasabi
hot cloud storage

www.wasabi.com

1-844-WASABI-1
info@wasabi.com