Calamu™

SOLUTION GUIDE:

How to Improve Your Backup Data Security

Contents

Why Data Backup Has Become Synonymous with Data Security

Disasters happen all the time. Data is accidentally deleted. Earthquakes, fires, or floods damage critical infrastructure. And the most threatening disaster in recent years–a ransomware attack–can wipe out your entire production environment.

Backup is often considered the last line of defense to any of the above disaster scenarios. However, relying on backup to recover from ransomware is unique because there is an adversary with malicious intent trying to compromise your systems. Earthquakes don't deliberately undermine your layered defenses–hackers do.

How can you adapt your backup systems to operate more like a cybersecurity solution, while also being efficient, reliable, and cost-effective? That is the question this guide will answer.

NEXT UP **ASSESS YOUR CURRENT BACKUP VULNERABILITIES**

Using Backup for Ransomware Protection Requires Adaptation

If stored backups are being used to safeguard your production environment, the backup data itself needs to be very well secured.

Assess Your Current Backup Vulnerabilities

Backup workflows are a critical component to business continuity and disaster recovery. With well functioning and secure backup copies, you can restore from a ransomware attack and counteract the opposing party's leverage. So it should come as no surprise that backup repositories themselves are under attack. **In fact, 94% of ransomware attacks now target backup repositories before the hacker makes their presence known.**[1]

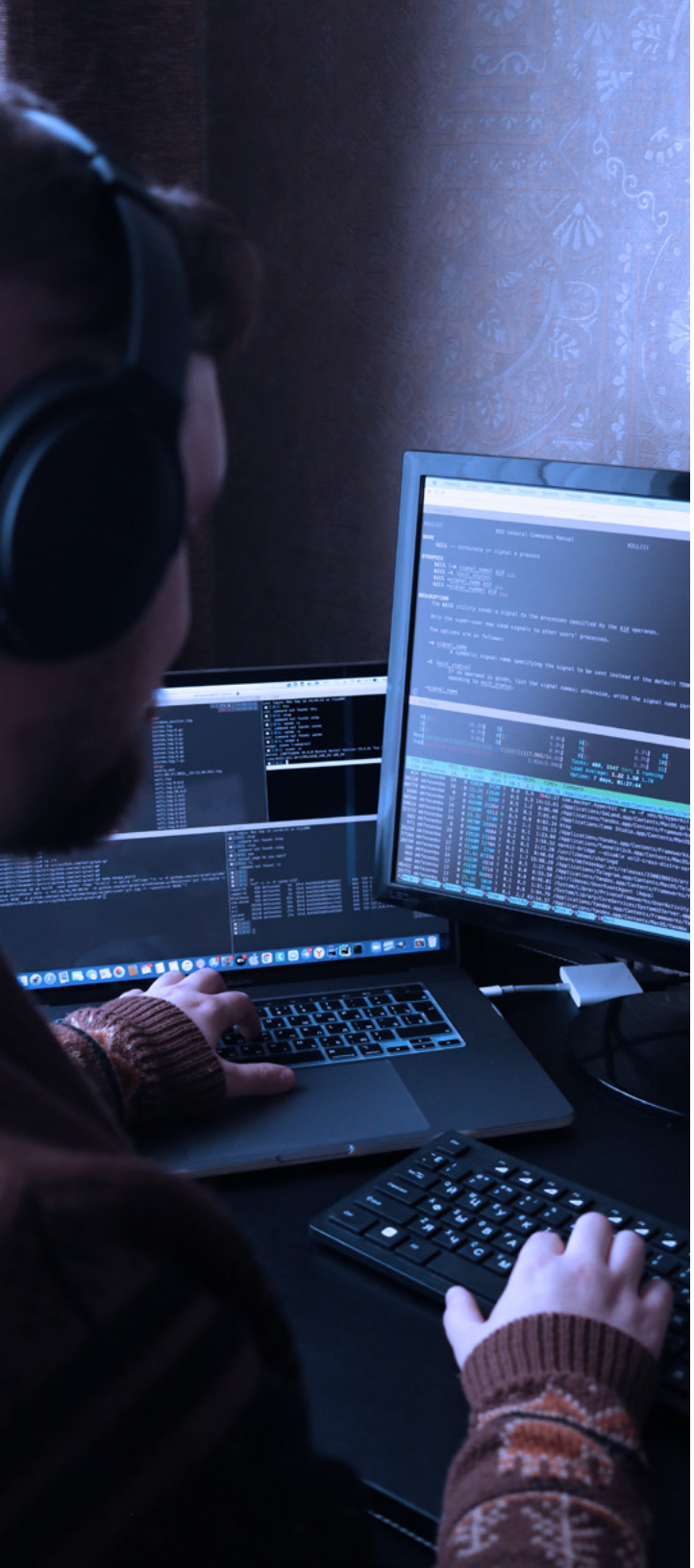
Sending backup copies to an **ultra secure, purpose-built storage repository** is becoming common practice for protecting data against ransomware and evolving threats like data theft and exfiltration. Adapting legacy backup workflows to include an additional, ultra secure offsite copy is an investment in the future of your business and can have an ROI in the many millions of dollars.

Consider these common threats and backup vulnerabilities:

- Software credential theft
- Malicious insider threats
- Misconfigured storage repositories or cloud environments
- Supply chain attacks and backdoor exploits (CVEs)
- Cloud outages or hardware failures

There are many ways that hackers can undermine defenses and gain control of your backup systems with the goal of incapacitating them or exfiltrating any sensitive data. Further, incidents like cloud outages or hardware failure can leave you stuck without the ability to restore when needed, resulting in costly downtime and downstream consequences. This may explain why in a recent poll of 100 IT executives, 89% said they're always on the lookout for better data protection solutions.

[1] 2023 Veeam Ransomware Trends Report



5 Questions to Assess Your Current Backup Data Security:

- [ ] 1. Have you taken steps to prevent backup data theft and exfiltration?
- [ ] 2. Do you have controls to prevent malicious encryption or deletion of backup data?
- [ ] 3. Are you confident that your backup data is readily available and accessible when needed?
- [ ] 4. If your backup software credentials were compromised, could the hacker access the stored data?
- [ ] 5. Do you have an ultra-secure offsite copy of your backup data?

NEXT UP **TOP 3 APPROACHES FOR BACKUP SECURITY & RESILIENCE**

Top 3 Approaches for Backup Security & Resilience

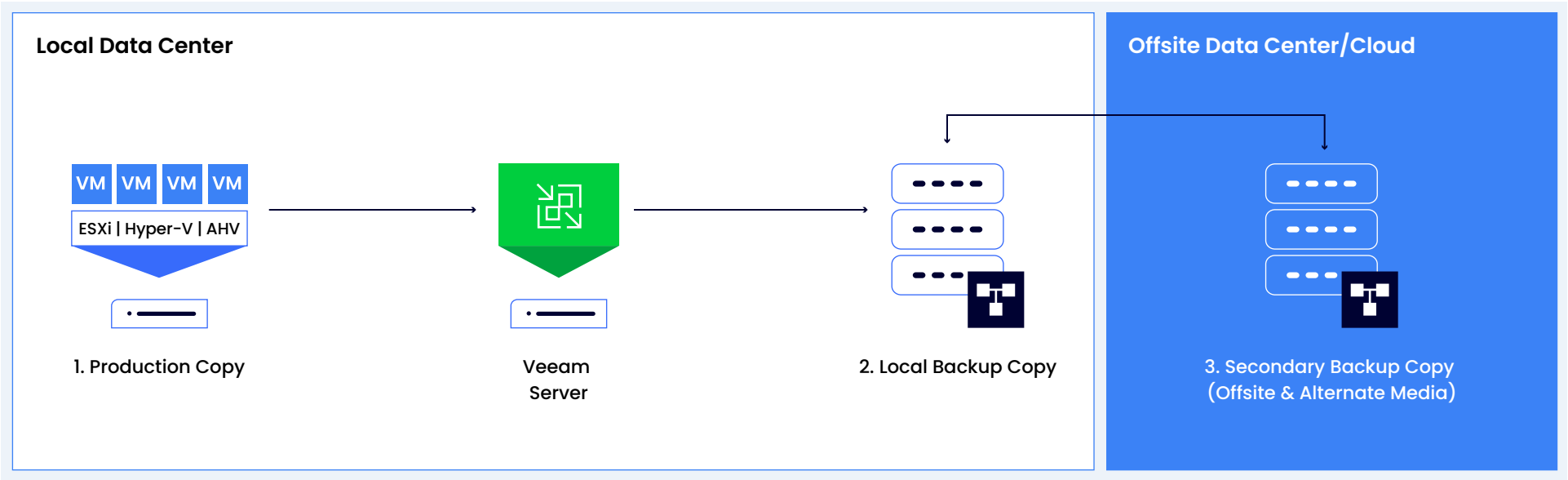
The recommended approach to backup security combines implementation best practices with modern technology. When using a software-defined backup solution, you have several decisions to make in how you structure the infrastructure and operations. The decisions you make will have an impact on business resilience and data security, and will also impact overall performance, complexity, and cost.

1 Follow the 3-2-1-X Backup Rule

The general 3-2-1 rule for backup has gained popularity in recent years and offers a simple way to improve resilience against a number of threats and disasters. If your backups are not structured this way today, there are several plug-and-play solutions designed to help you quickly improve your preparedness.

- 3 Different Copies of Data
- 2 Different Types of Media
- 1 of Which is Offsite

Here's an example using the popular backup solution Veeam



Modernizing the Rule for Improved Ransomware Preparedness

With the goal of adapting backups for ransomware protection, the 3-2-1 rule has been modernized in different ways. This is to stay current with today's ransomware tactics, and to future-proof against evolving threats like artificial intelligence or brute force computing.

- **3-2-1-I** is used to indicate that at least one of the copies should be WORM immutable. Immutable, "Write Once Read Many" data storage typically cannot be altered or changed during a specified window of time. However, there are limitations as to how well this protects against ransomware and other threats, and alone doesn't secure many of the CVEs and backup vulnerabilities.

- **3-2-1-X** is shorthand for immutable with anti-exfiltration protection, meaning that one of the copies is WORM immutable and it has controls to prevent data theft and exfiltration. This is considered most effective in combating modern ransomware tactics.

83%

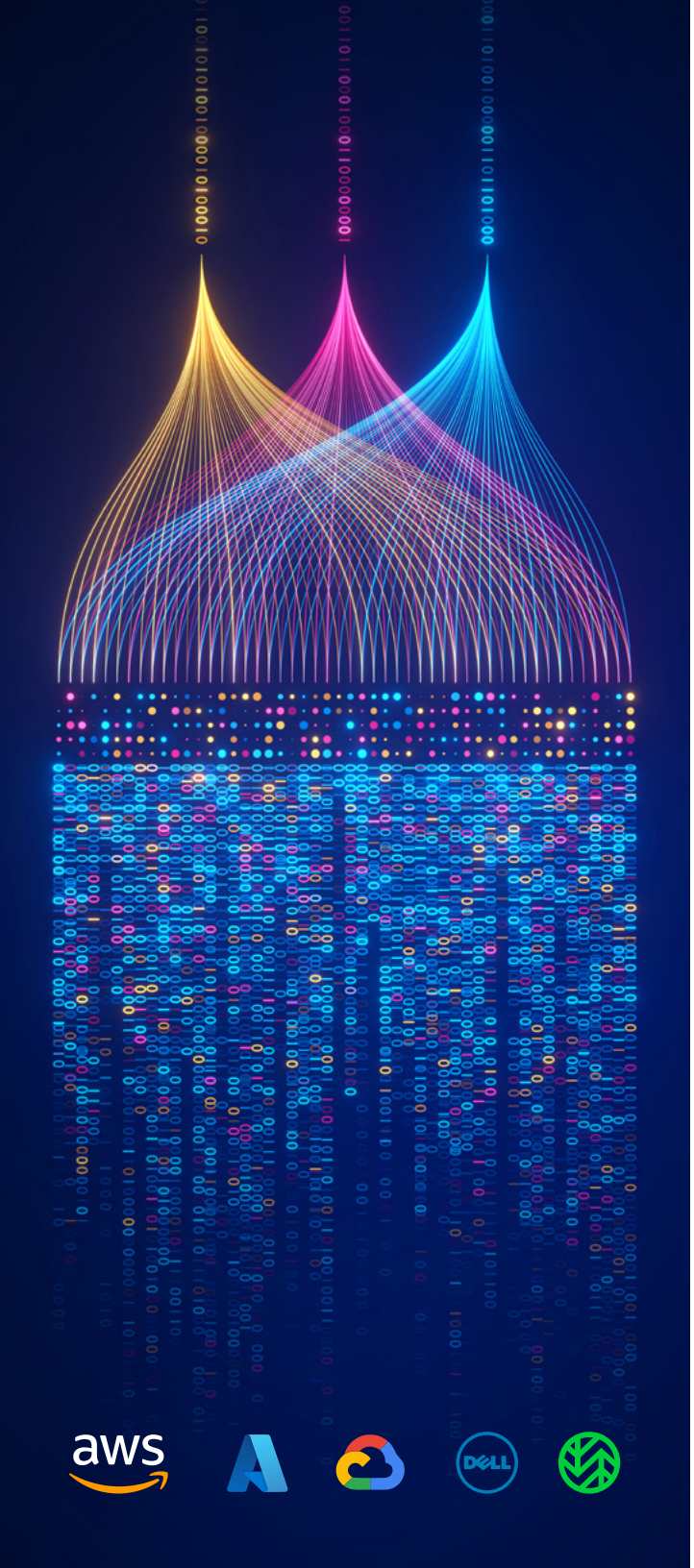
of Ransomware Attacks Exfiltrate Data

The latest studies reveal that data theft and exfiltration is augmenting or replacing the more traditional **"pay-to-decrypt"** ransomware attacks. Backup repositories are a common target for data exfiltration because they're often less secure than production environments. Having a WORM or immutable data repository alone does not address this particular threat, and therefore should be combined with additional cybersecurity layers.

2 Use Secure and Reliable Storage for an Offsite Copy

To achieve 3-2-1-X security and resilience, the offsite backup copy is critically important. Typically this houses the majority of data and has implications across regulatory compliance, cyber insurance premiums, and your ability to combat a ransomware attack. Choosing secure storage media will ensure that no matter what happens, your backup data will be available to you in an unadulterated state.

Storage Types	Advantages	Risks
Online Media (SSD, HDD)	• Greater control over your data • Faster performance • Readily accessible • Perform routine health checks	• Networked media can be more easily compromised • Hardware failure and EOL upgrades • Offsite management and overhead • Can be costly to scale
Offline Media (LTO Tape)	• Can potentially be less expensive • Physical air-gap is more secure	• Slower to restore in a disaster • Hardware failure • Offsite management and overhead • Limited health checks • Less accessible
Cloud (Object Storage)	• Makes the offsite copy fast and easy • Performance options • Affordable • Endlessly scalable • Multiple provider options	• Less control over your data • Misconfiguration is a common risk • Cloud outages and downtime • Supply chain and backdoor exploits



Mitigate the Risks Using Multi-Cloud RAID (A Data Harbor)

Cloud storage is growing in popularity for offsite backup storage. It is fast and easy to deploy, scalable, and has a variety of pricing and performance options. However, it's important to keep in mind that data security in the cloud is entirely up to the owner of the data according to most public cloud provider policies, and there are risks to security and resilience unique to public cloud storage.

A Data Harbor is an approach to cloud storage that offers unique advantages and mitigates many of the risks. It is a virtual storage repository that fragments data objects at the byte level across multiple cloud providers (think AWS, Azure, Google, and Wasabi), ensuring no single provider has a complete file or object. This approach adds precision access control and prevents common threats like credential theft, insiders, and many backdoor CVE's from compromising your data. Multi-Cloud Data Harbors combine physical security and cyber security, and are well suited to achieving 3-2-1-X while also improving download speeds and backup performance.

80%

of companies had experienced a cloud data breach in the previous 18 months, and nearly half of them (43%) reported more than 10 cloud breaches.[2]

[2] 2022 Ermetric Study

3 Apply The Right Mix of Cybersecurity Controls

Backup repositories intended to prevent ransomware typically use one or a combination of cybersecurity controls. Each approach has its own benefits and concerns, which is why the best solutions are layered. At the beginning of this guide we reviewed the most common vectors exploited by hackers to access stored backup data. **The below chart offers guidance on several measures to prevent unauthorized access.**

How Ransomware Breaks In

Most commonly, attackers will try to reach backup data over the network via NFS or SMB. If this doesn't work they may look for known exploits (CVE's) or common misconfigurations directly on the operating system of the backup server. Compromised credentials are also targeted for gaining administrator rights to turn off existing security or decrypt files.

	How it protects data	Concerns
Encryption	Encrypted backups are unreadable without the decryption keys, securing against theft attempts.	Emerging attack vectors including *steal-now-decrypt-later*, compromised decryption key management and quantum computing undermine traditional encryption methods. Additionally, hackers using compromised administrator credentials can decrypt the data.
Third-Party Key Management	Separating the encrypted data from the decryption key reduces the chance that threat actors will get access to both.	Outsourcing to a third party may increase cost and complexity, and needs to be implemented correctly.
Immutability (WORM)	Immutable backups ensure that data in the repository cannot be altered for a period of time.	Immutability alone does not protect data from exfiltration attacks, and can be circumvented via stolen privileged credentials or with some backdoor exploits.
Multi-Factor Authentication	Requiring additional methods of determining user identity to prevent unauthorized users from accessing data.	Some software-defined backup solutions don't offer MFA protection before restoring or exfiltrating data, or the ability to add custom checkpoints. Additionally, insider threats or misconfiguration can result in data exposure.
Physical Air-Gapping	Air-gapped solutions restrict all wired access to the data repository including email clients, browsers, SSH and FTP.	Failure points exist during data transfer through USB installers, exploits on remote code executions and trojans. Additionally, restore times from backup are long and the process can be expensive and cumbersome.
Logical Air-Gapping	Creating a logical separation between the production environment and the backup repository adheres to zero-trust frameworks while maintaining overall data availability.	Logical or virtual air-gapping is only as strong as the vulnerabilities affecting the storage itself, and the measures taken to avoid privileged credential compromise.

Which Approach is Best?

The best approach will depend on your particular needs such as budget and existing investments you've made into storage infrastructure. To make things simple, we've outlined an approach below that is highly secure, easy to implement, affordable, and follows industry best practices.

RECOMMENDED APPROACH:
HIGHLY SECURE BACKUPS THAT PREVENT RECOVERY FAILURE

Follow the 3-2-1-X Model
This will provide the greatest level of backup security and resilience without significant disruption to your existing operations. This will also future-proof the updates you make today against tomorrow's cyber threats and disasters, and comply with most any regulatory requirement.

Local Backup Copy: Secure with Encryption and Multi-Factor Authentication
Make sure that your locally retained data is encrypted while in-transit and at-rest, and that it requires some form of MFA to be accessed.

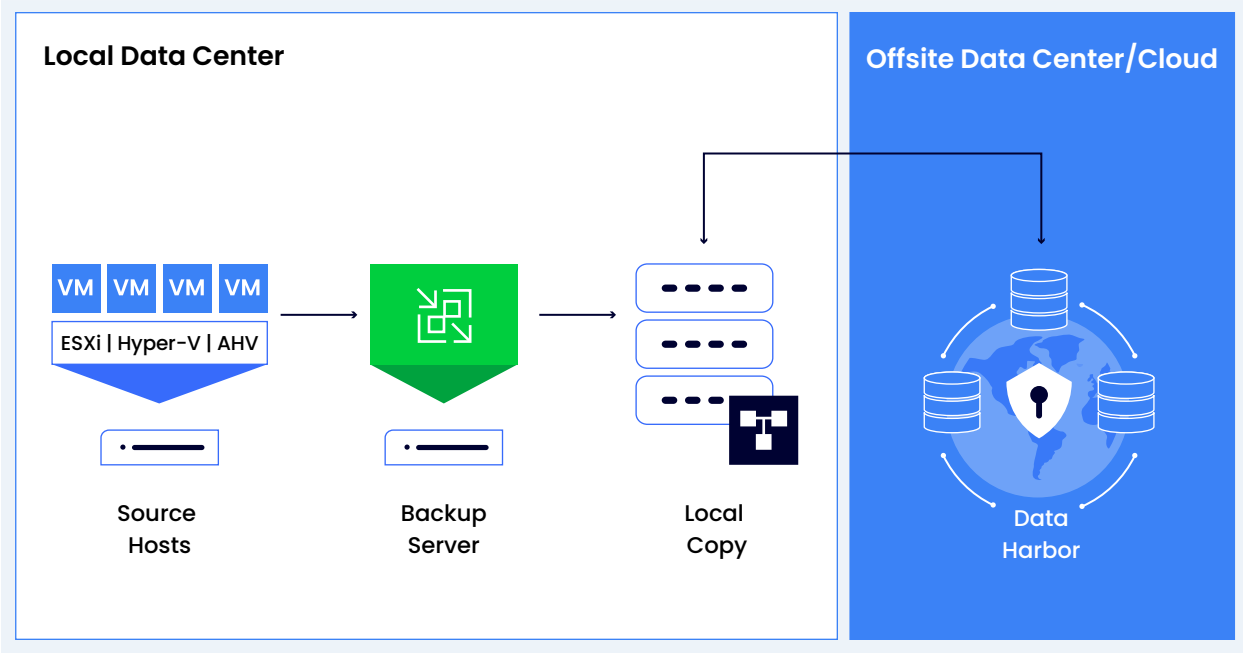
Secondary Backup Copy: Multi-Cloud Data Harbor

Immutable - use object locking capabilities to prevent malicious encryption and deletion.

Distributed - fragment data across multiple clouds to prevent data theft and exfiltration, and ensure availability during any cloud outages or disasters.

Logically Air Gapped - only accessed with secure MFA for Zero Trust Security. We also recommend implementing the "2-Man Rule" for bulk data restore.

Our recommended approach includes using a Data Harbor because it packages many of the best capabilities into a readily deployable repository that's compatible with most backup software and tooling. It can be composed of any combination of major cloud providers, and connected with industry protocols like S3-API.



NEXT UP **TAKING A CLOSER LOOK AT DATA HARBORS**

Taking a Closer Look at Data Harbors

A Data Harbor functions just like any S3-Compatible object storage. However, instead of files being sent to a single cloud in their entirety, the file is fragmented across multiple clouds in a RAID type configuration with no single cloud storing a complete file or object. This architecture inherently removes any single point of failure.

Data is secure from theft and exfiltration, malicious encryption, deletion, or manipulation – all the tactics commonly used by ransomware actors. The data is also redundant across clouds, maintaining accessibility if one cloud experiences an outage or downtime.

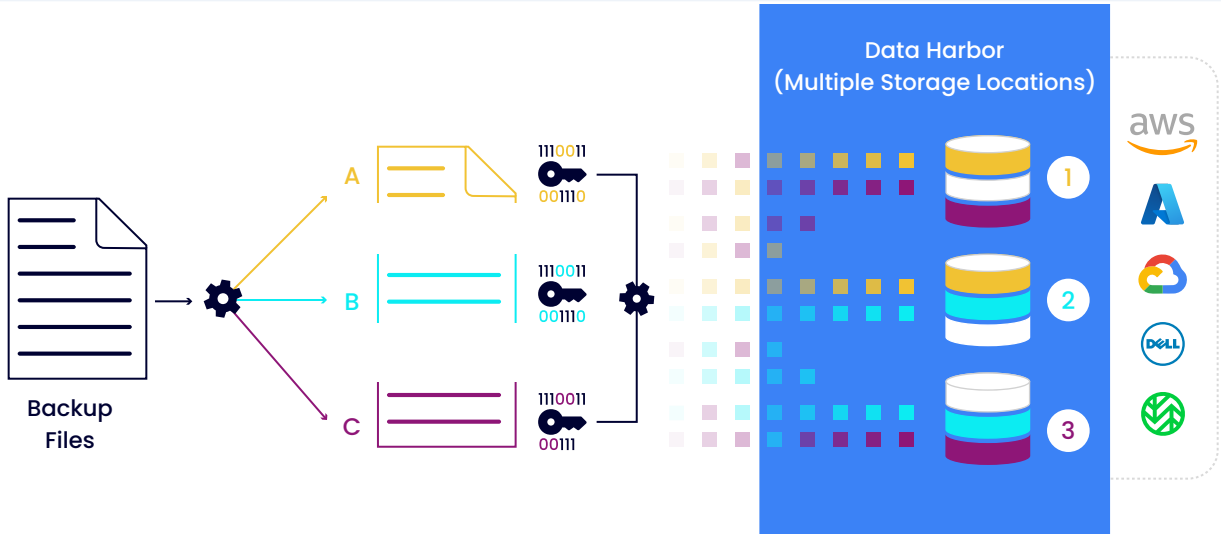
- Creates a Zero Trust, Logical Air Gap
- Adds unique controls against data exfiltration
- Enables deep MFA to control data access privileges
- Data is encrypted in-transit & at-rest
- Fully immutable with versioning
- Accessible during cloud outages or failures
- Self-heals from malware
- Deployable via S3-API object storage

Considering a Data Harbor?

START HERE

How it Works: Backup Process with a Multi-Cloud Data Harbor

1. Backup files are broken into multiple pieces or fragments (for example, parts A, B, & C)
2. Each fragment is encrypted with a unique encryption key
3. The encrypted fragments are then distributed across multiple clouds such that no cloud has a complete file, and the fragments are redundant
4. When a restore job is initiated, the data is reassembled in real-time, with deep MFA and 2-Man Rule challenge-backs ensuring only verified administrators can access the data or initiate movement



About Calamu

Calamu is the leading provider of storage and backup security software. Calamu Protect makes it fast, easy, and affordable for customers to use a Data Harbor without the burden of new tool fatigue. Users can combine their preferred storage providers into a Data Harbor and begin protecting sensitive data in 30 minutes or less.

To learn more and start a free test drive, visit **www.calamu.com/get-started.**

Calamu™