

.00, Jesse J Perez, 201
Reese, 241, Jun-11, 201
745 SHARDSECURE
594.00, Joe N Mc
594.00, Joe N Mc

White Paper

How to Achieve Secure Cold Storage Migration with Microsharding



Overview

Until recently, most organizations stored their cold data on-premises. Now, with new estimates suggesting that total global data storage is projected to [exceed 200 zettabytes by 2025](#), companies need to optimize how and where they keep their data.

This is especially true for cold data, which is infrequently accessed but must be archived for purposes including backup, historical, legal, audits, and compliance. Shockingly, cold data currently comprises [60% of all enterprise data](#).

Maintaining that cold data on-premises is expensive, with hardware replacements, energy and cooling costs, and licensing, support, and maintenance fees all adding up. Indeed, one detailed 2016 cost analysis estimates that [cloud storage is about 30% cheaper than on-premises storage](#).

Meanwhile, the cost of cloud services continues to drop. As one [2020 study](#) on data storage for clinical laboratories revealed, the most economical cloud storage option in 2020 was over 150 times cheaper than it was in 2006. Cloud storage is also more flexible for businesses that want to pay for only the amount of storage they actually need, allowing organizations to scale up incrementally as they grow.

As such, businesses are increasingly considering migrating cold data storage to the cloud, where they can [reduce storage costs by over 70%](#). But despite the cost savings, many organizations have been hesitant to make the move due to concerns over data security, data privacy, downtime, and more.

Fortunately, microsharding offers a way for organizations to strengthen their data protection and resilience so they can reap all the benefits of migrating their cold data to the cloud.



Factors that complicate cold storage migration

Data retention policies

Data retention policies require companies to store certain kinds of data for predetermined periods of time. Companies might need to access that data for internal disaster recovery, analytics, or archival reasons, or for local and federal regulatory compliance. For instance, publicly-traded companies in the United States must maintain Sarbanes-Oxley Act (SOX) data retention policies, while organizations that accept credit card payments must maintain Payment Card Industry Data Security Standard (PCI DSS) data retention policies. Similarly, an American healthcare system's data retention policies must adhere to the Health Insurance and Portability and Accountability Act (HIPAA), and any business that processes or stores personal information in the European Union must comply with the General Data Protection Regulation (GDPR).

Given the length of time mandated by these kinds of data retention policies (e.g., 7 years for SOX), it is no surprise that organizations need flexibility in their data storage solutions. The costs of different storage options can change drastically over a few years, and companies may be hesitant to migrate their cold data if they fear provider lock-in for an extended period of time.

An effective cold storage migration plan must still allow organizations the flexibility to move their data during that data's mandated lifespan — be that to another cloud provider with better rates or another type of storage altogether.

The shared responsibility model

While security for on-premises data centers is typically the sole responsibility of the data owner, cloud service providers (CSPs) operate under the shared responsibility model. In other words, both the storage provider and the data owner share an obligation to safeguard data in the cloud. With the CSP typically protecting hardware, software, physical hosts, networks, data centers, and physical buildings, the data owner is left to provide security for their applications, code repositories, identity and access management, passwords, and more. A good rule of thumb is that the CSP is responsible for security “of” the cloud and the customer is responsible for security “in” the cloud.

While it may seem beneficial to split the burden of data protection, the reality is that shared responsibility models can vary significantly between cloud providers. What may be covered with one CSP might be left unprotected elsewhere — and there are significant gray areas. Unlike the clearly defined responsibilities of on-premises cold data storage, cloud storage responsibilities can be much murkier. As a result, some organizations avoid migrating to the cloud altogether.

Cloud provider outages

Outages at major cloud providers can be deeply damaging to the businesses whose data is stored and processed in those clouds. As the [Uptime Institute Global Survey of IT and Data Center Managers](#) noted, third-party IT vendors — including cloud, hosting, and telecommunication providers — accounted for 63% of all publicly reported outages that Uptime tracked from 2016 to 2022.

These outages can cause costly downtime, making some CISOs hesitant to migrate to the cloud. After all, cold storage migration is only cost effective if the organization isn't regularly losing revenue to cloud outages. The damages from these outages can be major: The Uptime study noted that over 60% of failures in 2022 resulted in at least \$100,000 in total losses, up substantially from 39% in 2019. Moreover, 15% of outages cost upwards of \$1 million in 2022, up from 11% in 2019. Without a strong data resilience solution, companies may find themselves at the mercy of cloud outages.

Disruptions to existing systems

One of the most significant obstacles to cold storage migration is the transition for the data users themselves. Companies may struggle to execute a smooth, seamless move from on-premises to the cloud if their new system is substantially different for employees accessing or archiving data. Changes mean that companies must retrain employees, redesign workflows, and monitor employee adherence — all of which require time and resources.



How microsharding supports secure cold storage migration

The Austin Technology Council puts it bluntly: “Most on-premises solutions are [woefully inefficient](#).” But the complications of cold storage migration keep many companies locked in these inefficient systems.

Fortunately, the right microsharding solution allows companies to address their concerns about data privacy, security, and resilience — as well as cloud outages and employee workflows — while still saving significantly on storage costs.

Data security and privacy

Microshard™ technology desensitizes cold data for privacy and protection in the cloud. It shreds data into tiny microshards and distributes them across multiple storage locations, ensuring that each location only contains an unintelligible fraction of a whole dataset. Unlike encryption, which can be broken, this innovative solution renders cold data completely incomprehensible and useless to any unauthorized users, regardless of their compute power.

Data resilience

Microsharding also offers high availability and failover and helps protect against the impact of cloud provider outages, power outages, cyberattacks, and more.

Each instance of ShardSecure is a virtual cluster that, when deployed in different regions and different clouds, can maintain availability and performance with even greater reliability than on-premises options. If one cold storage location becomes inaccessible, user activity is seamlessly directed to an operational location.

Additionally, ShardSecure's self-healing data reconstructs cold data that is deleted, lost in an outage, tampered with during a cyberattack, or altered in any unauthorized way. If microsharded data fails a data integrity check, it is reconstructed transparently and

in real-time. If a storage location becomes unavailable due to an outage, a network issue, a misconfiguration, or a ransomware attack, users can continue working uninterrupted without the company needing to restore data from backups.

Ease and speed of access

Ease of access to data is a vital part of successful cold storage migration. Microsharding allows instant access to cold data when it's needed, with no lag time introduced by ShardSecure.

ShardSecure also avoids disruptions to employee workflows. It operates as an abstraction layer, meaning that companies can migrate their storage from on-premises to the cloud without any changes to what the user sees or where they interact with data.

Transparent, vendor-agnostic integration

Microsharding allows you to seamlessly migrate data from on-premises cold storage to the cloud storage locations of your choosing. Data migration and microsharding happen in the background and are a zero-downtime event, with no impact to your applications and no visible changes for your users. If you need to migrate data from one storage location to another for cost, availability, or performance reasons, you can start the process with just a few clicks.

Embedded data control

Microsharding keeps you in control of your own data. Organizations can use the cloud storage providers of their choice, in the geographic locations and jurisdictions of their choice, in order to maintain control over data access. This gives them the control they need to mitigate data transfer risk, address data sovereignty, and stay compliant with data regulations.

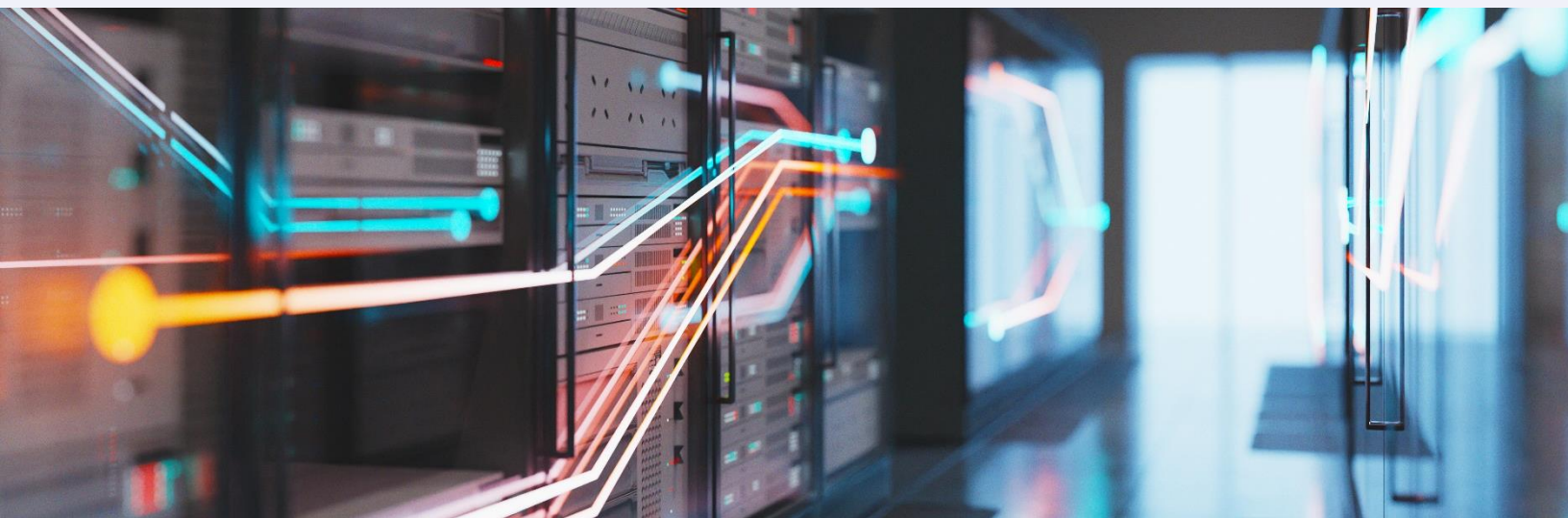
Microsharding does not rely on keys, so issues of third-party key ownership, key management, and credential abuse are nonexistent. It's also not possible for a third party to deploy an instance of ShardSecure to reassemble microsharded data.



Conclusion

Concerns about data security, privacy, availability, and compliance have held many organizations back from cold storage migration. Microshard technology addresses these concerns with data integrity checks, self-healing data, high availability, strong resilience, vendor-agnostic integration, ease of access, and virtually unbreakable data protection in the cloud. Finally, organizations can reap the financial benefits of migrating cold storage to the cloud with confidence.


For more information on how ShardSecure helps leading organizations in financial services, pharmaceuticals, biotech, and beyond to securely migrate their cold data to the cloud, [contact us today](#).



 @ShardSecure

 @ShardSecure

 @ShardSecure

 101 Avenue of the Americas
9th Floor, New York, NY 10013
United States of America

 info@shardsecure.com

**SHARD
SECURE**