

Solution Brief



Cloud storage is approximately **30%** cheaper than on-premises storage.¹



The average energy cost to power a single server rack in a US data center can be as high as **\$30,000** a year depending on its configuration of storage and compute capabilities.

On average, storage can account for **11%** of the energy, with storage accounting for an average of **\$3,300 per rack**.²

We provide native support for:

- Microsoft Azure
- Amazon AWS
- Google Cloud Platform
- IBM Cloud
- Oracle Cloud Infrastructure
- Alibaba

¹Deckler, Greg. (2016). Cloud vs. On-Premises Costs. Codilime. Retrieved April 20, 2022, from <https://codilime.com/pdf/faCloudOnPremisesFoundations.pdf>

² Gartner, "2022 Strategic Roadmap for Storage", J. Vogel, Julia Palmer, M. Hoeck, J. Rozeman, J. Unsworth, March 16, 2022. Disclaimer: GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

ShardSecure Enables Cold Storage Migration to the Cloud

Companies looking to significantly lower their cold storage costs can use our patent-pending Microshard™ technology to secure the migration of sensitive data to the cloud.



The High Price of Cold Data Storage

Financial institutions, pharmaceutical companies, and myriad other businesses often need to store regulated data for compliance and legal purposes for years at a time. But, due to data security concerns, many companies continue to use expensive, on-premises cold storage rather than cheaper cloud storage. It is difficult to estimate exact storage costs, but a 2016 Codilime report written for Fusion Alliance estimated that the cloud is approximately 30% cheaper than on-premises storage.¹

The price of on-prem cold storage includes licensing, support, and maintenance fees, in addition to incidental energy and cooling costs. According to a 2022 Gartner® report, the average energy cost to power a single server rack in a US data center can be as high as \$30,000 a year depending on its configuration of storage and compute capabilities. On average, storage can account for 11% of the energy, with storage accounting for an average of \$3,300 per rack.²

Lastly, cold data storage systems degrade or go end-of-life and must be replaced. Companies must essentially pay to maintain dormant data for years at a time.



Enabling Secure Cold Storage Migration to the Cloud

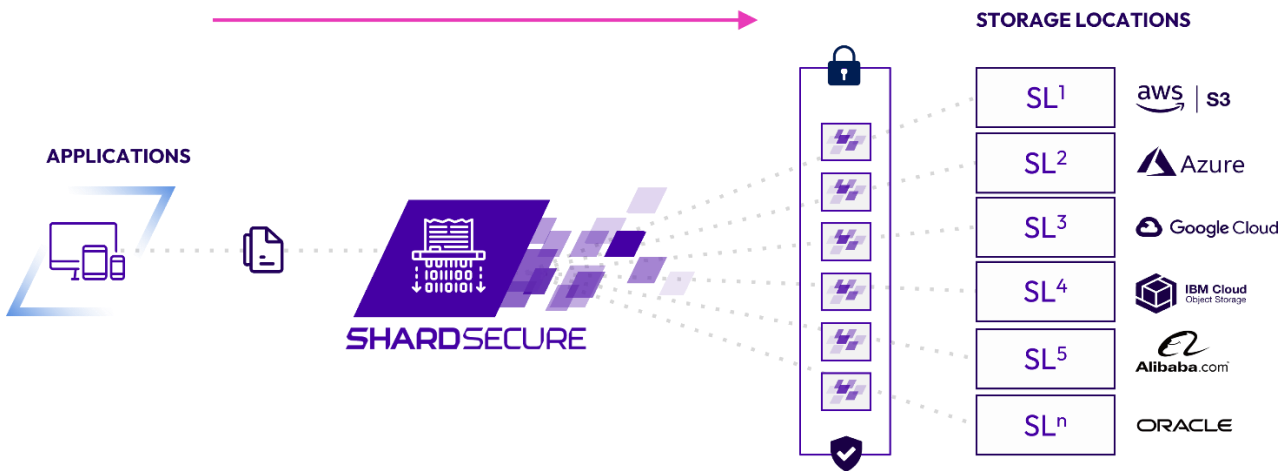
Our Microshard technology offers an answer to companies looking to significantly lower their cold storage costs by securely migrating their sensitive data. In conjunction with our data migration partners, we microshard your sensitive data as it is migrated to the cloud.

By integrating with your storage solutions and desensitizing your sensitive data in the cloud, we help to ensure that your data is unintelligible and of no value to unauthorized users. Our process offers the added benefits of neutralizing ransomware and data tampering while maintaining full data availability. This makes microsharding an inherently strong choice for organizations that want to migrate their data from on-prem cold storage to the cloud—but are worried about privacy and security.



ShardSecure Keeps Data Safe After Migration

ShardSecure's three-step process renders data unintelligible, incomplete, and useless in the wrong hands.



- **Shred:** Microshard technology begins by shredding data into four-byte microshards that are too small to contain a complete birthdate, social security number, and most other pieces of sensitive data.
- **Mix:** Next, the microshards are mixed into different Microshard containers and poison data is added. Identifying information like file extensions, file names, and other metadata are removed. This renders all your company's data—confidential or otherwise—completely unintelligible.
- **Distribute:** After being mixed, the Microshard containers are distributed across multiple, customer-owned storage repositories. These storage repositories can comprise multi-cloud or hybrid-cloud configurations.



Data Confidentiality, Integrity, and Availability

Microsharding adheres to the CIA triad pillars of confidentiality, integrity, and availability. Data confidentiality is maintained by shredding, mixing, and distributing data as described previously.

Data integrity is enforced through multiple data integrity checks that detect and roll back unauthorized deletion of and/or tampering with Microshard data, including cloud storage ransomware. And while these types of activities are neutralized, your application users continue working without interruption.

Data availability and business continuity are maintained, even during a cloud storage service outage. Our RAID-5-like ability to reconstruct affected Microshard data means that your business operations can continue functioning like normal. Additionally, our virtual clusters support high-availability and failover functionality within a cluster and among multiple clusters to help ensure your critical data at rest stays secure and available.

Learn More

Visit us at <https://shardsecure.com> for more information and to schedule a demo.