SHARDSECURE

# Case Study

## Leading Financial Services Firm Banks on ShardSecure for Secure Cloud Migration

A large financial institution wanted to move to the cloud to take advantage of the innovation, agility, scalability, and efficiencies it enables. However, as with any company that operates in a highly regulated industry, security is always top of mind and can significantly challenge cloud migration strategies. Concerns over data privacy and control had created a roadblock to the project as the team charged with supporting digital transformation initiatives and those responsible for securing the data searched for a mutual path forward. ShardSecure was able to give them confidence they could migrate to the cloud securely and meet rising customer and business expectations.

### Challenges:

Security concerns presented roadblocks that were delaying the financial institution's digital transformation initiatives.

**Data privacy and compliance.** Customer data, including account numbers, credit card data and other personally identifiable information (PII), is the firm's crown jewels. Encryption was the firm's weapon of choice to protect sensitive data and comply with rapidly evolving regulations. They had spent considerable resources finely tuning their encryption key management processes for their on-premises environment and internal users. They felt that relying on their cloud provider's encryption would expand the attack surface and introduce additional cost, complexity, and risk as there are more opportunities for keys to be lost or stolen.

**Losing control of data.** Cloud providers operate with a shared responsibility model, which includes varying levels of security responsibility depending on deployment models – IaaS, PaaS and SaaS. The lines of responsibility for protecting data in the cloud can become blurred. Even if the arrangement were crystal clear, entrusting someone else to shepherd their data was a non-starter for security leadership. A highly resourced threat actor, motivated by high-value data and with enough time could decrypt data. And storage misconfigurations and other security lapses that frequently make headline news were also a huge concern.


Copyright © 2023, ShardSecure, Inc.

## Solution:

The company turned to ShardSecure for secured cloud enablement. ShardSecure's Microshard™ technology is a three step process that consists of shredding, mixing, and distributing data across multiple storage repositories, and protects data by making it unintelligible and unusable in the wrong hands.

- **Shred:** Microsharding begins by "shredding" files into microshards, which effectively removes the sensitivity of the data. Microshards are typically too small to contain a complete birth date, ID number, address, or other kinds of sensitive data.

- **Mix:** Microshards are mixed across multiple containers along with poison data to make it more unintelligible to unauthorized users.

- **Distribute:** The containers are distributed across multiple, segmented storage repositories of your choosing — multi-cloud, multi-region, or hybrid cloud. Unauthorized reassembly of the microsharded data is virtually impossible.

## Outcomes:

The financial institution augmented their approach to security and were able to accelerate their journey to the cloud with confidence.

**Stronger data security and privacy.** Microshard technology provides the flexibility to safely move data among cloud providers, cloud regions, and hybrid cloud locations. Given their risk posture, the firm decided to layer security and use ShardSecure in combination with encryption, with little to no additional work required. Should encryption keys be compromised, an attacker would not be able to decrypt without first reassembling the Microshard data, which is virtually impossible since it is mixed across containers and distributed across multiple storage locations.

**Data protects itself.** ShardSecure helps protect the firm's extremely valuable client data by making it incomplete, unintelligible, and of no value to bad actors, cloud providers and IT administrators. Shared responsibility is a moot point. Microsharding essentially makes sensitive data no longer sensitive, so the customer maintains control of their data and no keys are required. The data is shredded and mixed before it is distributed to ensure it is incomplete, which shields it from malicious activity and inadvertent exposure due to misconfigurations and other human errors.

+1 (800) 760 9445
info@shardsecure.com
@ShardSecure

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

SHARD SECURE