SHARDSECURE

Case Study

Multinational Biotechnology Pioneer Turns to ShardSecure to Make Data Safe and Accessible

For companies in life sciences, data is the key to unlocking a better quality of life for people facing health threats. A large, multinational biotechnology company needed to ensure this data remained secure yet accessible to their workforce as they develop innovative therapies. The company had accumulated a mix of old and new systems over the years with data stored in different regions and locations, on premises and in the cloud. As databases, and ultimately intellectual property (IP), have become prime targets for attackers, the company needed a uniform approach to data security and accessibility and turned to ShardSecure.

Challenges:

The company's existing approach to secure data storage had become inefficient and ineffective for several reasons.

Myriad data storage locations. The company is comprised of business units that operate independently, each with their own technology strategies to address their needs. The initial on-premises data storage strategy, evolved to a hybrid configuration with a single cloud provider and multiple datacenters. The company needed to make sure all their data is reliably secured, and would like the flexibility to move to a multi-cloud strategy over time to avoid the risks of cloud provider lock-in.

Disparate systems and data types. The company's combination of legacy and new systems makes it difficult to establish a unified data storage policy. Dealing with a variety of data, structured and unstructured, adds further complexity because unstructured data is typically unorganized and has no predefined format. Sensitive information is located in PDFs, documents, spreadsheets, and images, which are difficult to secure uniformly.

Poor cyber hygiene. Collaboration with consultants is an integral part of their innovation and growth strategy and has allowed the company to bring medical breakthroughs to market faster. However, relying on individuals and third parties for good cyber hygiene is problematic. Users put encryption keys in source code or upload them to GitHub to facilitate collaboration with different systems and users, including their cloud provider. Consultants copy encryption keys and store them on their laptop to have an offline copy. If accounts are compromised due to these poor practices, data and IP are at risk of breaches, ransomware attacks, cyber espionage, and more.

Solution:

The company turned to ShardSecure for an enterprise-wide, secure data storage platform. 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 environments. Unauthorized reassembly of the Microshard data is virtually impossible.

Outcomes:

Using ShardSecure to enable a consistent approach to data security and storage, the company realized several benefits.

Uniform platform for secure data storage. The ShardSecure virtual appliance cluster appears as storage to systems and users, and the company decides where data is ultimately stored – multi-cloud, multi-region, or hybrid cloud. They can move that data securely with no impact on availability, so teams can collaborate without worrying about downtime. ShardSecure can also cloud enable data from older systems, allowing the company to store that data in the cloud and extend the lifespan of legacy technology until they refresh.

Secure all types of data. ShardSecure ingests structured and unstructured data from applications, databases, and servers via an S3-compatible Object Storage API and iSCSI for object storage and retrieval, with little to no additional work required. The company is able to augment security of their existing server backup solution as well as better secure data from their database management system and healthcare applications – whether on file servers or cloud-based applications.

Protect data access. ShardSecure helps protect data and IP by making the company's data incomplete, unintelligible, and of no value to unauthorized users. ShardSecure's approach separates storage and infrastructure from people and works in the background with minimal administration support. Users have access to data on a project basis, with no need for encryption keys. Unauthorized access to a given storage location only returns an unintelligible portion of the data.

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

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