

Solution Brief



ShardSecure's Approach

Microshard technology desensitizes unstructured data and offers strong file-level protection for multi-cloud and hybrid-cloud environments. Here's how:

Shred: Microshard technology begins by shredding data into four-byte microshards that are too small to contain a birthdate, an ID number, or any complete piece of sensitive data.

Mix: Next, poison data is added and the microshards are mixed into multiple logical Microshard containers. Identifying information like file extensions, file names, and other metadata is also removed.

Distribute: After being mixed, the Microshard containers are distributed across multiple customer-owned storage repositories in multi-cloud or hybrid-cloud configuration.

ShardSecure Integrates With Fortanix for Advanced Data Protection



Overview

In the modern workplace, data security risks abound. Threats like ransomware and man-in-the-middle attacks are becoming both more sophisticated and more expensive to recover from. Add in the growing complexity of remote work and multi-cloud and hybrid-cloud infrastructures, and the task of data protection can seem daunting.

ShardSecure's patented Microshard™ technology offers an advanced solution with self-healing data to desensitize sensitive files for the cloud. For added security, ShardSecure also partners with Fortanix.

This integration between ShardSecure and Fortanix combines the data security benefits of Microshard technology with the robust encryption of an HSM (Hardware Security Module). The partnership ensures that both unstructured data and structured data are well protected against outages, attacks, and other forms of data compromise.

File-Level Protection

Microshard technology excels at ensuring that the privacy, integrity, and availability of unstructured files are protected in the cloud. It helps prevent unauthorized access to data at rest and reduces the attack surface and risk of human error.

Even if a Microshard storage location is compromised, unauthorized users can only obtain access to an unintelligible fraction of the complete data set. No single storage container contains enough data microshards to reassemble, and metadata and other file identifiers are removed to add yet another barrier to unauthorized reassembly. This means that sensitive files remain unintelligible even if a storage location is compromised by misconfiguration, compromised credentials, motivated threat actors, or outages.

Protecting Data Before It's Stored in the Cloud

While cloud service providers (CSPs) typically offer strong protection against front-end attacks, the shared responsibility model means that individual organizations are still responsible for securing their own data against back-end threats in the cloud.

In conjunction with its data migration partners, ShardSecure microshards organizations' sensitive data as it is migrated to the cloud. It also offers easy integration with storage APIs and transparent data proxy to ensure that files are microsharded prior to storage.

The microsharding process makes sensitive data unintelligible to anyone other than the data owners, meaning that neither CSPs nor government agencies nor even attackers can access complete datasets without the owner's consent.

Transparent Data Protection

ShardSecure's data protection is transparent to storage locations and to the application, which allows for easier deployment and implementation. ShardSecure's architecture also allows for an easy plug-and-play integration with any application.

Protecting Privacy and Resilience

ShardSecure's self-healing data supports business continuity through its RAID-5-like ability to reconstruct data impacted by storage service outages. This means that Microshard data containers can be rebuilt whenever they're tampered with, deleted, or held hostage by ransomware.

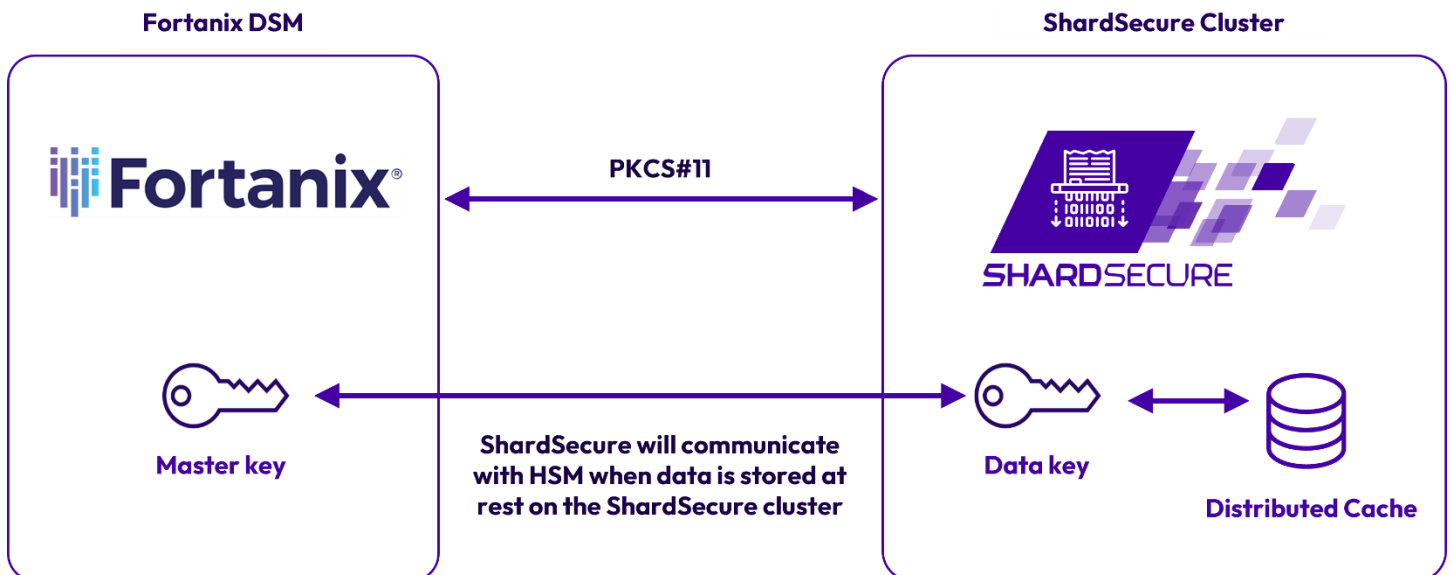
Using an automated control, multiple data checks detect unauthorized modifications — including those caused by cloud storage ransomware — and roll back data to its earlier state. They also provide early detection and alert the SOC and security team. This means that real-time ransomware repairs can begin automatically and in a way that is transparent to users, resulting in minimal downtime and fewer disruptions to business operations.



ShardSecure + Fortanix Partnership

The ShardSecure and Fortanix partners protect both unstructured and structured data.

The integration leverages Fortanix's PKCS #11 interface to store the ShardSecure cluster Master encryption Key of the distributed cache database in Fortanix Data Security Manager with FIPS 140-2 Level 3 protection.



The Fortanix Data Security Manager

Fortanix Data Security Manager (DSM) provides integrated data security with encryption, multi-cloud key management, tokenization, and other capabilities from a single platform. Its technology ensures the secure generation, storage, and management of private keys with automation across key lifecycles to protect data and preserve privacy.

Secured with Intel® SGX, Fortanix DSM delivers HSM-grade security with software-defined simplicity. It provides flexible consumption options — a hardened appliance, HSM as a service, or software running on commodity x86 servers — as well as central management, tamper-proof logging, rich access control, and REST APIs.

Organizations can use Fortanix DSM to secure their sensitive cloud and traditional applications, including digital payments, PKI systems, IOT applications, and remote TLS terminations — all while reducing integration complexities and expenses.

Summary

In the face of rising ransomware attacks and cybercrime worldwide, organizations must implement advanced data protection solutions. Safeguarding sensitive data, confidential user information, and intellectual property is essential — especially given that cybercrime is estimated to cost companies \$10.5 trillion annually by 2025. By leveraging ShardSecure's innovative microsharding approach and Fortanix DSM's advanced HSM capabilities, organizations can improve their data security and be better prepared for future threats.


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



 @ShardSecure

 @ShardSecure

 @ShardSecure

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

 info@shardsecure.com

**SHARD
SECURE**