

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 configurations.

ShardSecure Partners with Entrust for Robust 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 Entrust.

The integration between ShardSecure and Entrust combines the data protection benefits of Microshard technology with the secure key generation and management of Entrust's nShield HSM (Hardware Security Module). The partnership ensures that unstructured data in cloud environments is well protected against outages, attacks, and other forms of data compromise.

ShardSecure's protection of unstructured data complements Entrust's key management solutions for the protection of structured (database) data to address a wide range of customer needs.

File-Level Protection

Microshard technology excels at ensuring that the privacy, integrity, and availability of unstructured files are protected in the cloud. 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 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 + Entrust Integration

ShardSecure and Entrust have partnered to provide advanced data protection, adding a layer of security with a FIPS 140-2 Level-3 certified Entrust nShield HSM that generates and manages the underpinning keys to protect ShardSecure processes.

The integration leverages Entrust's nShield HSM using a PKCS #11 interface. Specifically, the ShardSecure engine encryption keys for the internal distributed cache reside in Entrust for at-rest encryption on the ShardSecure cluster. This enables all encryption keys leveraged by ShardSecure to be protected by a very secure hardware security module. The use of the Entrust nShield HSM adds a critically important layer of security for a defense-in-depth approach.

Entrust Security Solutions

Entrust offers a comprehensive and unified database security platform that secures critical data from external and internal threats and maintains data availability for business continuity. Its products offer a greater level of trust for interactions among enterprises, people, and data.

Entrust's identity and payment solutions enable the trusted access and secure transactions needed to keep global commerce and data moving safely. Meanwhile, its data protection solutions keep enterprises, consumers, governments, citizens, and their data secure with high assurance security through trusted identities, applied cryptography, and PKI.

Entrust's advanced technologies include full VM encryption for sensitive databases, lifecycle management and protection of database encryption keys, a cloud key management server that supports bring your own key (BYOK) capability to protect databases housed by major cloud service providers, and workload encryption management in multi-cloud infrastructures.

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 Entrust'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**