SHARDSECURE / utimaco®

Solution Brief

ShardSecure Partners with Utimaco for Robust Data Protection

Overview

We are on the cusp of a new generation of computing devices capable of cracking the most sophisticated algorithms and potentially eliminating encryption as a reliable way to secure data. Able to solve problems too complex for today's computers at speed and capacity, quantum computing could provide humans with tools to decrypt any type of encryption used today—regardless of length, complexity, and number of algorithms involved.

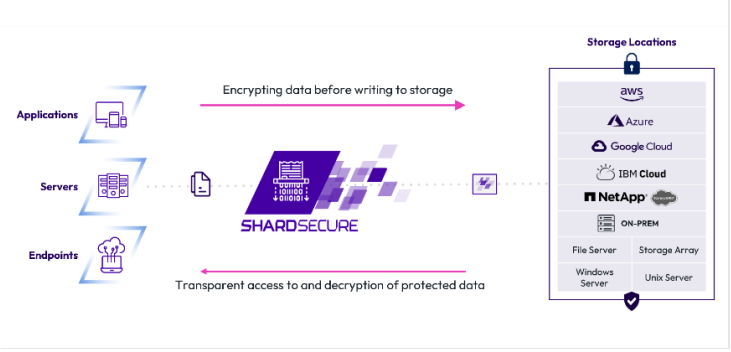
ShardSecure has devised a quantum-safe approach to file-level encryption using microsharding, which protects data at rest and essentially makes sensitive data unintelligible to unauthorized users. When data is shredded using the ShardSecure platform, the resulting microshards are too small to contain sensitive data. Mixing the microshards with poisoned data and distributing them across different storage locations helps to ensure unauthorized users never have a complete, intelligible dataset.

The integration between ShardSecure and Utimaco combines the data protection benefits of Microshard technology with the secure key generation, management, and storage of the tamper-proof Utimaco HSM (Hardware Security Module). The partnership ensures that unstructured data is protected against outages, attacks, and other forms of data compromise. ShardSecure and Utimaco provide a path forward to prepare for quantum computing regardless of whether that data resides in multi-cloud, multi-region, or hybrid cloud architectures.

ShardSecure's protection of unstructured data complements Utimaco solutions for the protection of structured data to address a wide range of customer needs.

Agentless File-level Protection

In the past, organizations protected their data from unauthorized access with agent-based encryption solutions. Unfortunately, traditional agent-based solutions tend to slow performance by 5% to 40%. They are also difficult to manage and scale and may be incompatible with newer workloads and cloud services.



ShardSecure offers an innovative, agentless alternative to agent-based file-level protection with "set and forget" management. The ShardSecure platform secures data from threats without the cost and complexity of agent-based solutions and provides strong data confidentiality and resilience in the process.

ShardSecure's API-based abstraction layer sits between applications and storage infrastructure, where it performs advanced file protection. This approach allows for a simpler deployment without changes to data workflows.

ShardSecure's low-latency and fast throughput architecture has minimal to no performance impact and maintaining data access does not require changes to existing applications.

Mitigate ransomware risks

ShardSecure offers transparent, real-time reconstruction of data that has been encrypted by ransomware. As soon as data fails a data integrity check, the ShardSecure platform automatically reconstructs affected data to minimize downtime and prevent disruption to users and data flows.

ShardSecure maintains strong data integrity with multiple health checks to detect unauthorized data tampering, alert security teams of a potential attack, and automatically reconstruct compromised data in real-time, ensuring that data remains accurate and unaltered, not just available.

The ShardSecure platform also mitigates the impact of double extortion ransomware attacks, where criminals threaten to release or sell sensitive data that they have exfiltrated prior to encrypting it. Since the ShardSecure platform renders data unintelligible to unauthorized users, exfiltrated data is of no value to attackers.

Protect 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 protects 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, so that neither CSPs nor attackers can access complete datasets without the owner's consent.

Simple integration & access

Despite its powerful data security, privacy, and resilience features, the ShardSecure platform has minimal impact on existing applications and operations teams and delivers instant data access and fast data migration among different storage locations with just a few clicks.

A vendor-agnostic solution that works in the background as a zero-downtime event, the ShardSecure platform appears and behaves like traditional storage to applications, requiring minimal code changes to get started.

Since the platform is also transparent, user workflows are not impacted. There are no visible changes to employee interfaces, and retraining employees or redesigning applications is unnecessary. This allows for seamless integration with existing operations.

ShardSecure + Utimaco Integration

ShardSecure and Utimaco have partnered to provide advanced data protection by adding a layer of security with a FIPS 140-2 Level-3 certified Utimaco Hardware Security Modules to generate and manage the underpinning keys used to protect ShardSecure processes.

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

Utimaco Solutions

UTIMACO is a global platform provider of trusted Cybersecurity and Compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA). Based on more than 40 years of experience in cybersecurity, Utimaco has developed a family of General Purpose Hardware Security Modules (HSM), with models that address different levels of performance and physical security for enterprise, government, and large infrastructure use cases. The FIPS 140-2 Level 3 certified General Purpose HSM from Utimaco offer:

- Plug and play integration with numerous business applications
- Support for a variety of cryptographic interfaces and algorithms
- True Random Number Generator to ensure uniqueness of keys
- Crypto agility and upgradability with PQC algorithms
- Free software simulator for evaluation and integration testing

For more information, visit: www.utimaco.com

Summary

Data security, privacy, and resilience have never been more important, and the threats to organizations have never been greater. Regardless of where sensitive data resides — on-prem, in the cloud, or in hybrid- or multi-cloud architectures — it needs to be always protected and secure. ShardSecure provides this security and privacy, while keeping you in control of your data, and offers agentless file-level protection, robust data resilience, advanced data privacy, support for compliance with cross-border regulations like the GDPR, and ransomware mitigation. By leveraging ShardSecure's innovative microsharding approach and Utimacos 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