SHARDSECURE

White Paper:

Transparent Database Encryption

Executive summary

Database encryption is crucial for data security and compliance, but traditional solutions slow down performance, present incompatibilities with newer architectures, and require the use of agents. Forward-thinking organizations are seeking solutions that offer strong data security without requiring agents or other resource-intensive processes.

Key findings

- While some enterprise databases provide built-in encryption, others lack functionality, exposing data to common threats.
- Although traditional encryption solutions offer strong privacy controls, they come with significant performance hits and require agents and endpoint management.
- Traditional encryption solutions are increasingly incompatible with new architectures and modern cloud infrastructures.

Recommendations

- With ShardSecure's Data Control Platform, organizations can achieve transparent database encryption with no performance drawback, no endpoint management, no changes to workflows, and no agents.
- The ShardSecure platform also provides robust data resilience with high availability, virtual clusters, and self-healing to reconstruct compromised data during outages and attacks.

Introduction

Databases and especially database files have been the target of cyberattacks for years. While some enterprise databases have addressed security concerns by providing built-in encryption, others don't support native encryption. Databases are also at risk for ransomware attacks, data exfiltration, and other malicious attacks on the availability and integrity of their data at rest.

In the past, companies have mitigated these threats with agent-based encryption. Today, however, agent-based solutions often slow performance and require resource-intensive endpoint management. They can also present incompatibilities with newer workloads and cloud services, keeping enterprises stuck with legacy systems.

The current state of database encryption

Native encryption support, but with caveats

Enterprise database providers have addressed some of the basic concerns around database encryption and security. Depending on the database and its license model, transparent encryption might be available within the product. This ensures that organizations can encrypt their data at rest without third-party tools and without integration issues for database administrators and applications.

Unfortunately, not all databases provide the level of security required for today's needs. Some databases still do not offer adequate encryption for data at rest within their product. Others require upgraded versions for database encryption, which can significantly increase licensing costs.

Traditional transparent database encryption: resource-intensive and incompatible

The most common method of implementing transparent database encryption has traditionally been to install agents, or software code, onto each device, server, and client system the database runs on. The agent is typically tied to a certain folder or file to protect data, and it controls access to those files.

Today, agents are increasingly difficult to manage and scale, and they require endpoint management. It can be challenging to install, configure, and maintain them on each device and server that requires file-level protection, particularly for companies with many devices or with remote teams. Agents also require access to the kernel of the OS of the database server, which increases the likelihood of kernel issues and complete system crashes.

Additionally, agents can present incompatibilities with newer architectures, including blob storage, S3 storage, K8s containers, and many other cloud offerings. These architectures — as well as modern tools like network storage, cloud storage, Platform as a Service (PaaS) solutions, and containers — were not designed to support the installation of software code to secure data.

Costly downtime and a lack of data resilience

Companies investing in data encryption solutions are increasingly seeking built-in data resilience features. After all, if an organization requires strong security for their critical data, they will also want to ensure access to that data at all times.

Strong resilience makes business sense. With the cost of downtime averaging over $9,000 per minute ($540,000 per hour) for a large enterprise, ensuring high availability is imperative.

Traditional database encryption solutions were not designed to provide data resilience. Encrypted files can still be tampered with and deleted in the most common types of cyberattacks, including ransomware. Although data confidentiality is maintained by traditional encryption, data integrity and availability both suffer in attacks and outages.

Simpler, stronger database encryption with ShardSecure

ShardSecure provides advanced database encryption with no performance drawback, no resource-intensive management, and no agents. Our Data Control Platform allows companies to secure their data from internal and external threats without the complexity of agent-based encryption solutions. We also offer strong data resilience and an easy interface that allows companies to leverage whichever data storage options work best for them.

Advanced protection for databases

ShardSecure protects databases in on-prem, hybrid-cloud, and multi-cloud environments with an innovative approach to database encryption. Specifically, our technology shreds and distributes data to multiple customer-owned storage locations in a way that prevents third parties from reconstructing data.

Even in the highly unlikely scenario that an attacker gains access to all the data fragments in a storage location for a given data set, they will not have enough material to ever reassemble it. Our technology:

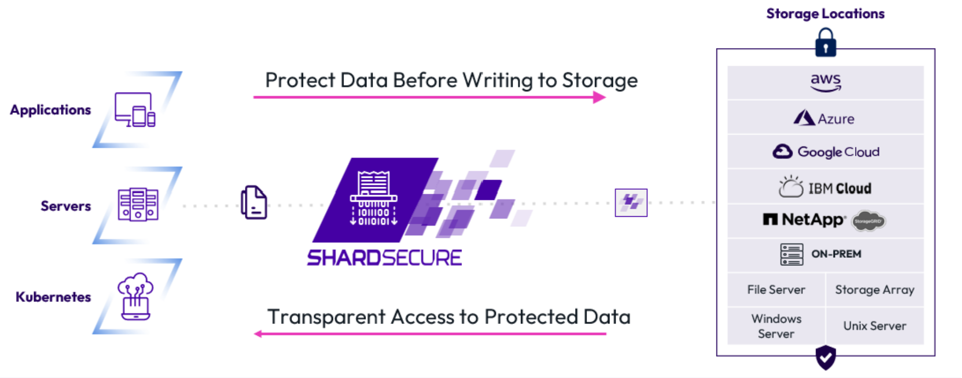
- Encrypts file content, file names, file extensions, and all other metadata.
- Allows organizations to add a configurable amount of poison data to their real data.
- Requires multiple components to be used in concert with both each other and the complete dataset for reassembly, making it impossible for an unauthorized user to deploy their own instance of ShardSecure to reconstruct data.

With ShardSecure, the data owner controls exactly who has access to their data, as well as where that data is stored. The result is strong privacy and protection for your data, regardless of which third-party providers have access to it.

An agentless solution for modern architectures

ShardSecure's Data Control Platform does not require any agents. This means that companies can avoid the overhead, complexity, and endpoint management of traditional file-level encryption. Because our technology is transparent to users, servers, and applications, workflows do not change, and reengineering is not necessary.

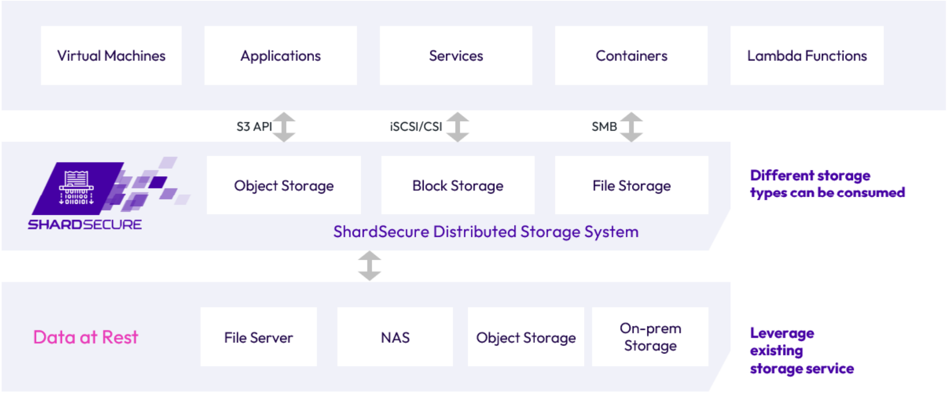
ShardSecure is easy to manage and has a low impact on operations teams. The design is vendor-agnostic and works in the background as a zero-downtime event.



Easy implementation and integration

ShardSecure's Data Control Platform easily integrates with existing interfaces for applications and databases. Our API-based abstraction layer sits between an organization's database and its data at rest, enabling advanced data protection without the need to install software on the database server or make changes within the database.

ShardSecure exposes itself to the database server as a disk (e.g. over iSCSI), as a folder (e.g. with container storage interface in Kubernetes), or as any other block storage method commonly used by database servers. Additionally, ShardSecure supports both object storage (e.g. S3 API) and file storage (e.g. SMB), which enables easy integration with databases — no matter where data is stored at rest.



Strong data resilience for business continuity

In addition to guaranteeing the privacy of data, ShardSecure also strengthens data resilience. The platform's self-healing feature detects when data is lost, deleted, tampered with, or otherwise compromised. If there are any problems, automatic controls begin to reconstruct the affected data immediately and transparently, returning it to its original state in real-time.

The platform also sends alerts to the company's security teams for faster incident response, reducing the need for restoring from backups and the likelihood of downtime. It can be configured to automatically move data to an unaffected storage location after a certain number of failed data integrity checks.

With ShardSecure, organizations can maintain their critical operations, avoid reportable security breaches, and mitigate third-party data access.

Conclusion: Regaining control of your data

Data is growing exponentially, straining bottom lines. At the same time, cyberthreats are on the rise, and the global regulatory landscape has become increasingly complex. Strong data privacy and security are key to tackling these challenges — but traditional file-level encryption solutions are consuming valuable time and resources.

ShardSecure offers a new and innovative approach to encryption. We protect data in the cloud and on-prem without agents, performance drawbacks, or resource-intensive management. Our transparent, easy-to-integrate solution keeps data private from attackers and infrastructure providers alike, supporting confidentiality and compliance.

ShardSecure's Data Control Platform also offers additional benefits like robust data resilience for outages and attacks. We make advanced data encryption a reality so organizations can regain control of their data and focus on what they do best.

For more information on ShardSecure and our data protection solution, view our other resources or schedule a demo today.

@ShardSecure
@ShardSecure
@ShardSecure

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

info@shardsecure.com

SHARD
SECURE