SHARDSECURE

White Paper:

A Guide to Agentless File Encryption

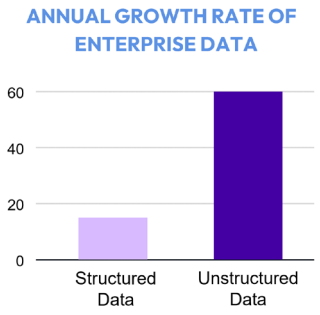
Achieving file encryption without performance drawbacks or agents

Executive summary

File Encryptoin 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

- Separating data from infrastructure providers and administrators is key for data confidentiality and compliance.
- Even though unstructured data is growing rapidly and needs strong data protection, it is under-served in the encryption space.
- Although traditional file encryption solutions offer strong privacy controls, they come with significant performance hits and require agents and endpoint management.
- Traditional encryption solutions are also increasingly incompatible with new architectures and modern cloud infrastructures.



Recommendations

- With ShardSecure's Data Control Platform, organizations can achieve file-level encryption with no performance drawback, no endpoint management, no changes to workflows, and no agents.
- ShardSecure's technology separates data from infrastructure providers and administrators for confidentiality and compliance. The data owner can control exactly who has access to data in on-prem, cloud, and hybrid- and multi-cloud environments.
- Organizations can strengthen not only their data protection but also their data resilience with ShardSecure. Our technology offers high availability, virtual clusters, and self-healing data to reconstruct compromised data during outages and attacks.

Introduction

A cornerstone of data privacy and security is separating data from the infrastructure owners, cloud storage providers, and system administrators who would otherwise have access to it. This separation of duties is crucial to prevent leaks and breaches — especially since data leaks are most often caused by improper access credentials and abuse of administrative access. As one study shows, 83% of security professionals believe that sensitive data has accidentally been exposed at their organization.

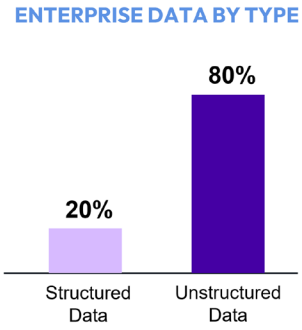
Separating data from third parties is also essential for maintaining compliance with cross-border data protection laws like the EU's General Data Protection Regulation (GDPR), financial regulations like the Sarbanes-Oxley Act (SOX), and guidelines from agencies like the National Institutes of Standards and Technology (NIST).

In the past, companies have achieved this separation of duties with agent-based file-level encryption. Today, though, 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 file encryption

Unstructured data: under-protected and at risk for breaches

Unstructured data — any file or collection of files that isn't stored in a structured database format — comprises at least 80% of all enterprise data. It comes in many forms, including text, image, video, audio, and web server logs, and it doesn't adhere to conventional data models.



Unstructured data is growing at a rate of 55 to 65% annually, four times faster than structured data. But it's still under-served in the encryption space.

Because of how unstructured data is stored in filesystems and blob stores, its privacy is reliant on the filesystem or the storage service it resides in. As a result, infrastructure providers, including cloud storage, local storage, and server administrators, often have access to unstructured data. When that easily accessed data also includes sensitive information like PII, mission-critical files, or trade secrets, companies can face major problems with confidentiality and compliance.

Traditional file-level encryption: slow for users and developers

Traditional file-level encryption provides strong access controls, but it has several major drawbacks.

First, the constant encryption and decryption of data often affects the performance of applications and slows down operations. Performance drawbacks with traditional file-level encryption can range from 5% to 40%.

Second, having to incorporate file-level encryption processes into the architecture of a new application can slow developer teams substantially. Key rotation, including regularly retrieving data to re-encrypt with new rotation keys, can be highly resource-intensive and cumbersome to implement.

Endpoint agents: resource-intensive and incompatible

The most common means of implementing file-level encryption has traditionally been to install agents, or software code, onto each device, server, and client system. 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.

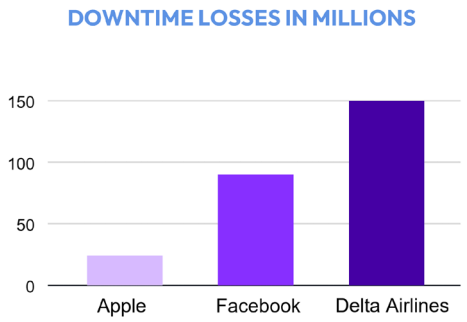
Agents can also present incompatibilities with newer architectures, including blob storage, S3 storage, K8s containers and many other cloud offerings. These architectures — as well as modern tools like network storage, cloud storage, Platform as a Service (PaaS) solutions, and containers — were not designed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

Lack of data resilience: causing costly downtime

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

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

Traditional file-level 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, integrity and availability suffer in attacks and outages.



Simpler, stronger file-level encryption with ShardSecure

ShardSecure provides advanced file encryption with no performance drawback, no resource-intensive management, and no agents. Our Data Control Platform allows companies to secure their unstructured 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 unstructured data

ShardSecure protects unstructured data in on-prem, cloud, and multi-cloud environments with our innovative approach to file-level 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 strips file content, filenames, file extensions, and all other metadata, meaning that there is not enough identifying information to reconstruct data.
- Our technology allows organizations to add a configurable amount of poison data to their real data.
- Our solution also requires multiple components to be used in concert with both each other and the complete dataset for reassembly, meaning that it's not possible for an unauthorized user to deploy their own instance of ShardSecure to reconstruct data.

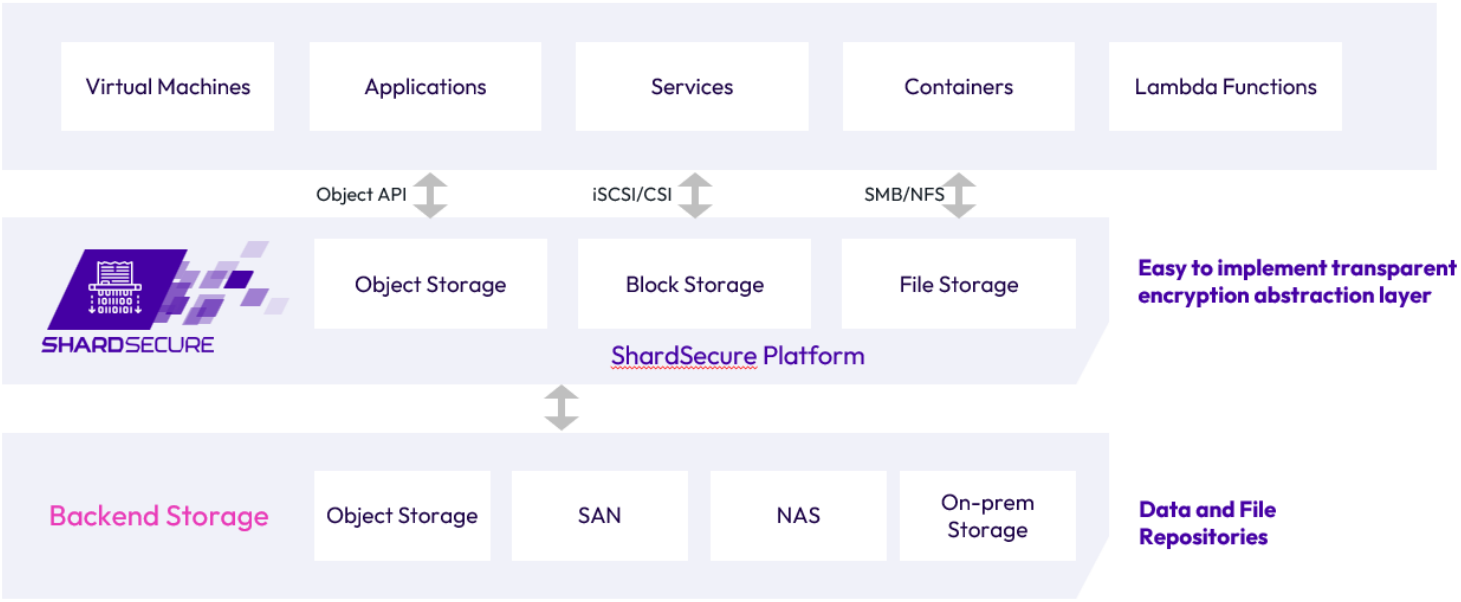
With ShardSecure, the data owner controls exactly who has access to their data, as well as where that data is stored. The result is strong privacy and protection for unstructured data, regardless of which third-party providers have access to it.

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, workflows do not change, and retraining is not necessary. Data on end devices can be accessed exactly as usual, with no visible changes to user or data workflows.

Additionally, ShardSecure is easy to manage and has a low impact on operations teams. Our encryption abstraction layer sits between an organization's applications and its infrastructure, where it performs advanced file-level enryption. The design is vendor-agnostic and works in the background as a zero-downtime event.



Fast performance for users and developers

Unlike agent-based performance drawbacks of up to 40%, ShardSecure's Data Control Platform introduces minimal to no performance drawbacks. Its low latency and fast throughput can sometimes even improve performance.

Additionally, developers can use ShardSecure for offloading file-level encryption. Rather than having to incorporate key rotation and management processes into their architecture, they can simply have their application read and write to ShardSecure's Data Control Platform, which will perform all the necessary security processes.

Strong data resilience for business continuity

In addition to guaranteeing the privacy of data, ShardSecure also strengthens data resilience. Unlike traditional solutions, which often focus on data confidentiality alone, our Data Control Platform ensures data integrity and availability.

Our self-healing data 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 costly downtime. It can even 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 — even in the face of ransomware attacks, cloud provider outages, misconfigurations, and more.

Conclusion: Are you ready to regain control of your data?

Unstructured data is growing, 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 file-level encryption. We protect data in the cloud 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 cloud cost savings and robust data resilience for outages and attacks. We make advanced file-level protection 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