SHARDSECURE

White Paper

Our Technology Explained

Executive Summary

ShardSecure helps companies regain control of their data in the cloud. This white paper discusses the product details and key use cases for ShardSecure's technology.

Key findings

- Organizations face challenges ranging from ransomware attacks and outages to rising cloud costs. As a result, they often lack the flexibility to store their data where they want.
- Protecting data from unauthorized access by attackers as well as storage admins and cloud service providers is key for maintaining compliance and confidentiality.
- Unstructured data is particularly underserved by traditional data protection solutions, which often slow performance, introduce complexity, and lack resilience features.
- Regulations like the EU's GDPR make a difficult data protection and environment even more challenging.
- With an economic downturn on the horizon, companies need data security solutions that solve a range of problems without increasing costs, complexity, or management burdens.
- ShardSecure helps organizations leverage the flexibility and cost savings of storing their data wherever they want — whether on-premises, in the cloud, or in hybrid-cloud architectures.
- With strong data privacy, agentless file-level protection, robust data resilience, support for cross-border regulatory compliance, native ransomware protection, and easy plug-and-play integration, ShardSecure's technology offers a multifaceted solution to a complex set of challenges.

Introduction

Until now, there have been few options for organizations to store their sensitive data exactly where they like while also preventing third-party access to that data. Enjoying the cost savings of the cloud can bring unwanted cloud storage admin access and unforeseeable outages; choosing the security of on-prem brings high costs and lack of flexibility.

Now, with companies under threat from everything from cybercrime to cloud outages to increasingly sophisticated RaaS attacks, the stakes have never been higher. Companies need a comprehensive data protection solution to cope with the myriad challenges of today's digital landscape — without draining their resources or adding complexity.

Growing data, rising costs

Unstructured data currently makes up at least 80% of all enterprise data and is growing at four times the rate of structured data. And yet, despite this rapid growth, the current solutions to secure unstructured data are slow and resource-intensive. With storage costs skyrocketing, and with data retention policies requiring organizations to store more and more data, companies need solutions fast. Strong file-level protection that enables both cost savings and compliance is a must.

Cross-border compliance

Data privacy has never been more important, with regulations like the EU's GDPR making a challenging environment even trickier. Unfortunately, most solutions can't keep up with changing cross-border data regulations. With the constant release of new guidelines like the EU-US Data Privacy Framework — not to mention new challenges to those guidelines like Schrems II and the likely Schrems III — compliance has become an ever-shifting target.

High-performance file protection for resource-strapped teams

Most common solutions address only a single aspect of privacy, protection, or resilience, but data security needs to extend to every part of the organization. With budget cuts looming, technologies that can address multiple pain points at once are in high demand.

Most data security solutions also slow down workflows and add complexity. They typically leverage decades-old technology like encryption, which introduces a significant performance hit and requires behavior changes from users, applications, or servers. These solutions often use agents, which are incompatible with newer architectures and difficult to scale.

Taken together, these challenges demand multifaceted solutions with high performance and easy management. Teams need to know they're investing in software that will address their greatest security challenges without slowing them down or adding unnecessary complexity.

ShardSecure's technology: a multifaceted data security solution

At ShardSecure, we believe that all organizations can enjoy the flexibility and cost savings of storing their data wherever they want — whether on-premises, in the cloud, or in hybrid-cloud architectures. With strong data privacy, native ransomware protection, robust data resilience, support for cross-border regulatory compliance, and easy plug-and-play integration, our technology offers a multifaceted solution to a complex set of challenges.

Below, we'll explain our technology's top use cases. We'll also explore our product details and key features to explain how ShardSecure enables companies to gain control of their data.

1. Agentless file-level protection

In the past, organizations have protected their data from third-party access with agent-based file-level encryption. But traditional agent-based solutions can slow performance by 5% to 40%. They are difficult to manage and scale, and they can be incompatible with newer workloads and cloud services.

ShardSecure offers an innovative alternative to agent-based file-level protection with no performance hit, no agents, and "set and forget" management. We secure data from threats without the cost and complexity of agent-based solutions, and we provide strong data confidentiality and resilience in the process.

Our API-based abstraction layer sits between your application and your infrastructure, where it performs advanced file protection. The design allows for an easy plug-and-play implementation without changes to data flows or user behaviors.

Our low latency and fast throughput has minimal to no performance drawbacks and can even improve performance. Data on end devices can be accessed and moved exactly as usual, with no visible changes and with strengthened confidentiality and resilience.

2. Cross-border data protection and GDPR compliance

A growing number of jurisdictional data privacy regulations makes it difficult for businesses to store data where they want. With strict cross-border data privacy laws like the EU's General Data Protection Regulation (GDPR), it's increasingly difficult for companies to protect their data, remain compliant, and still take advantage of cost savings in the cloud.

With ShardSecure, you can use the cloud storage providers of your choice, in the geographic locations and jurisdictions of your choice, to mitigate data transfer risk and address data sovereignty and compliance concerns. Data can be distributed across different regions of a single cloud provider, across multiple cloud providers, or across a hybrid mix of on-premises storage and one or more cloud providers.

ShardSecure also meets the requirements of Use Case 5 for Schrems II, part of GDPR compliance. Our technology is a split processing technology that can be easily deployed in a multi-party processing environment, meaning that it allows organizations to store and process data safely under Use Case 5.

As cyber audit and assurance firm UHY Advisors states: "ShardSecure has the potential to lower cyber risks and compliance costs while maintaining compliance with the spirit of European and US data protection regulations."

3. Neutralizing cloud ransomware

In the face of rising cyberattacks, ShardSecure offers early detection and transparent, real-time reconstruction of data that's been encrypted by ransomware. As soon as data fails a data integrity check, we send an alert to your security team for incident response and begin to automatically reconstruct affected data. This helps avoid disruption to users and reportable security breaches.

We also neutralize the impact of double extortion ransomware attacks, where criminals threaten to release or sell sensitive data that they've exfiltrated prior to encrypting it. With our technology, exfiltrated data will be unusable to attackers, since they cannot reconstruct any part of it.

Additionally, our configurable data migration feature allows companies to automatically migrate affected data to a safe alternate location. If a specified number of data integrity check failures take place, all the data in the affected storage location can be automatically migrated — in the background, with no downtime — to the secure location.

4. Robust data resilience

Everything from accidental misconfigurations to extreme weather and cyberattacks can cause companies to lose access to their most important data. ShardSecure mitigates that risk by keeping data available, accessible, and accurate in the face of tampering, deletion, outages, ransomware, and other unexpected events.

We help maintain high availability at multiple levels. Each instance of ShardSecure is a virtual cluster that can be run on-premises or in the cloud, and customers can configure two or more virtual clusters for failover.

We also help maintain strong data integrity with multiple checks for data integrity that detect unauthorized modifications, alert your security team, and automatically begin reconstructing data in real-time. This helps ensure that data remains accurate and unaltered, not just available.

5. Secure cold storage migration

ShardSecure allows companies to safely migrate their on-prem data to the cloud by rendering that data unintelligible to unauthorized users. With sensitive material protected from third party access, organizations can securely store that material in the cloud and enjoy the reduced hardware, maintenance, and licensing costs that accompany cloud adoption.

Organizations can also use ShardSecure to easily migrate their data to a new cloud provider, allowing them to change their storage options as they scale. Businesses remain in complete control of their data, including in hybrid- and multi-cloud environments, and they can move data among different storage locations with just a few clicks.

Additionally, our self-healing data can ensure that business continuity is not interrupted by cloud service outages and other provider issues.

6. Cloud storage optimization and cost savings

Choosing the right cloud storage solution can help companies cut costs and increase agility. Unstructured data is growing exponentially at 55% to 65% annually, and organizations are turning to cloud resource optimization to rethink their data storage and reduce their risks.

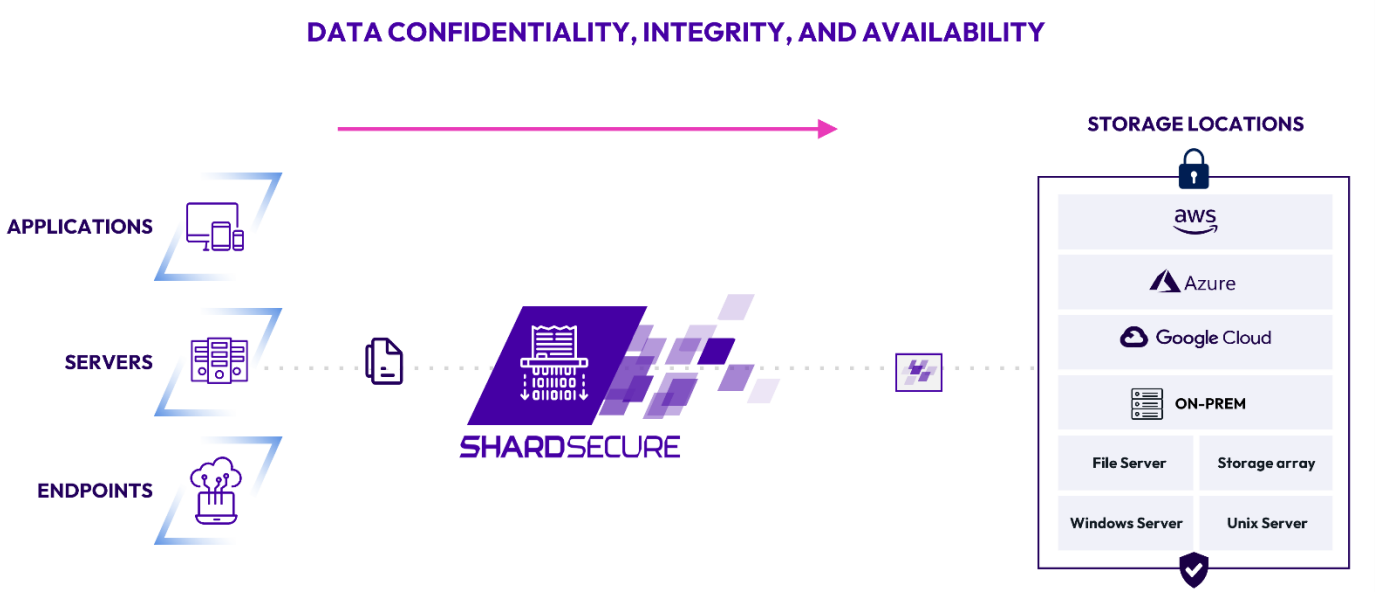
But many companies are stuck in more expensive storage tiers because of their legacy applications, which usually rely on block devices like hard drives or network attached storage. These applications typically need to be rewritten to support more cost-effective object storage.

ShardSecure allows organizations to optimize their cloud storage and protect their data in the cloud without rewriting applications or redesigning data flows. With ShardSecure's transparent plug-and-play technology, companies can easily leverage object storage like AWS S3 — while still enjoying vastly improved data security and EFS-level performance.

7. Additional use cases

Beyond the benefits we've listed above, ShardSecure also:

- Protects sensitive files so teams can collaborate safely and without losing functionality.
- Integrates with your existing cloud backup solutions to protect your assets and restore damaged data quickly and securely.
- Helps you save on operational costs with Bring Your Own Storage.
- Accelerates cloud migration and transformation initiatives, giving you the confidence that you're protected from common pitfalls like configuration errors and outages.
- And much more.



Key features and product details

Flexible storage options

Our technology offers significant flexibility for businesses to choose the type of storage systems that work best for them. With ShardSecure, your data can be distributed across different regions of a single cloud provider, across multiple cloud providers, or across a hybrid mix of on-premises storage and one or more cloud providers. We also make the number and location of your storage locations user-configurable, so your data can be stored in whatever geographic locations and jurisdictions you choose.

ShardSecure works with cloud providers ranging from AWS and Azure to Google Cloud Platform and Alibaba Cloud, giving organizations the freedom to embrace the infrastructure that best suits their needs. Whether they prefer to keep some data on-premises or use several different cloud providers in different parts of the world, companies can rest assured that their data will remain safe from unauthorized users.

While our front door emulates network-based storage, the secured side of our appliance places data in files and objects on real storage. We support a number of storage destinations, including:

- Local disk
- NFS drives
- Microsoft SMB shares
- Amazon EFS and S3
- FUSE
- Google Cloud Platform
- Microsoft Azure Object Storage
- IBM Cloud Object Storage
- Box
- Dropbox
- Alibaba Cloud

We've also designed our technology so that it's easy to add more storage providers to your setup. This means companies can be confident that they will be able to easily expand with or migrate to new providers in the future.

Ease of integration and access

Despite its powerful data security and resilience features, our technology has no significant impact on applications. ShardSecure is extremely easy to manage and has a low impact on operations teams. It also allows for 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, our technology simply looks like storage to applications. It is quick and seamless to integrate, with only one line of code change needed to get started.

Because our technology is transparent to users, workflows do not change. There are no visible changes to employee interfaces, and retraining employees or redesigning applications is completely unnecessary. This allows for seamless integration with your existing operations.

High performance

Introducing privacy and security almost always brings a performance cost. ShardSecure offers a rare exception in which adding data protection also generally improves overall performance. By reading/writing in parallel and compressing pointers, we are able to achieve high throughput and low latency.

Microsharding explained

Microsharding is the foundation of ShardSecure's patented technology. It was inspired by traditional data sharding, which is the process of fragmenting data into small pieces and then distributing those pieces to multiple storage locations for faster performance. Sharding has long been used by storage and database companies like Oracle, Altibase, and MongoDB, as well as tools like ElasticSearch and MySQL.

Our microsharding solution takes the benefits of traditional data sharding and adds numerous advantages for security and compliance. By shredding data into much smaller fragments, we make it impossible for unauthorized users to reconstruct that data. Unlike traditional shards, which typically range from a few thousand to a few million bytes in size and are large enough to contain dozens of social security numbers, our microshards can be as small as single-digit bytes. They are too small to reveal a social security number, credit card number, or even email address — and, as we'll discuss below, they're impossible for unauthorized users to reassemble.

Our microsharding solution is also highly customizable: Microshard size can be configured to eliminate the possibility of sensitive data and contextual metadata existing, and poison data can be added before microshards are distributed to the customer's storage locations.

Preventing unauthorized access

Our technology provides advanced data protection — even when storage locations are misconfigured or left open to attack by human error. It also separates storage admins and cloud providers from data access to support confidentiality and compliance.

In the unlikely scenario that a malicious actor is able to gain access to every storage location for a given data set, that data still can't be reconstructed. Here's why:

- Our technology strips file content, filenames, file extensions, and all other metadata, meaning that there is not enough identifying information for reassembly.
- 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 data set for reassembly; it is not possible for a third party to deploy their own instance of ShardSecure to reconstruct data.
- Lastly, our ShardSecure platform architecture is highly protected, making unauthorized reassembly of data impossible.

Conclusion

Data security and resilience have never been more important, and the threats to protecting data have never been greater. From economic concerns and the rising cost of cloud services to cyberattacks and cross-border compliance, the challenges faced by companies are wide-ranging and immense. Whether you're working on-prem, in the cloud, or in a hybrid architecture, your sensitive data needs to be kept safe and secure at all costs.

ShardSecure provides this security while keeping you in control of your data. With unbeatable file-level protection, strong data privacy, support for compliance with cross-border regulations like the GDPR, native ransomware protection, and robust data resilience, our technology keeps you safe and in charge.

For more information about ShardSecure, visit us online, follow us on social media, or schedule a demo.

@ShardSecure
@ShardSecure
@ShardSecure

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

info@shardsecure.com