White Paper

Top Use Cases & 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
• Unstructured data is particularly underserved by traditional data protection solutions, which often impact performance, introduce complexity, and lack data resilience features.
• Protecting data from unauthorized access by attackers as well as storage admins and cloud service providers is key for maintaining privacy, compliance, and confidentiality.
• Regulations like the EU’s GDPR and California’s CCPA make a difficult data protection environment even more challenging.
• Organizations face challenges ranging from ransomware attacks to outages. As a result, they often lack the flexibility to store their data where they want.
• 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. Leveraging the operational efficiencies of the cloud can bring unwanted cloud storage admin access and unforeseeable outages, while opting to store data on-prem can bring high costs and lack of flexibility.

Companies are under constant threat from cloud outages, increasingly sophisticated cybercrime, and other disruptions; the stakes have never been higher. Organizations need a comprehensive data security and privacy solution to cope with the myriad challenges of today’s digital landscape — without straining their already limited resources or adding complexity.

High-performance file protection for resource-strapped teams
Many data protection solutions address only a single aspect of privacy, security, or resilience, but data protection 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 tend to have an impact on workflows and add operational complexity. They typically rely on decades-old technology, like encryption, which introduces a significant performance impact and requires changes to user experience, applications, or servers. These solutions often use agents, which may be incompatible with newer architectures and difficult to scale.

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.

Privacy & compliance
Data privacy has never been more important, and regulations like the EU’s GDPR are making a challenging environment even trickier to navigate. Unfortunately, most traditional data security and privacy 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 challenges to those guidelines like Schrems II and the likely Schrems III — meeting compliance requirements has become a moving target.

**Growing data, rising costs**

Unstructured data 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 increase, current solutions for securing unstructured data tend to impact performance and are resource intensive. With storage costs skyrocketing, companies need solutions fast. Strong file-level protection that enables both flexibility and compliance is a must.

---

**ShardSecure’s Multifaceted Approach to Data Security & Privacy**

At ShardSecure, we believe that all organizations can enjoy the flexibility of storing their data wherever they want — on-prem, in the cloud, or in hybrid-cloud architectures. With strong data privacy, cloud 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 are ShardSecure’s top use cases. We’ll also explore 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 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 an easy plug-and-play implementation without changes to data or user workflows.

ShardSecure’s low latency and fast throughput architecture have minimal to no performance impact. Data on end devices can be accessed without requiring changes to existing applications.

2. **Meeting regulatory requirements for data privacy**

A growing number of jurisdictional data privacy regulations make 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), the anticipated Schrems III ruling, and CCPA/CPRA in the US, it’s becoming increasingly difficult for companies to protect their data, remain compliant, and take advantage of 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 the EDPB’s Use Case 5 in Schrems II. The ShardSecure platform 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. **Robust data resilience**

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

The ShardSecure platform maintains high availability at multiple levels. Each instance of ShardSecure is a virtual cluster that can be run on-prem or in the cloud, and customers can configure two or more virtual clusters for failover.
ShardSecure’s configurable data migration feature allows admins to automatically migrate data to a safe alternate location in the event that tampering is detected. If a specified number of data integrity check failures take place, all the data in the affected storage location can be automatically migrated to the secure location with no downtime.

4. Mitigate cloud ransomware
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. This ensures 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.

5. Protection for AI/ML models & training data
Given their importance, cost, and susceptibility to tampering, protecting AI/ML models and training data is becoming a priority for organizations. AI/ML models and training data are typically stored in the cloud with providers like AWS, Azure, and GCP, which can present unique data privacy risks. Cloud admin access to sensitive data means that companies must take additional security measures to keep these high-value models and datasets safe.

With ShardSecure, organizations can protect AI/ML models and training data in the cloud and in multi-cloud architectures. The platform prevents unauthorized access to data, allowing organizations to safeguard their AI and ML datasets without the complexities and overhead of traditional security solutions. With advanced data security, support for data sovereignty, robust data resilience, and simple integration, ShardSecure mitigates common threats to AI/ML models and training data integrity, such as exposure and tampering.

6. Additional use cases
Beyond the benefits listed above, ShardSecure also:
- Protects sensitive files so teams can collaborate safely and without losing functionality.
- Integrates with existing cloud backup solutions to further protect backup data.
- Accelerates cloud migration and transformation initiatives.
- Supports secure cold storage migration from on-prem to the cloud.

Key features & product details
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.

Microsharding augments the benefits of traditional data sharding by adding numerous advantages for security, privacy, and compliance. By shredding data into much smaller fragments, microsharding makes 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, 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 they are impossible for unauthorized users to reassemble.
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 customer storage locations as an additional layer of protection.

Preventing unauthorized access
ShardSecure offers advanced data protection — even when storage locations are misconfigured or are vulnerable to attack due to human error. The platform also separates storage admin and cloud provider access from data access to support privacy, confidentiality, and compliance.

In the unlikely scenario that a malicious actor gains access to every storage location for a given data set, that data still cannot be reconstructed, since ShardSecure:

- Strips file content, filenames, file extensions, and all other metadata, meaning there is not enough identifying information for reassembly.
- Allows organizations to add a configurable amount of poison data to their real data.
- Makes the unauthorized reassembly of exfiltrated data impossible.

ShardSecure also requires multiple components to be used in concert for data reassembly, making it impossible for unauthorized users or attackers to reconstruct the data.

Flexible storage options
The ShardSecure platform offers significant flexibility for businesses to choose the type of storage systems that work best for them. With ShardSecure, data can be distributed across different regions of a single cloud provider, across multiple cloud providers, or across a hybrid mix of on-prem storage and one or more cloud providers. It allows users to configure the number and locations of storage buckets, so data can be stored in any geographic location or jurisdiction.

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-prem 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.

The ShardSecure platform supports many storage destinations, including:

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

The platform also supports adding more storage providers to future-proof existing deployments.

Ease of 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.

High performance
Introducing privacy and security almost always brings a performance cost. ShardSecure is a notable exception. By reading/writing in parallel and compressing pointers, the platform achieves high throughput and low latency.
Conclusion

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 a hybrid- or multi-cloud architecture — it needs to be protected and secure at all costs.

ShardSecure provides this security and privacy while keeping you in control of your data. With agentless file-level protection, robust data resilience, advanced data privacy, support for compliance with cross-border regulations like the GDPR, and ransomware mitigation, 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.