

# Solution Brief

## ShardSecure for Data Backups

Learn how ShardSecure addresses common challenges with data backups, including cloud provider access, regulatory compliance, and resilience.



### Are your backups protected?

Enterprises rely on backups for disaster recovery, but protecting those backups can be challenging in multi-cloud environments. Historically, backups were kept in secure and air-gapped locations, but a true air-gapped approach is not possible in most modern-day environments (e.g., cloud services). As a result, logical air gapping has become necessary to prevent threat actors from tampering with data backups.

Ensuring data resilience for backups is also a challenge. It is inefficient to duplicate full backups across multiple clouds, but organizations must still eliminate single points of failure, such as relying on a single cloud provider and its associated availability, to ensure resilience. Organizations must also introduce solutions to secure backups so that unauthorized data deletion and tampering can be mitigated.

Lastly, organizations must maintain the privacy of their backup data. By nature, backup data contains sensitive data like financial records, customer information, and IP. If unauthorized parties gain access to these backups, the company suffers the same repercussions as a breach of the primary data sources. Additionally, data protection regulations require companies to safeguard their backup data from breaches, exfiltration, and potential misuse to ensure confidentiality and compliance.



### Protecting data backups with ShardSecure

The ShardSecure platform allows companies to secure their backup data in on-prem, cloud, and hybrid- and multi-cloud architectures. With an innovative approach to file-level encryption, the platform separates infrastructure administrator and cloud service provider access from sensitive data. Regardless of where they reside, backups are rendered unintelligible to unauthorized third parties.

### Ensure data availability and integrity in multi-cloud environments

The ShardSecure platform offers multi-cloud resilience for unstructured data at rest without the need for system or full data redundancy. It also offers several features to support data availability and integrity and can reconstruct compromised data in multi-cloud architectures.

To achieve high availability, each instance of ShardSecure is a virtual cluster, and customers can configure two or more virtual clusters for failover. To achieve data integrity, ShardSecure performs multiple health checks to detect unauthorized data tampering, including those made by ransomware attacks and malicious deletion. If a storage location fails a data integrity check, ShardSecure's self-healing feature automatically reconstructs the affected data in real time. This ensures business continuity and keeps backups available despite outages, downtime, and data compromise.

## Compliance with data privacy and security regulations

The EU's EBA (European Bank Authority) and Germany's BAFIN (Federal Financial Supervisory Authority) require organizations subject to SREP (Supervisory Review and Educational Process) to ensure that data backups are not affected by the same potentially damaging events as production data. These regulations stipulate that backup data be stored in separate infrastructure from production data to ensure that it will not be affected by any disaster. This is especially important if an organization relies on a single data center or single cloud provider for infrastructure. In case of a disaster, backup data needs to be accessible at all times.

Additionally, regulations like the GDPR require data privacy for backups that contain sensitive personal data. Without a strong data privacy solution in place, multinational and EU-based organizations may face compliance challenges when storing backups with US-based cloud providers.

The ShardSecure platform provides advanced data privacy for backups in the cloud. ShardSecure is validated by independent privacy attorneys to meet the requirements of Use Case 5 of the EDPB's recommendations for cross-border data transfers, allowing organizations to store EU personal data within a US cloud provider without violating the GDPR.

## Unified, multi-protocol platform across multiple clouds

ShardSecure supports interfaces like S3 for object storage, iSCSI for block storage, and SMB/NFS for file storage to integrate with commercially available backup solutions.

Since the ShardSecure platform acts as an abstraction layer, it can consolidate all storage interfaces into one, even though each cloud provider may support a different data storage interface. This approach reduces the complexity associated with migrating data to a multi-cloud architecture and implementing backup solutions across the enterprise.

## Learn more


In addition to securing data backups, the ShardSecure platform supports robust data resilience, cloud ransomware mitigation, protection for AI/ML models and training data, and regulatory compliance. To learn more about our technology, follow us on [social media](#) or visit us [online](#).



 @ShardSecure

 @ShardSecure

 @ShardSecure

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

 [info@shardsecure.com](mailto:info@shardsecure.com)

**SHARD  
SECURE**