

# Solution Brief

## Agentless file-level protection for AWS

Organizations devote significant resources to separating their data from their infrastructure owners for confidentiality, compliance, and security. Discover how we achieve separation of duties with no performance hit, no agents or endpoint management, and strong data resilience and privacy.



### Separating data access for confidentiality and compliance

In today's digital environment, companies are under pressure to separate data access from infrastructure owners, cloud administrators, cloud providers, and even unknown services within cloud providers. Data privacy and protection are paramount, and the separation of duties is fundamental to prevent leaks, breaches, and other forms of data compromise. Separating data access is also an important aspect of compliance with many cross-border data protection laws.

Historically, organizations have achieved this kind of separation with agent-based file-level encryption. But agent-based solutions are increasingly at odds with modern cloud technology like AWS. Although they offer strong protection, these solutions can slow performance and eat up security team budgets. 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 our easy and transparent plug-and-play software solution, we provide strong data confidentiality and resilience — while avoiding the need for agents altogether.



### File-level protection in AWS with ShardSecure

ShardSecure provides agentless file-level protection with no performance hit, no agents, and “set and forget” management. Our solution protects unstructured data and metadata in specific files, folders, or storage locations, and it separates this data from infrastructure owners to ensure strong confidentiality.

With the help of our agentless solution, companies can secure their data from internal and external threats without the complexities and overhead of agent-based encryption solutions. ShardSecure allows you to streamline your operations, mitigate the risk of data leaks, and improve security and resilience all at once.

### Separation of duties for confidentiality and compliance

With ShardSecure, you can control exactly who has access to your data in your cloud environments. Like encryption, we separate infrastructure admins from your data — but we do so in a less resource-intensive way. By splitting data into very small pieces (microshards) and then distributing those containers to multiple customer-owned AWS storage locations we ensure that data is unintelligible to unauthorized users, including cloud providers and other infrastructure admins.

See our [white papers](#) for more technical details.

## Agentless file-level protection

ShardSecure does not use agents, which means no endpoint management, no struggles with installation or configuration, and no competition for processing power. Unlike agent-based file-level encryption, which introduces performance drawbacks ranging from 5% to 40%, ShardSecure involves minimal to no performance drawbacks. (In some cases, its low latency and fast throughput can actually improve performance.)

Instead, our agentless solution sits between your application and your infrastructure, where it performs advanced file protection. There are no agents, and data on the end devices can be accessed and utilized exactly as usual, with no visible changes to user or data workflows.

## Stronger protection with fewer resources

ShardSecure was designed to be extremely easy to manage. A plug-and-play approach, it provides an easy and transparent implementation via common interfaces within AWS with no need to change user behaviors or data flows. Without the overhead and complexity of traditional file-level encryption, it is vendor-agnostic and appears to other applications as a storage location.

All of this translates to a low impact for operations teams. Our solution works in the background as a transparent, zero-downtime event, and data confidentiality is achieved without expending significant resources on running and maintaining complex systems.

## Strong data resilience

Unlike traditional solutions, which often focus on data confidentiality alone, ShardSecure also ensures strong data resilience. Our self-healing data feature detects when data is lost, deleted, tampered with, or otherwise compromised in ransomware attacks, cloud provider outages, and more.

If a problem is detected, we reconstruct the affected data automatically and transparently, returning it to its original state without costly downtime or disruption to users. As a result, organizations can maintain their critical operations, avoid reportable security breaches, and prevent any loss of data or data access.

## Learn more

ShardSecure integrates seamlessly with your existing applications and with AWS for ease of deployment. We support secure cold storage migration, neutralize cloud-based ransomware, and offer high availability in the face of outages, attacks, and other disruptions.


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**