SHARDSECURE

# Solution Brief

Data resilience has massive implications for companies worldwide.

In a global study by Opengear, 31% of senior IT respondents reported losing more than $1 million in the past year due to outages.

23% of respondents reported a significant increase in network outages over the past five years.[1]

According to IBM's 2021 Cyber Resilient Organization Study, 51% of respondents reported a significant data breach within the past year and 61% paid a ransom in a ransomware attack.

Only 35% of respondents had a plan for disaster recovery in fiscal year 2021.[2]

[1] Measuring The True Cost Of Network Outages. Opengear. Retrieved August 12, 2022, from https://opengear.com/infographics/measuring-the-true-cost-of-network-outages/

[2] Cyber Resilient Organization Study 2021. IBM. Retrieved August 12, 2022, from https://www.ibm.com/resources/guides/cyber-resilient-organization-study/

# ShardSecure Strengthens Data Resilience in the Cloud

Companies looking to strengthen their data resilience can use our patented Microshard™ technology in multi-cloud and hybrid-cloud environments.

## What Data Resilience Means for Companies

Strong data resilience means that organizations are able to maintain their operations in the face of unexpected events like cyberattacks, network outages, data theft, and more. Without data resilience, those organizations may suffer outages, lower performance, losses of revenue, and sometimes even reputational damage from interruptions to business continuity. Outages may also leave some companies in violation of service level agreements that promise a certain amount of uptime or availability.

Achieving data resilience in the cloud brings an added layer of complexity. Although a cloud provider's infrastructure typically offers some resilience, organizations may still be affected by whatever outages and attacks the provider experiences. Lack of clarity within the shared responsibility model may also lead to potential weaknesses in data resilience, leaving organizations vulnerable.

Given how multifaceted it is, data resilience in the cloud can be difficult to achieve. While data security solutions typically protect data privacy and confidentiality, they don't always ensure that protected data will be available during an outage. Indeed, many tools to protect data at rest — like common encryption and tokenization and anonymization products — don't address data resilience at all.

## Strengthening Data Resilience with Microsharding

Microshard technology offers features like self-healing data to ensure data resilience in the face of tampering, deletion, outages, ransomware, and other unexpected events. The solution works transparently and in real-time to distribute data in multi-cloud and hybrid-cloud configurations, improving resilience.

ShardSecure helps maintain high availability at multiple levels. First, each instance of ShardSecure is a virtual cluster that can be run on-premises or in the cloud. Second, customers can configure two or more virtual clusters for failover. This means that organizations are not reliant on a certain piece of data being in a single place — or even on a single cloud provider being available, as long as they distribute their data across multiple providers.

## ShardSecure Maintains Data Integrity and Availability

Through its three-step process, Microshard technology helps ensure both data integrity and data availability, two fundamental components of data resilience.

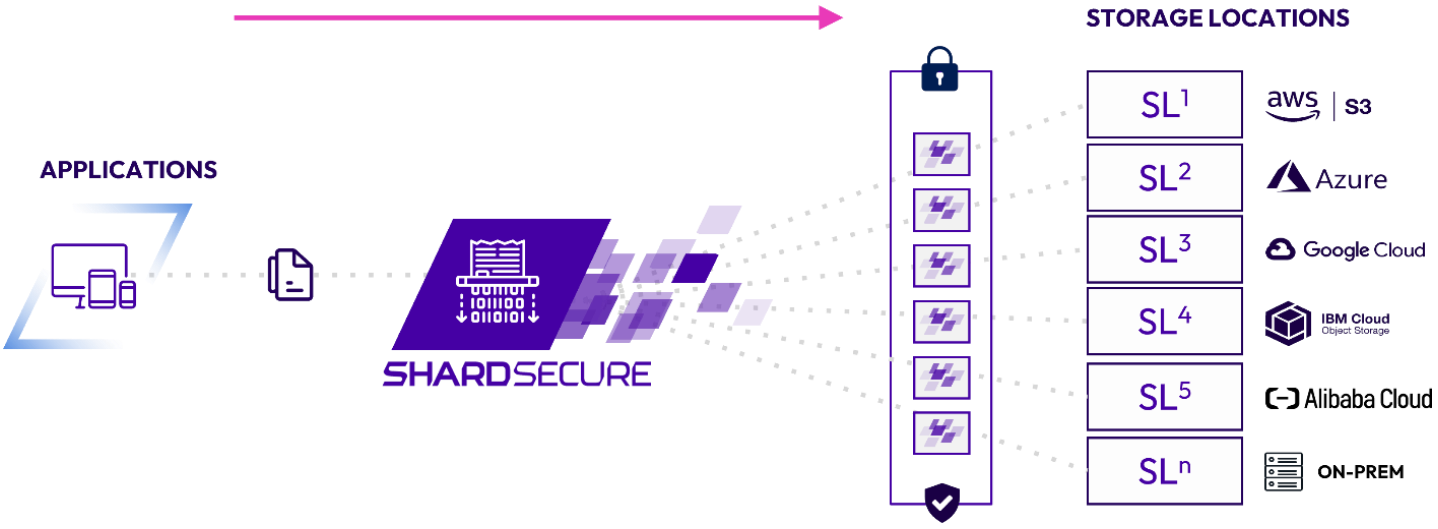


*Figure 1 - During ShardSecure's three-step microsharding process, Microshard data is shredded into four-byte microshards, mixed into multiple logical containers, and distributed to multiple storage locations of your choosing to help ensure that no one location contains any identifiable data.*

**Shred:** Microshard technology begins by shredding data into four-byte microshards that are too small to contain a birthdate, an ID number, or any complete piece of sensitive data.

**Mix:** Next, poison data is added and the microshards are mixed into multiple logical Microshard containers. Identifying information like file extensions, file names, and other metadata is also removed.

**Distribute:** After being mixed, the Microshard containers are distributed across multiple customer-owned storage repositories in multi-cloud or hybrid-cloud configurations.

## Data Integrity

While some data resilience solutions focus only on data availability, ShardSecure offers multiple checks for data integrity as well. Using an automated control, these data integrity checks respond to unauthorized modifications by reconstructing data to its earlier state.

If a Microshard container fails a data integrity check during the reassembly process, the security team is alerted and the affected container is reconstructed. This helps ensure that available data is also accurate, unaltered data. If it's not, the recovery process can then begin transparently and without manual intervention.

## Learn More

Visit us at https://shardsecure.com for more information and to schedule a demo.


@ShardSecure
@ShardSecure
@ShardSecure

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

info@shardsecure.com