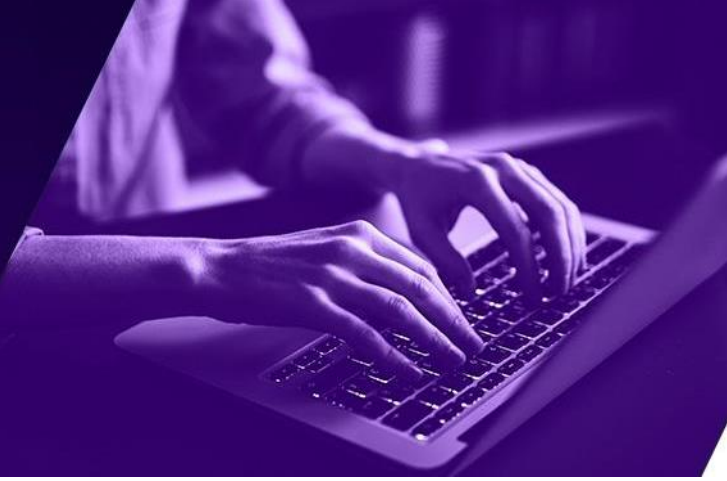# SHARDSECURE

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/

Strengthening Data Resilience in the Cloud

Companies can use ShardSecure for strong data security and resilience in the on-prem, cloud, or hybrid- and multi-cloud environments of their choosing.

Data resilience in a complex digital landscape

Strong data resilience allows organizations to maintain their operations in the face of unexpected events like cyberattacks, network outages, data theft, and more. Depending on the context, resilience can encompass anything from data integrity and availability to disaster recovery, redundancy, backups, and more.

The consequences of weak data resilience are myriad: outages, revenue loss, violations of SLAs, reputational damage, and loss of business continuity. But achieving strong data resilience can be challenging.

While data security solutions typically protect data privacy and confidentiality, they don't always ensure that data will be available during an outage or unaltered by attacks. Many tools to protect data at rest, including common encryption and anonymization products, don't address data resilience at all. Resilience is further complicated by the shared responsibility model in the cloud, which can lead to a lack of clarity about data protection duties. Luckily, new technologies can provide an answer to these challenges.

Strengthening data resilience with ShardSecure

Everything from accidental misconfigurations to cloud provider outages can cause companies to lose access to their mission-critical data. ShardSecure mitigates that risk by keeping data available in multi-cloud and hybrid-cloud configurations. Our technology provides strong data resilience in the face of tampering, deletion, outages, ransomware, and other disruptions.

Self-healing data

ShardSecure's self-healing data offers a RAID-like ability to reconstruct data that is lost, deleted, compromised, or unavailable. Our technology distributes data to multiple customer-owned storage locations, so when data in one location is damaged, it can be rebuilt using the other locations. All in all, organizations can lose up to half of their data and still reconstruct it. The feature also works transparently and automatically so that business continuity is maintained and users can continue accessing data without interruption.

Promoting high availability

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.

Our high availability extends to multi- and hybrid-cloud environments that use a mix of on-prem, private cloud, and public cloud services. With our technology, you can avoid infrastructure redundancy — duplicating data and systems across multiple data centers or cloud providers — and rest assured that your data will remain safe during outages, attacks, and more.

Maintaining data integrity

While some data resilience solutions focus only on data availability, ShardSecure offers multiple checks for data integrity as well. These data integrity checks respond to unauthorized modifications by automatically and transparently reconstructing data to its earlier state and alerting security teams for incident response. This ensures that a company's available data remains accurate and unaltered as well.

Learn More

ShardSecure integrates seamlessly with your existing security controls and cloud storage providers for ease of deployment. In addition to offering strong data resilience, we provide agentless file-level protection, neutralize cloud ransomware, support secure cold storage migration, and help companies meet compliance with cross-border data protection laws like the GDPR.

To learn more about our technology, follow us on social media or check out our resources page.
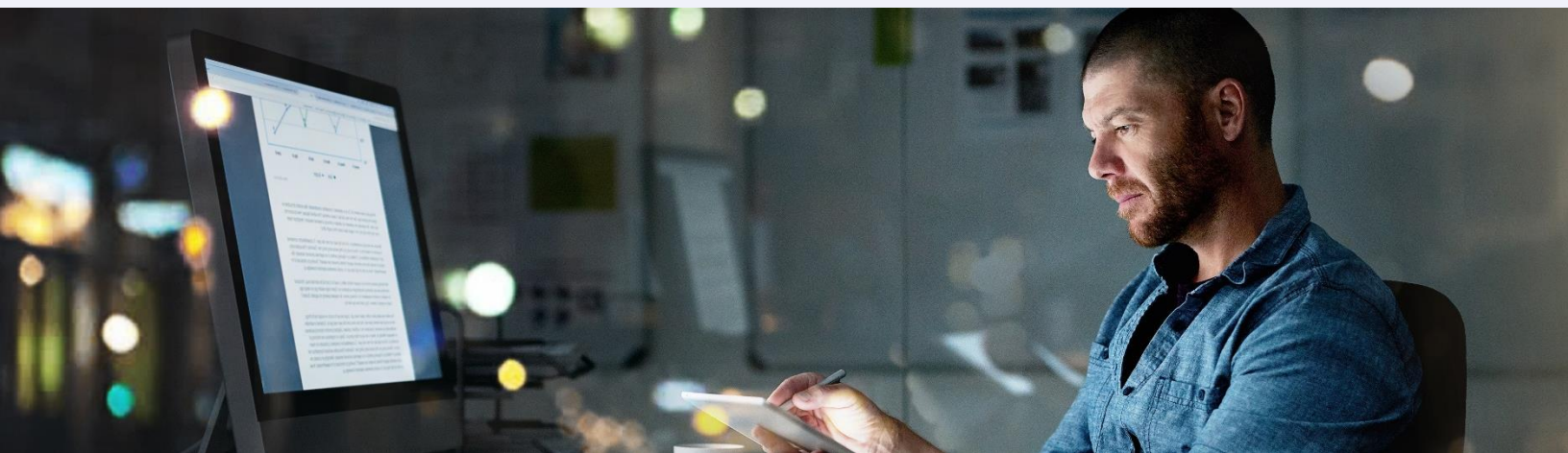
in @ShardSecure

f @ShardSecure

y @ShardSecure

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

✉ info@shardsecure.com

SHARD SECURE