SHARDSECURE

White Paper:

Strengthening Data Resilience

The high cost of inadequate data resilience

Data resilience is vital. It allows organizations to maintain operations during major disruptions and quickly recover. It helps ensure business continuity in the face of unexpected disruptions, including cloud provider outages, natural disasters, ransomware attacks, and more. And it often helps companies minimize or avoid revenue loss from downtime.

Many organizations underestimate just how costly inadequate data resilience can be. According to one study, the average cost of a critical server outage in 2019 was between $301,000 and $400,000 per hour.

The prices of weak data resilience are also rising: A 2016 study by the Ponemon Institute revealed that the average cost of a data center outage rose from $505,502 in 2010 to $740,357 in 2015, a 38% increase. And that's not to mention the cost of ransomware attacks, which can similarly compromise data availability and cost an average of $4.35 million per attack.

THE HIGH COST OF DATA OUTAGES

Over **60%** of failures in **2022** have resulted in at least **$100,000** in total losses, up substantially from **39%** in **2019.**

The share of outages that cost upwards of **$1 million** has increased from **11%** to **15%** from **2019** to **2022**.

Outage trends suggest there will be at least **20** serious, high-profile IT outages worldwide in **2023**.

*Statistics taken from the 2022 Uptime Institute Global Survey of IT and Data Center Managers.

Current challenges in the data resilience landscape

Below, we'll explain the top threats to two cornerstones of resilience, data integrity and data availability. We'll also explore the different models for redundancy and the reasons that data backups are no longer enough to ensure business continuity.

Common challenges to data integrity

Data integrity refers to the accuracy, consistency, and reliability of data. It means that every file is byte-for-byte identical to the file that was written, with no corruption, tampering, or modification by unauthorized users.

Common data integrity threats include:

- Human error
- Misconfigurations
- Hardware failures
- Software bugs
- Insider threats
- Malware, ransomware, and other cyberattacks

To protect data integrity, many organizations use traditional encryption solutions, which prevent unauthorized modifications to data. However, these solutions can be resource-intensive, and they do not maintain data availability during outages or attacks. This makes traditional encryption an incomplete solution for data resilience.

Common challenges to data availability

High availability — the ability to operate continuously without a single point of failure — is key to achieving data resilience. Although it doesn't prevent outages, cyberattacks, or other major events, high availability does ensure that business operations can continue in the face of disruptions.

Common data availability risks include:

- Infrastructure failure
- Infrastructure overload
- Hardware failure
- Software glitches
- Errors in data access controls
- Network outages
- Ransomware and other cyberattacks

To achieve high availability, organizations may employ solutions ranging from a basic backup or a few spare servers to a fully redundant network infrastructure with automatic failure detection.

The shift to data redundancy

In the past, organizations achieved resilience by making their systems redundant, typically with a primary data center and a backup data center that contained all of the same infrastructure, devices, and settings. By duplicating entire components or systems across multiple data centers, companies could ensure that their data would remain available and accurate even if one system or storage location went down.

However, with the explosive growth of data and the rising cost of cloud storage, infrastructure redundancy is no longer a cost-effective model. Companies no longer want to pay for the VPNs, internet service, firewalls, fire servers, and other backup storage systems and devices required for this type of redundancy.

Instead, many organizations are turning to data redundancy. This model requires companies to duplicate only their data across multiple cloud storage providers, helping save money on infrastructure costs.

Still, even the data redundancy model requires organizations to double up on storage fees, since they are storing the same volume of data with at least two cloud providers. This has led some companies to look for new ways to achieve data redundancy without paying for full backups across multiple clouds.

Why backups aren't enough

Many organizations fall into the trap of believing that their backups are sufficient to ensure data resilience. While maintaining and protecting backups is an important part of data resilience, it's only one component of a much larger strategy that includes monitoring, data redundancy, regular testing, disaster recovery, and more.

Both data backups and data resilience can work to restore a company to full functionality. But relying solely on data backups will result in a much slower and costlier recovery than having a strong data resilience solution.

Data backups	Data resilience
A company can eventually rebuild its files and systems after a disruption — provided its backups were not stored in a compromised location.	A company's systems and files can continue functioning immediately after a disruption.
The timeframe for recovery may be days, weeks, or even months.	Without the need to restore from backups, the timeframe for recovery is very short, with little to no downtime or loss of revenue.

Achieving strong data resilience with ShardSecure

ShardSecure's Platform offers strong data resilience for unstructured data at rest. Our technology provides data redundancy without the need for full data backups, helping companies lower storage costs.

Our technology also offers several features to support data integrity and availability, including the ability to reconstruct compromised data in a wide variety of environments.

Achieve high availability in on-prem, cloud, and multi-cloud environments

ShardSecure achieves high availability at multiple levels. First, each instance of ShardSecure is a virtual cluster that can run on-premises or in the cloud. Second, customers can configure two or more virtual clusters for failover. We can achieve this high availability across multiple clouds as well as in hybrid-cloud environments that use a mix of on-premises, private cloud, and third-party public cloud services.

Ensure accuracy with multiple data integrity checks

While traditional data resilience solutions focus only on data availability, ShardSecure offers multiple checks for data integrity as well. These data integrity checks detect unauthorized modifications, including those made by ransomware attacks and malicious tampering.

Reconstruct data to maintain business continuity — no backups needed

By creating slight overlaps of distributed data across different storage locations, the ShardSecure Platform can rebuild compromised data in real-time. This self-healing feature means that organizations can lose up to half of their data and still reconstruct it.

This feature also works during outages and downtime. If a data storage location becomes unavailable for any reason — a cloud provider issue, a misconfiguration, etc. — the same process reconstructs the unavailable data. This process happens transparently and automatically to maintain business continuity.

Easy, agentless integration

The ShardSecure Platform does not require the use of agents, providing advanced file-level protection without complicated integration or management. It also allows for instant data access and fast data migration with just a few clicks.

ShardSecure is easy to manage and has a minimal impact on operations teams. It offers transparent implementation with no need to change user behaviors or data flows. It is quick and seamless to integrate, with minimal code changes needed for integration.

Conclusion

Given the continued acceleration in digital transformation, legacy approaches to data resilience are no longer adequate. Companies need to adopt new strategies and technologies to ensure the continued integrity and availability of their critical data.

ShardSecure's Platform offers an innovative approach to data resilience. With its self-healing data, high availability, data integrity checks, and more, our technology can keep your unstructured data accurate and available — regardless of where you choose to store it.

For more information on how ShardSecure is improving resilience for companies in financial services, healthcare, and more, take a look at our other data resilience resources or schedule a demo today.

@ShardSecure
@ShardSecure
@ShardSecure

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

info@shardsecure.com