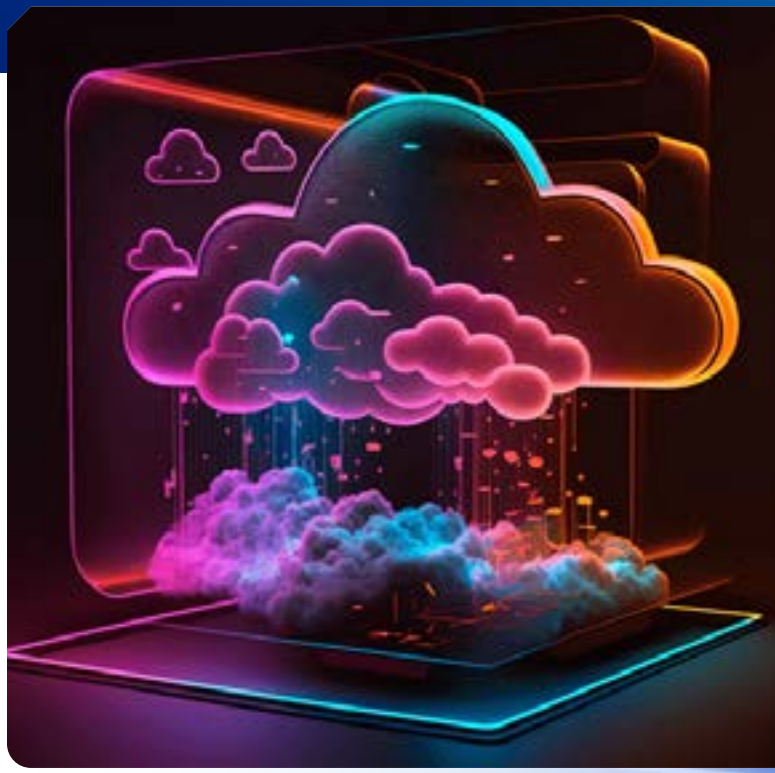
arcserve®

Everything You Need to Know About Data Resilience

Table of Contents

McKinsey Offers Survival Guide for Technology and Data Resilience



McKinsey recently released its “technology survival guide for resilience,” no doubt because that’s what consumes just about every business leader and IT pro to some degree these days.

The guide starts with this definition: “Resilience means understanding the criticality of a business process, the capability of the underlying technology, the business impact if the technology fails, and the organization’s risk tolerance.”

A 2022 study by ITIC found that the hourly cost of downtime exceeded $300,000 for 91 percent of enterprises of all sizes. And 44 percent of midsize and large enterprise survey respondents said that a single hour of downtime could cost their businesses over $1 million. So, if, as McKinsey writes, a technology fails, it can be costly.

Resilience Requires Understanding Criticality

The McKinsey guide states that to achieve resilience, your organization needs to understand the criticality of a given process. You then need to assess the underlying technology, identify the business impacts of a failure, and establish your organization’s risk tolerance—as well as your partners’.

The guide notes that, to get there, “an organization needs to understand where and what its resilience is today and be able to answer the question: Could we recover and rebuild after a catastrophic event?”

Put in context, Sophos’ The State of Ransomware 2022 found that 66 percent of responding IT pros from around the world said their organization had been hit by ransomware in the previous year, and 65 percent of those attacks resulted in data encryption. Meanwhile, the Uptime Institute’s 2022 Outage Analysis found that 80 percent of data center managers and operators have experienced some outage in the past three years.

Technology Resilience Principles

McKinsey also shares the foundational principles for maintaining resilient technology:

Applications, systems, platforms, and the IT workforce are flexible and scalable.

- Data sets, applications, and network technology infrastructure are fully visible to data owners, and applications are traceable within the environment.
- Data sets and applications are built to be agile and mobile.
- The architecture of applications, data platforms, network environment, and the IT workforce is resilient by design, i.e., the architecture is built to compensate for probable failures and inform future designs.
- Systems are interoperable and leverage standard API approaches that are defined and well-architected internally and between third-party services.

Resilience Maturity: Architecture by Design

McKinsey says that "resilience capabilities fall on a maturity spectrum from simple redundancy to duplicate servers through to advanced capabilities with resilience built into the architecture by design." They break this spectrum into four areas:

- Architecture and design
  Mature organizations incorporate technology resilience into enterprise design and architecture.
- Deployment and operations
  Resilient operations need to consider not only operational contingencies like disaster recovery but also the root cause of incidents.
- Monitoring and validation
  Mature organizations use proactive and predictive approaches that stress-test solutions, disaster response, and contingency plans.
- Response and recovery
  Mature technology resilience ensures a fast response to incidents as they occur while learning from operations, industry trends, and disasters in a continuous feedback loop.

Building a Resilient Organization

There are three areas where McKinsey says to start and grow a more resilient technology environment:

- Establish a blame-free culture, so when problems happen, instead of pointing fingers, everyone works toward solving the problem.
- Use metrics to measure performance and focus on the incidents they identified, like unpatched software, to avoid repeating incidents.
- Rehearse the outage so you can anticipate problems and iteratively prepare for and train your team to respond to complete system outages.

The McKinsey guide, which you'll find here, offers a wealth of valuable information for organizations on their technology resilience journey.

Make Data Resilience a Priority

While establishing technology resilience is an organization-wide endeavor, ensuring data resilience tends to fall to IT. That's where Arcserve is a game changer. Arcserve delivers data resilience with the broadest set of best-in-class solutions to manage, protect, and recover all data workloads, from SMB to enterprise, regardless of location or complexity.

Arcserve solutions eliminate complexity while bringing cost-effective, agile, and massively scalable data protection, and certainty across all data environments. This includes on-prem, off-prem (including backup as a service [DRaaS], backup as a service [BaaS], and cloud-to-cloud software as a service [SaaS] backup), hyper-converged, and edge infrastructures.

Get expert help on your technology and data resilience journey by working with an Arcserve technology partner. To learn more about Arcserve products, contact us.

5 Steps You Must Take To Ensure Data Resilience (And Why #5 Might Surprise You!)

Data resilience is the talk of IT these days and for good reasons. Data breaches continue to soar—IT Governance recently posted that its research identified 100 publicly disclosed incidents just in March 2023, accounting for 41,970,182 breached records.

Meanwhile, Sophos' State of Ransomware 2023 report found that 66 percent of those surveyed said their organizations were hit by ransomware last year, with 76 percent of those attacks succeeding in encrypting the victims' data.

Data Resilience: Preparing for the Worst

With so many threats, ensuring your data is resilient is the only way to ensure your organization can spring back from any attack, breach, natural disaster, hardware failure, or other incident. While many IT pros may think of data resilience as data recovery, the difference between the two is straightforward: data resilience is proactive, while data recovery is reactive.

So, what should you do to ensure your organization's data is resilient and always available when needed? Here are five steps to get you there.

1. Strengthen Your Security Posture

As we said, data resilience is all about being proactive. That starts with implementing a comprehensive approach to cybersecurity and data protection. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is an excellent resource for doing so, offering standards, guidelines, and best practices to manage security risks.

Then there's ISO/IEC 27001, the world's best-known standard for information security management systems (ISMS), which provides companies of any size with guidance for establishing, implementing, maintaining, and continually improving ISMS.

While these frameworks cover most of the areas you need to consider as you enhance your data security, here are some specific areas where improvements can make a significant difference:

- Conduct regular risk assessments to identify potential vulnerabilities, threats, and risks so you can prioritize your security efforts and allocate resources accordingly.
- Implement strong access controls, including multifactor authentication (MFA) and the principle of least privilege, granting users only the minimum access required for their roles.
- Encrypt all sensitive data in transit and at rest.
- Regularly update and patch systems to ensure vulnerabilities that hackers often exploit are removed.
- Train your employees in security best practices, including how to recognize ransomware and other social engineering schemes and what to do if they encounter anything suspicious.
- Implement robust firewall and intrusion detection/intrusion prevention systems (IDS/IPS) to detect and prevent unauthorized access or malicious activities within your environment.
- Conduct regular security audits and assessments and add a security information and event management (SIEM) system to collect, monitor, and analyze security logs.

2. Develop (Or Update) Your Comprehensive Disaster Recovery Plan

A well-defined disaster recovery plan is crucial for minimizing downtime and ensuring you can quickly get operations back up and running. Your plan should include your data backup strategy—including your RPOs and RTOs—and detailed procedures for data restoration, system recovery, and business continuity. Regular testing and updating of your disaster recovery plan is essential for ensuring it will be effective as your business evolves.

3. Implement an Effective Backup Solution

Data backups are fundamental to achieving data resilience. The 3-2-1-1 backup strategy is the best way to ensure your backups are always safeguarded and available. And it's pretty simple. Keep three copies of your data (one primary and two backups), with two copies stored locally in two formats and one copy stored offsite in the cloud or secure storage. The last one stands for immutable storage, where your backups are saved in a write-once-read-many-times format that can't be altered or deleted. Immutability is different from encryption in that there is no key, so there should be no way to "read" or reverse the immutability. That gives you a last line of defense against any disaster.

4. Embrace the Cloud

The cloud offers unmatched scalability and flexibility. Cloud services like AWS also provide solutions like S3 Object Lock, an immutable format that lets you take advantage of the cloud without sacrificing security. And cloud-based disaster recovery solutions like Arcserve SaaS Backup and Arcserve Disaster Recovery as a Service (DRaaS) offer you rapid recovery with automated backups and replication to multiple data centers so that even if a local disaster strikes, your data remains accessible.

5. Harness the Benefits of Tape Backup and Air Gapping

You may be surprised to learn that magnetic tape was created in 1928. Let that sink in. But it wasn't until the 1950s that the technology was applied to data storage on mainframe computers.

So why are we talking about a technology nearly 100 years old? Because it still works—very well. Tape is an excellent option for long-term data archiving and is especially effective for offsite, air-gapped storage—whether you use a virtual or physical air gap. Tape is also very cost-effective for large volumes of data. That may be why the global tape market is projected to grow to nearly $4.24 billion by 2027, a CAGR of more than 7 percent.

With your data air-gapped and stored offsite on tape, you have one more reliable option for disaster recovery if all of your other options fail.

Choose Backup Software Built for Tape

Arcserve Tape Backup offers powerful tape backup software for your high-capacity storage. The software centralizes management and storage resource manager (SRM) reporting, so you can monitor all backup activities, find the nodes that are taking the longest, locate backed-up data, and track volume, disk, and memory usage on every production server. It also incorporates sophisticated functionality for VMware, Microsoft Hyper-V, and Citrix XenServer platforms.

Most importantly, Arcserve Tape Backup software lets you quickly restore individual application objects from Active Directory, Microsoft Exchange, Microsoft SQL Server, and Microsoft SharePoint. And it delivers faster, more efficient backups and restores with UNIX and Linux data movers for storage-area network (SAN)-based backups.

Arcserve Tape Backup is versatile, too, meeting application-specific requirements with backup to disk, backup to tape, disk-to-disk-to-tape (D2D2T), disk-to-disk-to-cloud (D2D2C), virtual tape library (VTL), hardware snapshot support, multiplexing, and multi-streaming.

For expert help with ensuring your organization's data is resilient, and you can recover from any disaster, choose an Arcserve Technology Partner.

Why Your SaaS Data Needs a Backup Plan: The Importance of SaaS Data Resilience

Salesforce, Microsoft Office 365, and Google Workspace may be a few of the names that come to mind when you think of software as a service (SaaS). But SaaS is the primary way software is consumed these days, with Zippia saying that by the end of 2023, 99 percent of companies will be using at least one SaaS solution.

In a survey of more than 700 IT and security professionals by SaaS management software company BetterCloud, 43 percent of respondents said they had added a new SaaS app that stores sensitive data in the previous 12 months.

SaaS is today's solution of choice—and where many businesses' critical data is being generated. The reasons for this are many, but simplicity, convenience, scalability, and cost savings are just a few.

SaaS Data and the Shared Responsibility Model

The security risks related to SaaS applications and data aren't lost on IT pros. The BetterCloud survey's good news is that most IT pros understand the shared responsibility model: 81 percent of respondents say they are responsible for protecting sensitive data within SaaS apps.

They understand that while SaaS providers handle data availability and security, they don't always provide comprehensive data backup and recovery solutions. And they typically have limited data retention periods, lack protections against accidental deletions, and may not offer recovery options for all types of data.

But 43 percent of the BetterCloud respondents say they have difficulties securing users' activities within SaaS apps.

The Hacker News says the top five SaaS security challenges include SaaS misconfigurations, access risks, device risks, identity and access governance, and identity threat detection and response (ITDR). Each of these threats, among others, can lead to a data breach, ransomware attack, or some other data disaster. Power outages, hardware failures, and network failures can also make SaaS platforms inaccessible, leading to downtime and lost productivity.

Data Resilience for Vital Applications

SaaS providers' data protection efforts can't ensure data resilience and disaster recovery. Another layer of protection is required.

That's where SaaS backup makes all the difference. With SaaS backup, your data is stored offsite, so you can quickly recover it and get operations back up and running. But not all SaaS backup solutions are created equal.

Arcserve SaaS Backup: Complete Protection for SaaS Data

When choosing a SaaS solution, disaster recovery best practices come into play. Look for a reliable and reputable backup solution that fits your specific requirements. Arcserve SaaS Backup offers complete protection for data stored in Microsoft 365, Microsoft 364 Azure AD, Microsoft Dynamics 365, Salesforce, and Google Workspace.

Arcserve SaaS Backup slashes the time IT teams spend managing and protecting SaaS data with a simple setup that takes less than five minutes before starting protection. All backup and data protection activities are handled via a single pane of glass. Security is built in, with multi-tenant and role-based access controls. And your data is encrypted in transit and at rest.

Compliance is also simplified with guaranteed data sovereignty that stores four copies of your backups in two different data centers within the same region.

Immutable Backups and Automatic Application Updates

Arcserve SaaS Backup features immutable backups, where your data is saved in a write-once-read-many-times format (WORM) using a blockchain-based algorithm. Immutable backups can't be altered or deleted, ensuring ransomware resilience. Arcserve SaaS Backup offers 30-day delete retention, protecting you from accidental deletions and ransomware attacks. And the backup application is automatically updated without impacting active jobs.

Regular testing and validation of your backups are crucial to ensuring your backed-up data can be restored when needed. Arcserve SaaS Backup makes that easy, too.

Get Advice from SaaS Experts

Arcserve technology partners include experts who can help guide you through the process of strengthening your SaaS data resilience and ability to recover from any disaster. Find an Arcserve technology partner here.

And check out our no-obligation, 30-day free trial of Arcserve SaaS Backup.

Immutable Storage: The One Solution That Ensures Data Resilience Across Multicloud and Hybrid-Cloud Environments

Your business likely relies increasingly on the cloud to manage your data as you address more pressing concerns like data security and resilience.

That's especially true if you're responsible for complex multicloud and hybrid-cloud environments where your data is distributed across multiple platforms. Statista says that over 60 percent of all corporate data is stored in the cloud.

Immutable Storage: Secure Across Environments

That's where immutable storage changes everything. Immutable storage saves your backups in a write-once-read-many-times (WORM) format that can't be altered or deleted. So hackers can't hack it, and malicious actors can't victimize you with ransomware. With immutable storage, you can be sure your data is secure and its integrity is assured in multicloud and hybrid-cloud environments.

Immutable storage also gives you a transparent record of all data transactions. Each change to data is recorded and stored as a separate immutable object. If you are attacked, it is much easier to trace the origin of the breach and identify which data has been affected. And immutable storage gives you an added layer of protection against accidental data loss or corruption. Because it can't be altered once created and saved in an immutable format, it is much more difficult for essential data to be overwritten in error.

Implement Immutable Storage Across Platforms

Some challenges come with implementing immutable data storage in multicloud and hybrid-cloud environments. One of the biggest is the complexity of managing the solution across multiple platforms. Each cloud platform may have its storage protocols, which makes it challenging to maintain a consistent immutable storage strategy spanning all platforms.

Your strategy may work well for one cloud, but another cloud might not support immutability. As your data moves between multiple destinations, the question you need to answer is: Am I getting the benefits of immutable storage everywhere my data ends up?

Shadow IT that may exist within your company compounds this problem. Your organization might have multiple groups—from marketing to product management—all using different SaaS applications without the IT department even knowing it. That means you don't know if the data is being backed up or, ultimately, whether it will be stored in an immutable format. And that makes shadow IT a problem of outsized proportions. So it's crucial to ensure that the data generated in all shadow IT applications is stored in an immutable format to maintain data integrity.

Getting there demands that you implement a unified data storage strategy that spans all your cloud platforms. This strategy should include standardizing on a single immutable data storage protocol or investing in tools and technologies that can help manage data across multiple platforms.

Immutable Storage Covers Compliance

Immutable data storage also addresses the challenges posed by data privacy and compliance requirements, like GDPR and industry standards for healthcare and finance, which now mandate data preservation or retention by law. Any business subject to these requirements must have mechanisms to prove that it maintains secure copies of its data that can't be altered or modified. Here, immutable data storage is often the answer because it helps ensure compliance with strict data retention and audit requirements.

Immutable storage makes it easier to demonstrate compliance during audits. And it prevents data alteration while providing an audit trail that lists the history of all data changes, ensuring transparency and accountability. It's essential because regulators and auditors must verify that your organization follows specific rules and compliance requirements.

With immutable storage as a resource for audit trails, you can show the outside world, including customers, partners, and investors, that you are compliant. That increases trust and confidence in your organization and its capacity to handle sensitive data.

Enforce Strict Access Controls

While a multicloud approach to immutability brings many benefits, it still can be vulnerable due to a lack of controls over privileges and administrator rights to data. Even though an immutable solution is very secure, if a bad actor gains access—whether a malicious employee or a third party with privileged account-management access—they can delete your data. If someone has privileged access to the data, they can delete it, regardless of the security measures in place. That presents a real risk since data alteration or deletion can cause irreparable damage to your organization's operations.

Think about the keys to your home. If the bad guys get ahold of them and gain access, they can take anything they want. Similarly, if someone gains privileged access to your data, they can delete it, causing significant harm to your organization. That's why it's essential to couple immutable storage with strict access controls and monitoring mechanisms to prevent unauthorized access and ensure data integrity.

Immutability is a Must Have

While there are many things you need to do to ensure data resilience, immutability is no longer an option; it's a necessity. It's not just a matter of data resilience; it could impact your organization's very survival.

To get expert guidance regarding the right immutability and data resilience strategy for your organization, choose an Arcserve technology partner. To learn more about Arcserve's immutable storage products, check out our free demos.

Need Answers?

Arcserve is always here—standing by and ready to help.

arcserve®

+1 844 639-6792

arcserve.com