



Data Resilience: Why It Matters and What You Should Know

Table of Contents

- 3 Solving the Data Resilience Equation in the Age of Near-Infinite Data**
- 5 How Unified Data Protection Ensures Data Resilience in Cloud Computing**
- 7 Data Resilience: The Key Component of Every Disaster Recovery Plan**
- 9 Your Data Is Your Responsibility: How to Ensure Data Resilience in the Cloud**



Solving the Data Resilience Equation in the Age of Near-Infinite Data

It's no secret that the amount of data being generated is exploding. Statista projects that the amount of data created, captured, copied, and consumed globally will grow to more than [180 zettabytes](#) by 2025.

That growth is driven by the rise of big data and analytics, internet of things (IoT) devices, and artificial intelligence (AI), all of which make data management a challenge for the foreseeable future. Another issue for companies is that they tend to focus exclusively on cybersecurity instead of thinking more broadly about data resilience.

Threats are only going to get more sophisticated and more frequent. The 2022 Verizon Data Breach Investigations Report found that ransomware attacks grew dramatically in 2022, accounting for [25 percent](#) of all breaches. Cybersecurity Ventures expects global cybercrime to reach an incredible [\\$10.5 trillion](#) annually by 2025—up from 3 trillion in 2015.

These statistics should motivate every IT pro to improve their organization's data resilience by solving the data protection equation. Let's start with a simple definition. Data resilience is the ability of a system to withstand everything from cyberattacks to network outages to natural disasters. And it's crucial for businesses that rely on hybrid- and multi-cloud environments for storing and accessing vital data.

Measure Your Recovery Gap

In his ongoing conversations with IT decision-makers, Arcserve executive vice president of marketing, Florian Malecki, has uncovered a sad fact: While many companies have data resilience strategies, they're too focused on IT security solutions rather than taking a broader view. "Many IT leaders have mainly invested in next-generation IT security products, but many organizations are not necessarily up to the mark with their backup and recovery capabilities," said Malecki.

Ransomware attacks occur in the time it takes to click on a link. And threats are increasing from all corners, with ransomware as a service and tool kits readily available on the dark web. IT pros need to do more. "To recover your data, you need to understand where your backup data is stored—and how it is protected," said



Malecki.

Ensure Your Recovery With a 3-2-1-1 Backup Strategy

The point is that even if you have backup data ready to restore, it still may not meet your requirements. You must test your recovery capabilities and leverage immutable storage to secure critical data.

Ransomware attackers frequently go after your backup data first to prevent recovery. Without available backups, you could be forced to pay the ransom. Even then, that doesn't ensure you'll get your data back. And some attackers just use [wiperware](#) to destroy your data. [Immutable storage](#)—part of a [3-2-1-1 data protection strategy](#)—protects your backups by using a write-one-read-many-times format that can't be altered or deleted, even by an admin.

To illustrate, Malecki also shares the story of [one Italian city](#) that was hit by ransomware earlier this year. As a result, some of its backups were corrupted, and its Veeam server and VMware infrastructure were unavailable. The city turned to its [Arcserve tape recovery solution](#) and other accessible data from its Oracle database and NetApp storage for its initial recovery efforts. But the attack still left a significant gap in the city's recovery capabilities.

Immutable storage is your last line of defense for recovering data and backups after a successful ransomware attack. And immutability is now available for both [on-premises](#) deployments and the cloud. That gives you choices.

Solve the Data Resilience Equation

Malecki recommends storing an air-gapped copy of your backup data separately from your network and securing it offline.

“Essentially, you're making it hard for ransomware attackers to wipe backup data as you have copies that are not connected to the corporate system. The only way that can happen is if they have an insider or someone social-engineered to corrupt or delete it physically.”

“But cybercriminals are constantly probing, looking for new ways to wreak havoc on your business. So, it's about ensuring that you address every aspect of your data resilience strategy equally, from cybersecurity to orchestrated recovery. That way, when an attack gets through, you are fully prepared and ready to recover quickly,” concluded Malecki.

Get Expert Help

Arcserve technology partners are experts at helping large and small organizations put together effective data resilience strategies that ensure recovery no matter what. Find an Arcserve partner [here](#). And be sure to check out our [free trial offers](#).



How Unified Data Protection Ensures Data Resilience in Cloud Computing

Cybercrime will cost [\\$8 trillion](#) in 2023, increasing to \$10.5 trillion by 2025, according to Cybersecurity Ventures. That's an incredible amount of money. But, even at the individual company level, the costs of a data breach still average a breathtaking [\\$9.44 million](#) in the United States, according to IBM. You've probably seen similar statistics.

You may not realize that nearly half of all data breaches happen in the cloud (45 percent), with the average data breach cost coming in at \$4.24 million for private clouds and \$5.02 million for public clouds, according to the same IBM report.

These statistics are a driving force behind more companies adopting strategies that ensure data resilience in cloud computing.

Compliance Is Critical, But Complexity Is Increasing

Aside from the costs of a breach, compliance with regulations ranging from the EU's General Data Protection Regulation (GDPR) to the U.S.'s Health Insurance Portability and Accountability Act (HIPAA) puts added pressure on your company—and your IT team—to ensure your sensitive data is protected and resilient.

Multi- and hybrid-cloud deployments often force IT teams to deal with diverse storage, backup, and recovery systems. Usually, each cloud provider offers its own set of tools and services for managing data, making it challenging to develop a consistent data resilience strategy across multiple environments. And integrating some data protection solutions with existing infrastructures adds more complexity, especially when dealing with legacy systems. Ensuring effective cybersecurity across all your environments creates another wrinkle for IT to overcome.

UDP: Data Resilience Across All Environments

[Arcserve Unified Data Protection](#) (UDP) simplifies the data resilience equation. That starts with protection against data loss and extended downtime across cloud, local, virtual, hyperconverged, and SaaS-based workloads. You can also reduce your downtime from days to minutes and validate recovery time and recovery point objectives ([RTOs/RPOs](#)) and service-level agreements (SLAs) with automated testing and granular reporting.

Ransomware Prevention and Recovery:



Crucial to Data Resilience

Arcserve UDP prevents ransomware attacks on critical disaster recovery infrastructure with available [Sophos Intercept X Advanced for Server](#). This cutting-edge cybersecurity solution uses a deep learning neural network to detect both known and unknown malware—without relying on signatures. You can also quickly respond to and neutralize threats with CryptoGuard and WipeGuard, which use behavioral analysis to stop never-before-seen ransomware and boot-record attacks.

And you can rest assured that your data backups are stored in an immutable write-once-ready-many-times (WORM) format with Amazon S3 Object Lock support. As Amazon's website [states](#), “You can use WORM protection for scenarios where it is imperative that data is not changed or deleted after it has been written.”

That's a key component of cloud data resilience. But recovery following a disaster is just as important. Arcserve UDP lets you restore faster with instant virtual machine (VM), local and remote virtual standby, application-consistent backup and granular restore, hardware snapshot support, and extensions delivering high availability and tape support. The solution also protects on-premises Microsoft 365 workloads, including Exchange Online, Teams, SharePoint Online, and OneDrive for Business.

Scalability With Flexibility

Arcserve UDP offers a multi-tenant, cloud-based console or private management console, depending on your requirements. And you can quickly scale your hybrid business continuity topologies locally or across long distances with multiple sites, including your service and cloud providers.

You'll get fast results because you can deploy the solution in minutes with a few clicks—there's no need for training or external professional services. Create data stores on your recovery point server (RPS), add the nodes you want to protect, a storage destination, and a plan. That's it. And it's easy to perform jobs like backup, virtual standby, and replication. You can choose a simple restore or a bare metal recovery, too.

Back up to a local machine (and folder) or a central RPS (in a remote, shared folder) with global, source-side deduplication. And add network CIFS/NFS shares, Office 365 Exchange, or SharePoint Online nodes and create related tasks.

Assured Data Resilience in Cloud Computing

Learn more about how you can put Arcserve products to work so you can be confident that your data is resilient in the cloud—and everywhere else in your organization—by talking to an [Arcserve technology partner](#). To see the power of Arcserve UDP for yourself, take advantage of our [30-day free trial offer](#).



Data Resilience: The Key Component of Every Disaster Recovery Plan

What is data resilience? In a nutshell, it's a mindset that all organizations should adopt to meet their business continuity plans and keep their operations up and running. There are many moving parts, but overall, it's as simple as that. Understanding that data resilience is an essential cog in a well-rounded disaster recovery program is also important.

According to a [global survey](#) commissioned by Arcserve, 83 percent of IT decision-makers now include data resilience in their business strategies. Still, only 23 percent are reported to have a mature approach to data resilience. But that isn't enough because a solid data resilience plan is essential as organizations move to hybrid IT environments. When performance needs arise or a catastrophic failure occurs, organizations must have a well-thought-out and battle-tested plan for recovering their data.

The reality is that data is the fuel that modern businesses run on. When companies lose access to their data, they lose the ability to keep moving forward. Data resilience prevents this from happening. It allows every organization to quickly recover from a data-threatening event and flourish in the digital economy.

Here are three key steps to help a business develop a robust data resilience strategy:

1. Create a Plan and Test It Often

The strength of any data resilience strategy depends on the regular testing and adjustment of all its parts. To be reactive is not good enough. A company can't wait for a disaster or attack to occur, then scramble to implement its strategy and find out if it's good enough.

Planning and testing are indispensable to success. Indeed, a well-devised and continuously tested data resilience strategy can mean the difference between staying in business and having no business.

Numerous studies have shown that organizations that suffer a ransomware attack or other data-loss event have significant difficulties winning back their customers. One survey by Okta revealed that [88 percent](#) of customers would stop using the services or products of a business they no longer trust and that 39 percent lose trust in a company that misuses data or suffers a data compromise.

You get the idea. A data-loss event or hack of any kind can be fatal to your business.



2. Get Executive Buy-In

Data resilience should be the responsibility of top executives and business owners, not just the IT department. And yet it still isn't a priority in the C-suite of many organizations. It must be, especially with new cyber security measures, such as the EU's [NIS Directive](#).

A successful data resilience initiative starts at the top, with buy-in from C-level executives and the board of directors. But, like any investment, a data resilience initiative needs support from the whole company, from the corner office to the cubicles, across every department. It also requires buy-in from external partners and service providers. All participants must know their role in everyday operations and during a disruptive event for an initiative to work. Without that, some may not meet expectations when disaster strikes.

3. Take a Multilayered Approach

The key to achieving data resilience is a “multilayered approach” and deploying an infrastructure that supports all data resilience requirements.

One vital layer should create frequent backups and make copies that can be stored in an immutable digital vault. Storage snapshots should be taken and secured in a digital vault during this process. When a disaster or attack happens and data is compromised, the company has these snapshots available for instant recovery. Indeed, that's how the Italian municipality of Palermo [recovered its data](#) after a recent cyberattack.

Automation and orchestration are other vital parts of a multilayered approach that help streamline data recovery. These parts should include processes and automated workflows that ensure consistency and minimize complexity when time is of the essence and quick thinking is required. That way, the organization can recover data quickly and return to business without critical damage.

Another critical element of a multilayered approach is [3-2-1-1 data protection](#). It means maintaining three backup copies of data on two different media—tape and disk, for example—with one of the copies placed offsite to enable quick recovery.

Further, the firm should have one copy. Immutable object storage continuously protects data by taking a snapshot at 90-second intervals. Even if disaster strikes, those data snapshots enable a return to a recent file state.

Final Thoughts

To conclude, a good data resilience strategy dramatically benefits a business. A good strategy enables it to manage rapid data growth, handle various workloads, unify data recovery, and quickly get operations up and running after any event that compromises data.

It brings many benefits to the organization, including enhanced performance, reduced costs, reliable and efficient business operations, minimized risk, and strong protection in every part of the company. For expert help in ensuring data resilience in your organization, talk to an [Arcserve technology partner](#).



3 Strategies for Achieving Data Resilience in the Cloud

Undoubtedly, we will eventually see a massive software-as-a-service (SaaS) outage. With so many organizations now dependent on SaaS to keep their operations moving, data backup and recovery must be front and center for every IT pro today.

Companies worldwide are increasingly consuming SaaS rather than running their own IT infrastructure on premises. However, many still mistakenly believe that data protection is the responsibility of their cloud providers. They may also assume that the provider will handle all aspects of data protection, including backing up and recovering the data.

If a service like Microsoft 365 suffers a major outage, organizations must know that while service is guaranteed, the organization's data protection is not. That responsibility lies solely with the organization. You don't need to look far for an example. In late January, Microsoft 365 was struck by a [worldwide outage](#) caused by a router IP address change that led to packet forwarding issues between all other routers in its wide-area network (WAN).

While cloud providers do take steps to protect their customers' data, it is ultimately the customers' responsibility to ensure that their data is backed up, secure, and recoverable. The cloud provider cannot control all factors that could lead to data loss, such as user error, hardware failure, natural disaster, or malicious attack. That's why it's essential to understand the [Shared Responsibility Model](#).

Data is the lifeblood of the enterprise today; losing it can result in loss of customers, brand reputation, revenue, and, ultimately, the enterprise itself. One Gartner [report](#) from way back in 2019 says that assuming SaaS applications don't require backup is dangerous. And about [70 percent](#) of total company software usage was SaaS in 2022, with projections showing that number will grow to as much as 85 percent by 2025. With so many users, every organization will likely experience disruption due to data loss from SaaS applications.

Too many IT decision-makers mistakenly rely on their SaaS vendors for data protection. Organizations need to address this disconnect. Businesses must understand that their data is their responsibility and implement proper security measures to protect that data in the cloud.



With that in mind, here are three strategies for organizations to ensure data security, even if disaster strikes one of their cloud providers.

1. Do Your Due Diligence

Ask your cloud provider several crucial questions to ensure it can provide security and continuity for your business. For starters:

- What measures does the provider have in place for business continuity and disaster recovery?
- What are its service-level standards for uptime?

For example, is the service designed to be operational 99 percent or 99.999 percent of the time? While the difference may sound small, it can significantly impact your business: 99.999 percent equates to minimal downtime, but 99 percent can equate to several days of disruption yearly.

It's also important to ask whether the provider offers data backup services. If so, are they included in the subscription cost or cost extra? Or do you need to secure additional coverage through a third-party partner? Also, how complicated is it to switch to a different cloud provider, if necessary? Considering this possibility is essential, as moving between providers can sometimes be a significant hassle.

2. Have a Backup Plan

The [2021 fire](#) at OVHcloud's data center in France highlighted the potential risks to data in the cloud. The incident affected many websites, including government agencies, ecommerce businesses, and banks, and resulted in permanent data loss for some.

A good disaster recovery plan is essential to protect your data in the event of a disaster, whether natural or caused by humans. Part of the plan should simulate a business disruption to test and assess the organization's ability to recover. It's also important to regularly test your backup images to identify and fix any potential issues before an actual disaster. In a disaster, it is critical to ensure that the backed-up data is available and can be quickly restored.

The OVHcloud fire puts a spotlight on the importance of having a recovery plan. Those customers with a plan in place during the fire were more likely to minimize damage and avoid permanent data loss.

3. Demand Immutability

When evaluating cloud providers, ensuring that the chosen provider offers immutable storage is critical. Immutability is a type of data storage in which, once data is written, it cannot be modified or deleted. Any changes to the data must be made by writing new data rather than by altering or deleting existing data. Immutable storage protects data integrity and ensures that data remains unchanged over time.



In the case of a ransomware attack, for example, attackers may attempt to encrypt or delete data to disrupt a system's operation or demand a ransom for the decryption of the data. The attackers cannot alter or delete the data if the organization uses immutable storage. And the company can use it to recover from the attack even if the attackers successfully encrypt or delete other data.

Similarly, in the case of a system outage, immutable storage can be helpful because it enables organizations to access a copy of their data. It can be essential in cases where the outage occurs due to a hardware or software failure, as it may be difficult or impossible to access the data stored on the affected system.

With immutability, organizations are protected from data loss, data corruption, external threats, or system failures.

The abundance of vital documents, records, and communications now stored in the cloud means that data loss is not an option. Organizations must back up all mission-critical data and ensure it is fully recoverable. However, it is also essential to understand that your cloud provider is not responsible for safeguarding your data.

In the realm of data protection in the cloud, it is wise to hope for the best and prepare for the worst. A solid plan will ensure that you're ready for any eventuality. For expert help ensuring data resilience for your SaaS applications, talk to an [Arcserve technology partner](#). To see what Arcserve SaaS Backup can do for your organization, check out our no-obligation [30-day free trial](#).





Need Answers?

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



arcserve®

+1 844 639-6792
[arcserve.com](https://www.arcserve.com)

