arcserve®

Data Resilience, Data Protection, and Immutability: Your Foundation for Disaster Recovery

Table of Contents

How Data Resilience Takes You Beyond Backup and Recovery

Data resilience is typically defined as an organization's ability to ensure business continuity in the face of any disaster or disruption. While there's more to the story regarding achieving data resilience, the concept itself is simple.

As we wrote in a recent post, a global survey of IT decision-makers commissioned by Arcserve found that 83 percent now include data resilience in their business strategies. The bad news is that only 23 percent have a mature approach to data resilience.

That won't cut it in today's threat-filled world, especially as organizations migrate to hybrid IT environments. That's why you need a well-thought-out and battle-tested data recovery plan that's ready to roll if a catastrophic failure or other disaster strikes. Your business runs on data, and if that data is ever unavailable, it can bring your company to an expensive standstill. That's where data resilience enters the picture, ensuring your business can quickly recover from any data-threatening event and continue to operate.

Here are three key steps you can take to develop a robust data resilience strategy:

Create a Plan; Test It Often

The success of your data resilience strategy depends on consistent testing of your plan and ongoing optimization of its components. You need to be proactive because it's too late once disaster strikes. Planning and testing are your keys to success and can make the difference between a thriving business and no business.

Plenty of research confirms that ransomware attacks and other data loss events lead to lost customers. A study by Okta found that 88 percent of respondents would be unlikely to purchase from a company they didn't trust, and 45 percent said they have serious reservations about buying goods and services online from a company if they have concerns about data breaches. Recovering from those repercussions is a lot harder than ensuring data resilience.

Ensure Your Executive Team is Included

It takes a collaborative effort between IT teams and company executives to ensure data resilience. Unfortunately, data resilience has yet to become a priority in many C-suites. For global businesses, that has to change, especially with the introduction of new cybersecurity requirements like the NIS 2 Directive in the EU.

In many organizations, data resilience initiatives can face obstacles to adoption if no executive champion supports their objectives. A successful data resilience initiative starts at the top, with buy-in from executives and even the board of directors. When that happens, everyone recognizes the importance of the effort and will more likely play their part in its success so that if—or when—disaster does strike, your business is more likely to recover.

Employ a Multilayered Approach

The key to achieving data resilience is a multilayered strategy where you deploy an infrastructure designed to meet your specific requirements. One vital layer is ensuring frequent data backups following the 3-2-1-1 backup strategy.

Snapshots of your data should be taken every 90 seconds to minimize any data loss and ensure instant recovery and placed in immutable storage. Immutability ensures the snapshots can't be modified or deleted by hackers or encrypted by ransomware. That's how the City of Palermo, Italy, recovered after a recent cyberattack.

Automation and orchestration are two essential components of a multilayered approach because they help streamline data recovery. Your chosen solution should include processes and automated workflows that ensure consistency and reduce complexity, especially when disaster strikes. That will help you get your data back fast, minimizing damage.

Make Data Resilience a Priority

Data resilience can save your business. At the very least, knowing your data is protected can help you sleep better at night. But a sound data resilience strategy can take you even further, helping you manage your ever-growing mountains of data, handle a variety of workloads, unify data recovery, and get you back in business fast if disaster strikes.

Learn how you can enhance your data resilience by choosing an expert Arcserve technology partner. And find out more about Arcserve products by checking out our free demos on demand.

Why You Need Immutable Network Attached Storage for Ransomware Recovery

Mordor Intelligence estimates that more than 80 percent of midmarket and enterprise organizations are using network-attached storage (NAS) today and predicts that the NAS market will grow at an impressive 19.5 percent CAGR between 2021 and 2026. Mordor also points out that the most significant factor driving this growth is the “explosion in unstructured data, increasing the footprint of scale-out NAS in enterprise IT systems.” We concur, only adding that this massive data growth also drives the need for scale-out backup storage.

Unfortunately, ransomware isn’t going anywhere either: Sophos’ The State of Ransomware 2022 report found that 66 percent of the respondent’s organizations were hit by ransomware in the last year, with 65 percent of the attacks resulting in data encryption. The Sophos report also found that backups are the number one method for restoring data, used by 73 percent of respondents whose data was encrypted.

But here’s where the numbers illustrate the problem: 46 percent of respondents said they paid the ransom to restore data. That leaves a 27 percent gap filled by organizations that had backups but still had to pay the ransom. And, once again, according to the report, even those who did pay could only restore 61 percent of their encrypted data.

Immutability Is the Answer

That brings us to the 3-2-1-1 backup strategy: keep three copies of your data—one primary and two backups—with two copies stored locally in two formats (network-attached storage, tape, or a local drive) and one copy stored offsite in the cloud or secure storage.

The last one in 3-2-1-1 stands for immutability. Arcserve OneXafe employs a file system based on an immutable object store, with every object written only once—it can never be altered or deleted. Any modifications you make to your file system result in new immutable objects being created.

OneXafe provides continuous data protection (CDP) by taking low-overhead snapshots—a view of your file system at the instant it is taken—every 90 seconds. These snapshots inherit immutability from the underlying objects, ensuring your backups can’t be hurt by ransomware. And if you ever need to, the snapshots let you go back to specific points in time and recover your entire file system in minutes.

The ransomware metrics we’ve shared above make a case for using OneXafe for immutable network-attached storage as a backup data target because availability and restorability are guaranteed. And OneXafe provides a logical air gap thanks to its immutable object store.

Scalability Matters

Statista projects that the total amount of data created, captured, copied, and consumed globally will rocket to 180 zettabytes by 2025, attributing the rate of increase over previous projections to remote work and the societal changes driven by the COVID-19 pandemic. Your organization is probably generating more data than you might have foreseen, too. That makes scalability a key backup feature of your backup infrastructure.

OneXafe makes scaling easy by letting you seamlessly add one drive at a time or multiple nodes in a cluster. This scale-out approach means you don’t have to allocate extra storage for “what ifs,” as with traditional storage architectures. You simply add storage as you need it. And OneXafe cuts your overall storage requirements by offering deep data reduction that combines inline deduplication with compression, delivering storage space savings of as much as 90 percent and dedupe ratios up to 10:1.

Added Value for File Server Consolidation and Unstructured Data Store

OneXafe is also designed to meet your performance and manageability requirements for unstructured data. You can seamlessly create NFS or SMB shares to meet accessibility requirements with commonly used protocols. And OneXafe’s storage architecture lets you free up virtual server resources—including costly virtual storage infrastructure—so you can use these resources elsewhere. OneXafe also helps you eliminate NAS data silos by consolidating storage onto a scale-out appliance that grows with you while giving you extensive disaster recovery capabilities.

Find Out More

Request a demo for a deeper dive into what makes OneXafe tick. And for expert help with ensuring your data is protected from ransomware and any other threats, talk to an Arcserve technology partner.

How to Choose the Right Data Backup and Disaster Recovery Solution for Your Business

The global data backup and recovery software market is predicted to grow to $23.1 billion between 2022 and 2030, an impressive 9.6 percent CAGR. That's a good sign because it shows that businesses are taking cyberthreats—like ransomware—seriously.

Those threats are increasing at an alarming rate, with the SonicWall 2022 Cyber Threat Report midyear update noting that there were an incredible 2.8 *billion* malware attacks in the first half of 2022. Europe also became a bigger target this year, with the report finding a 63 percent increase in ransomware attacks on organizations on the continent.

At the same time, the average cost of a data breach was a heart-stopping $9.44 million in the U.S. in 2022, while the average cost of a ransomware attack worldwide was almost as painful at $4.54 million. If you're an IT pro, those data points are telling you that it's time to push harder for increased investments in a cybersecurity and backup and recovery solution that ensures your business can survive a data breach or ransomware attack no matter what.

With that in mind, here are several backup and recovery solution options explicitly designed for small, mid-size, and enterprise companies.

Immutable Storage for Midsize Companies

As we noted in a recent post, cybercriminals are increasingly focusing attacks on encrypting files and deleting backups. That's why we recommend that every organization follow the 3-2-1-1 data protection strategy that includes immutable storage. When your backup files are saved to immutable storage, they are created in a write-once-read-many-times format that can't be altered or deleted. So, even if your primary data is encrypted and your systems are taken down, you can count on your backups for recovery.

One option is Arcserve OneXafe. Built for midsized companies, Arcserve OneXafe gives you scale-out network-attached storage (NAS) for your backups and unstructured data using a file system based on an immutable object storge—every object is written only once and never modified. OneXafe gives you continuous data protection by taking low-overhead snapshots every 90 seconds. These snapshots are the view of your file system at the instant the snapshot was taken. Thanks to their immutability, these snapshots let you go back to a specific point in time and recover entire file systems in minutes.

Unified Data Protection for Midmarket and Enterprise Companies

Arcserve UDP is a comprehensive software option for midsize and enterprise companies. Arcserve UDP unifies data protection across both on- and off-premises workloads while delivering orchestrated recovery. Safeguarded by Sophos Intercept X Advanced cybersecurity, Arcserve UDP is the only solution that combines deep-learning server protection and scalable onsite and offsite business continuity, giving you a multilayered approach that ensures complete IT resiliency for your virtual, physical, and cloud infrastructures.

Arcserve UDP also offers that all-important immutability for your data backups with Amazon S3 Object Lock or Arcserve OneXafe for those that prefer a non-cloud option. It also reduces your downtime from days to minutes and validates recovery time and recovery point objectives (RTOs/RPOs) and service-level agreements (SLAs) with automated testing and granular reporting. And Arcserve UDP is built for business, protecting Microsoft 365 workloads—Exchange Online, Teams, SharePoint Online, and OneDrive for Business—while delivering deep data reduction to limit storage usage, granular recovery, and offsite replication.

Cloud-Based Backup and Disaster Recovery for Small Companies and SMBs

Small to midsize companies can look to the cloud to protect on-premises business systems and data. Specifically, we're talking about Arcserve Cloud Services disaster recovery as a service. While local backups may be enough to recover your IT systems from server failure and other common problems, a site-wide disaster can destroy your backups—and result in painful downtime and data loss.

Use either Arcserve's ShadowProtect backup and disaster recovery software or ShadowXafe next-generation data recovery and backup software with Arcserve Cloud Services to count on complete business continuity.

Finally, for simpler environments, there's Arcserve OneXafe Solo. This plug-and-play data protection appliance streams your data directly to Arcserve Cloud Services for business continuity. It also includes Arcserve OneSystem for cloud-based management from anywhere using a web browser. Extremely easy to deploy and manage, OnXafe Solo brings the same data protection technology that drives ShadowXafe in a compact appliance form factor. OneXafe Solo is also perfect for remote and branch office (ROBO) environments, providing next-generation edge data protection in virtual environments and locations with little to no local storage. And it doesn't require dedicated IT staff; you just set it and forget it.

Find the Right Solution for Your Business

Get expert help choosing the best backup and disaster recovery solution for your specific situation by talking to an Arcserve technology partner. And be sure to check out our free trial offers for Arcserve UDP, ShadowXafe, and ShadowProtect here.

4 Ways Separated Data Protection Infrastructure and Immutable Backups Reduce Risks

Data protection is crucial to ensuring business continuity. But if disaster strikes and your data is encrypted by ransomware or lost due to human error, you need to know you can retrieve your backed-up data with absolute certainty. As every IT pro knows, the threats to your data are very real, with 66 percent of respondents to Sophos The State of Ransomware 2022 reporting they were hit by ransomware last year and 72 percent saying they experienced an increase in the volume and complexity of cyberattacks over the same time frame.

Separate Infrastructures Reduce Risks

If ransomware takes down your primary infrastructure, your backups could be toast, too. That's IT 101 and just about every IT pro knows it. With that in mind, here are four essential reasons data protection best practices dictate that you should keep these two infrastructures apart, with one serving as your primary backup storage and the other providing immutable object storage that ensures failsafe recovery.

1. Provides a Logical Air Gap

With separate infrastructures, you add another layer of redundancy. Keeping your data protection appliances in a different location from your immutable backup storage creates a logical air gap that can't be breached. The risks to your data are instantly reduced because your immutable backups ensure you can quickly recover your data—even if your data protection infrastructure is taken down by ransomware, a cyberattack, a natural disaster, or even an accidental deletion caused by human error.

2. Adds Redundancy

Separate infrastructures eliminate the risks that come with a single point of failure. Redundancy ensures you're covered if anything happens to either of your appliances.

3. Delivers Multi-Purpose Immutable Storage

There's no doubt that immutable storage is perfect for backup repositories. But it's also a sound choice for archival data and other unstructured data stores because it adds the power of immutability, defending all of your data from being altered or deleted.

4. Offers Flexible Independent Scaling

With a single infrastructure for data protection and immutable storage, you will often find yourself paying for storage and resources you don't need. With separate infrastructures, each appliance can be scaled independently as required, so you only pay for the resources you need when you need them.

Get Expert Infrastructure Advice

Learn more about how this best-practices approach can reduce your risks and costs by talking to an expert Arcserve technology partner. To see how Arcserve solutions solve your data protection and immutable storage equation, request a demo today.

Need Answers?

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

arcserve®

+1 844 639-6792
arcserve.com