arcserve®

Realizing Cost-Effective Data Resilience with an Optimized Storage Strategy

Table of Contents

What Is an Optimized Storage Strategy, and How Can It Help Your Company Thrive?

By Florian Malecki, Executive Vice President, Marketing, Arcserve

Today, data is the new gold. Every IT pro understands this. Your organization is probably generating oceans of data as you take advantage of new technologies that the cloud, IoT, edge computing, and other innovations offer. And there is no doubt you are under incredible pressure to store, manage, and protect your data because it is crucial to your business. What's needed are new approaches to storage that transform your operations and help you thrive in the digital economy.

IDC says that in 2020, 64.2 zettabytes of data were created or replicated worldwide. By 2025 that number is projected to exceed 180 zettabytes. With so much more data generated, you may be in the same position as many other companies—forced into urgently updating your storage strategy to meet demand. But it's not just about having enough storage space. Ransomware threats continue to grow. Two-thirds of IT pros surveyed for Sophos State of Ransomware Report say their organization was hit by ransomware in 2021—while hybrid and remote workforces demand that your data is always secure and accessible.

Focus Your Storage Strategy on Data

Not all data is equally valuable. Some is business-critical, while most is less important. Your first step is to identify the data critical to your success so you can factor that in as you develop your storage strategy. But having so much data requires careful, comprehensive management, or you could end up with critical data stored on less critical servers. That can create huge problems because it takes longer to access slower, secondary machines. That can slow down your access to the data and limit its value in driving your business forward.

Here's the core issue: Most organizations take a server-based approach to their data backup and recovery deployments. They focus on backing up their most critical machines—not their most essential data. That needs to change. Instead, it would be best to base your backup and recovery policies on matching your critical

servers to your business-critical data. In other words, when it comes to backups, your decisions should be driven by your data's value, not your server hierarchy.

More Storage, Better Value

All this generated data begs the question: where is it all being stored? Traditional storage isn't typically up to the task because disk drives are reliable but slow and limit your agility. With data needed instantly to keep business moving, you also need high-performance storage. Flash storage is one high-performance storage solution. But while flash is fast, it's also costly. That puts it out of reach of many businesses.

As the cost of flash storage drops, we'll see more storage vendors introduce all-flash arrays for mid-market customers. That increased affordability will lead more and more businesses to choose flash technology.

Scale-Out Storage: Efficiency with Data Protection

Traditional storage offers limited flexibility as you need more space for your data. Adding hardware is expensive, and managing storage is time-consuming. And because conventional storage often doesn't include deduplication and compression, your data isn't stored efficiently. Migrating your data when it's time to upgrade is one big challenge, while adding backup and disaster recovery capabilities is another.

That's why more businesses are adopting scale-out storage solutions. Scale-out storage eliminates traditional storage problems, delivering network-attached storage (NAS) that lets you add more drives to individual storage clusters—and more clusters—when you need to, with ease. Scale-out storage also includes data deduplication and compression, simple to use remote management, and built-in backup and disaster recovery (DR) options. Scale-out does more than give you another storage choice—it gives you a better way to manage, protect, and recover your data. That can save IT time, increase operational efficiency, and reduce downtime.

So much data has forced businesses to choose between moving data to the cloud, using a third-party storage provider, or upgrading their existing infrastructure. But depending on your requirements, scale-out storage may be your best choice. It can future-proof your infrastructure, and instead of having storage scattered across locations and hardware, scale-out storage lets you treat all your storage as a global pool. When it's time to upgrade, you just add more nodes or clusters.

With a centralized data infrastructure, your business can become more efficient with uniform policies and improved backup and recovery capabilities.

Halting Hackers With Immutable Storage

More storage and more data mean more risks from cyberattacks. Ransomware isn't going away anytime soon, and hackers are becoming increasingly sophisticated and employing more targeted attacks. Hackers are now setting their sights on backups because they recognize that your backup data is your last line of defense. If your primary and backup data is encrypted by ransomware, you'll face many massive problems.

That's why immutable backup storage and continuous data protection must be part of your DR plan. With continuous data protection, immutable snapshots of your data are taken frequently—every 90 seconds, for example. Because the object store is immutable, even if ransomware does make its way into your systems, your backup can't be altered or deleted. It will always be available, even if it includes hundreds of terabytes of data.

Storage Goes Green

You'd have to live in a cave to be unaware of the need for more sustainable solutions. Global data centers consume massive amounts of energy. That needs to be a key consideration in any data management strategy because data centers now use about three percent of the world's electricity supply—and put out two percent of global greenhouse gas emissions. That puts data centers on par with the entire airline industry.

Your company may already be developing supply-chain strategies to reduce your carbon footprint. And storage solutions are increasingly part of the conversation, as environmental considerations are weighed against power consumption costs and performance requirements.

Your data will continue to be one of your most precious assets, and it will continue to increase in volume and value. You can get more from the data you create and store by leveraging the latest technology and adopting a modern approach to data storage. The results? Reduced energy consumption, increased efficiency, tighter security, and the ability to thrive in today's digital economy.

If you'd like to learn more about your data protection, backup, and disaster recovery options, find an Arcserve technology partner. Or contact us for product information.

Cybersecurity Checklist: Ensuring Data Resilience While Managing Rising Costs

By David Lenz, Vice President, Asia Pacific, Arcserve

Businesses everywhere are under severe pressure from rising costs. But bearing the cost of increasing cybersecurity awareness in your business should be at the top of your priorities list. That's why the Cybersecurity and Infrastructure Agency (CISA) hosts a site dedicated to providing resources for cybersecurity awareness programs.

Here are some things to include in your cybersecurity checklist to address the need for greater cybersecurity resilience that protects, stores, and backs up your data while managing costs.

Keep Your Guard Up

Rising costs aren't your only problem. War rages in Ukraine, and the threat of all-out cyberattacks increases daily. Bad actors will look for opportunities to exploit a challenging situation and attack your business when you're most vulnerable. Indeed, when your business is struggling economically, your cybersecurity risk is higher than ever—because that's when attackers perceive you as easy prey.

A proper backup and disaster recovery plan lets you protect your data even if a cyberattack victimizes you. Your business should look for an "immutable" data-storage solution that safeguards information continuously by taking snapshots every 90 seconds. Even if you fall victim to an attack, your data remains protected and can be easily recovered.

Embrace Hybrid Working

With the rising cost of fuel, many workers want to stay at home rather than spend their money commuting to the office. Many companies successfully implemented remote and hybrid work programs during the pandemic. Continuing these policies can go a long way toward protecting the financial health of workers, keeping them happier and more productive.

However, when your workers are remote, your data is further fragmented, compounding your vulnerabilities. More support is needed at remote locations to manage and protect data effectively. The good news is that there are now simple, low-cost solutions that can effectively back up and protect data in your remote environments without deploying additional resources or capital.

Know Which Pieces of Your Data Are Most Critical

All data is not equally valuable. If you're on a mission to save money, it might not be necessary to store or back up every bit and byte of data in your business. Look for storage solutions that offer data-management capabilities like data tiering. Data tiering is a method by which less frequently used data moves to cheaper storage levels or "tiers," helping you save money on data storage while avoiding damage to your most essential data.

Maintaining healthy processes around data hygiene can help you efficiently retain and back up all your critical data—and offload the data you don't need. Another advantage to data tiering is improved energy and cost savings because you will need less computing power to store your business-critical data.

Don't Skimp on Data Backup and Security

You need to ensure that your data-protection program is not impacted by any budget cuts you consider. It may look like an easy place to save money. But any reductions to your data defenses will come with costs down the road. The 2021 IBM Cost of a Data Breach Report found that the average cost of a breach was USD$4.24 million.

It's critical to recognize the importance of your data and make sure that any cuts to your budget have minimal impact on your business operations. Look for cost-effective, next-generation solutions that enable you to safeguard your data and grow your business. The best solutions can quickly recover individual files and systems in minutes while ensuring that the data is always available.

If you'd like expert guidance in choosing a suitable data resilience, data protection, backup, and disaster recovery solution, choose an Arcserve technology partner. To learn more about Arcserve products, contact us.

Why Your Business Needs Data Resilience in an Unsafe World

By: Ahsan Siddiqui, Director of Product Management, Arcserve

Data is the lifeblood of every business today. It's not an exaggeration to say that data is now the most important asset on earth. It's more valuable than precious metals, oil, or gemstones for most corporations and individuals. In our digital world, the quantity and quality of data is ever-increasing, and so is our reliance on it.

That's why data resilience is such a critical issue these days. If you lose access to data due to a cyberattack or natural disaster, you can't power your business forward. However, a resilient organization has the proper backup and recovery processes in place, allowing it to quickly bounce back from any situation in which data is compromised.

Data resilience is not a single solution. It is a set of technologies and strategies that help maintain data availability and ensure it is always accessible, thus minimizing any disruptions or downtime that could lead to tangible—and intangible—losses to your business.

Some of these data resilience technologies include cluster storage, data replication, backup, and disaster recovery, which help minimize the damage caused by cyber threats, such as ransomware, and any disaster, like catastrophic climate events such as hurricanes and floods. Having these elements of data resilience in place can help ensure that companies get back on their feet as quickly as possible—with minimal data loss.

Indeed, the critical measure of data resilience is how fast you can spring back from a disruption to resume a normal state of operations and return to business as usual. Having the right technologies and mindset enables you to protect your data if and when disaster strikes. It includes having the right technologies, such as data backup and recovery solutions, and the right strategies, such as simulating a business disruption to assess your resiliency.

Another crucial part of data resilience is the capacity to do regular testing so you can resolve any issues before they occur. Sadly, many organizations don't test their data resilience plan. Many don't even have a plan in

the first place. At a minimum, organizations should prioritize periodical testing of their data backup and recovery proficiency to ensure they can reliably restore their data in the event of a cyberattack or natural disaster.

Any solid data resilience strategy includes recovery point objectives (RPO) and recovery time objectives (RTO) and ways to achieve them. RPO is the critical metric you establish for the amount of data your organization can stand to lose in a disaster. Your RPO plays a vital role in helping to determine how often you need to back up your data and the infrastructure you need to support your backup plan. RPO is less about the actual execution of recovery and more about establishing the framework. When you do have to recover from a data loss, you'll be able to get all the data you need to be restored and available.

By contrast, RTO is a metric you can use to understand how downtime can impact your organization. Once you have set up your RTO, you'll be better positioned to make educated decisions about your data resilience plan. For example, suppose you determine that your business can only handle an hour or two of downtime. In that case, you should invest in a disaster-recovery solution that allows you to get back up and running within that timeframe.

The success of any data resilience initiative is defined by how well you plan and test your processes and tools, rather than waiting for something terrible to happen and then desperately trying to figure out how to get back on your feet. Planning is 90% of success.

Of course, companies should hope for the best but prepare for the worst. When it comes to data resilience, having a reliable and rock-solid plan in place can mean the difference between having a successful business—or having no business.

It is not an exaggeration. Recent studies have shown that corporations impacted by ransomware or other data-loss events have trouble winning back consumer trust. One survey found that 88% of customers wouldn't use the services of or purchase products from an organization they distrust, while 39% said they had lost trust in a company due to a data breach or misuse of data. That can have devastating long-term effects on a business's survival and growth. Data loss has forced some businesses to shut down completely.

Data is the new gold. When companies lose access to their data, they lose the ability to propel themselves forward. Data resilience, however, gives every organization the ability to quickly recover from a data-destructive event and flourish in the digital economy.

Data Resilience Resources

If you're looking for help in developing your data resilience plan or putting the optimal data protection, backup, and disaster recovery solution for your company in place, choose an expert Arcserve technology partner to guide you along the way. Or contact us to learn more about Arcserve products.

How Immutable Network-Attached Storage Delivers Ransomware Protection

April 29th marked the first anniversary of the Colonial Pipeline ransomware attack that led to gas shortages and long lines at the pumps up and down the East Coast. While the Cybersecurity and Infrastructure Agency (CISA) continually improves its support for critical infrastructure owners—like Colonial—the agency also offers tools to help everyone fight back against ransomware, including its Cyber Security Evaluation Tool (CSET).

While you should do everything you can to prevent ransomware from getting in—including using these and other available tools and technologies—there's one specific weapon you can add to your ransomware ramparts that can make all the difference: immutable network-attached storage (NAS) for your unstructured data and backups.

Non-traditional NAS: Scale-Out Storage That Delivers Flexibility

OneXafe's scale-out architecture provides a highly scalable, plug-and-play disk-based backup target for your virtual and physical server environments, delivering scalability for your ever-growing backup data with minimal configuration required for storage management tasks.

Unlike traditional NAS, Arcserve OneXafe uses an object-based store that gives you a seamless pool of available capacity through a single namespace. OneXafe lets you seamlessly add storage—one drive at a time or multiple nodes in a cluster—as your organization grows. That dynamic scalability contains your storage costs because you don't have to allocate wasted storage capacity to meet potential usage spikes, as with inflexible scale-up storage.

Built-in enterprise-grade features further reduce your storage requirements. Those include deep data

reduction, combining inline variable and fixed-length deduplication with inline compression, and dedupe ratios of up to 20:1 that can decrease your storage requirements by up to 95 percent. OneXafe also offers customized data reduction based on application type. For example, an inline variable-length dedupe algorithm—compared to a fixed-length algorithm—is a better fit for backup copies. A single OneXafe cluster backup share can use variable-length dedupe, while a primary store can use fixed-length dedupe for data reduction.

Why an Immutable Object Store Matters

We frequently refer to the 3-2-1-1 backup strategy in our posts because it gives you an absolute last line of defense against ransomware—the last "1" in 3-2-1-1 stands for immutable storage. OneXafe is a native immutable store for your unstructured data and backup copies, providing you with a logical air gap so you can retrieve an unaltered copy of your data even if ransomware makes its way into your organization.

This logical air gapping aptly puts the last '1' in the '3-2-1-1' strategy in place, giving you object-level and snapshot-level immutability and snapshot granularity as low as 90 seconds. Add in OneXafe's point-in-time recovery, and you can bring back an entire file system within minutes.

The Perfect Backup Target

OneXafe makes an excellent backup target for data protection solutions like Arcserve UDP. OneXafe's native immutability ensures that you always have a 'golden' copy of your backup that is available for restore. And OneXafe's WAN-optimized replication lets you store secondary or tertiary backup copies offsite for added security.

OneXafe meets the performance and manageability requirements of unstructured data, so you can seamlessly create NFS or SMB shares to meet various accessibility requirements via commonly used protocols. OneXafe's storage architecture frees up virtual server resources, including expensive virtual storage infrastructure, so that you can use these resources elsewhere. OneXafe also helps eliminate NAS silos by consolidating storage and offering scale-out storage for expanding environments with extended capabilities to support disaster recovery (DR) use cases.

One Appliance Does It All

Arcserve OneXafe gives you a single solution that you can deploy across many use cases, so you don't need multiple point products anymore. To dig deeper into the benefits OneXafe can bring to your organization, talk to an expert Arcserve technology partner or contact us. For more product information check out our on-demand OneXafe demo.

Need Answers?

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

arcserve®

+1 844 639-6792

arcserve.com