arcserve®

Your Guide to Data Protection Best Practices: Unified Data Management, Next-Gen Business Continuity, Immutable Backups, and Air Gapping

Table of Contents

Why Unified Data Management Is Crucial for Securing Your Data

Your data is invaluable. You can glean business insights, make better decisions, foresee trends, recognize opportunities, and even anticipate customer desires. That all adds up to a competitive edge. But two requirements must be met if your data is to deliver on its promise of enhanced insights and increased efficiencies. First, you must keep your data safe by employing an air-tight approach to backup and recovery that prevents downtime and minimizes data loss. Second, you must draw the value out of your data by managing and analyzing it efficiently.

Unified data management helps you do both. For starters, it eliminates vulnerabilities that result from data silos and inefficient data management. Over the past two decades, many organizations have deployed best-of-breed solutions from network security to antivirus (AV) to backup and recovery. Because these systems were usually created separately, they have resulted in silos and operational and security gaps.

These gaps result in vulnerabilities and open the door for bad actors to hit you with a cyberattack or a rogue employee to do damage from within. Data silos compromise your overall data security posture and increase your risks. With unified data management, you gain better oversight and control of your data. From there, it's possible to build a more robust security, backup, and recovery strategy. You can also mitigate the other downside of data silos: distributed, disparate data that can't deliver the insights you need.

What is Unified Data Management?

Unified data management gathers disparate data sources into a single source of truth, with everyone working with the same information. That isn't the case in siloed environments, where data is often hidden or unavailable, creating blind spots that limit the value of analytics insights.

While unified data management is the goal, it isn't easy to achieve. Merging disparate data systems is complex, and your company's data storage may rely on fragmented technologies that aren't designed to work together. That isn't hard to imagine, given that there are thousands of hardware and software vendors, all relying on a variety of programming languages, vocabularies, syntaxes, and practices.

Then there's the fact that data comes in many forms. There's big data, small data, structured, unstructured, and multi-structured data. Some systems can only handle certain data types, and data sets can vary markedly. You might say that most data ecosystems are as complex as the United Nations—with just as many disagreements.

That's a problem because data assets drive your business forward by helping you make informed decisions based on relevant and actionable insights. And that's why you should make unified data management a key initiative for your business—if you haven't done so already.

Here are three ways to get started:

1. Consolidate Vendors

From a data storage, backup, and recovery perspective, consolidating on a single data management vendor will help you minimize gaps and increase your data resilience. A single vendor also helps reduce complexity and costs. And many companies have systems running today that they don't completely understand how to manage.

Part of that may be due to the dire shortage of IT talent today. Companies struggle to find people with the knowledge, experience, and skills to manage far too many point solutions. When you consolidate with one vendor, you cut down on IT time spent on operations and focus more on strategic initiatives.

2. Embrace Automation

Automation is a priority for many, if not most, IT teams today, especially when it comes to addressing the challenges that come with protecting your data in today's complex infrastructures. That makes sense since once implemented, companies can automatically consolidate and cleanse disparate data sources to create a single data source, saving valuable time for IT teams and data scientists.

Unified data management applies rules to data automatically, eliminating instances of non-compliance. That's essential because non-compliance can now bring hefty fines (think GDPR). Compliance also indicates that your business is focused on best practices and building trust with customers and vendors. And automatically linking policies and business rules centralizes management while improving data quality and protection.

3. Focus on Visibility

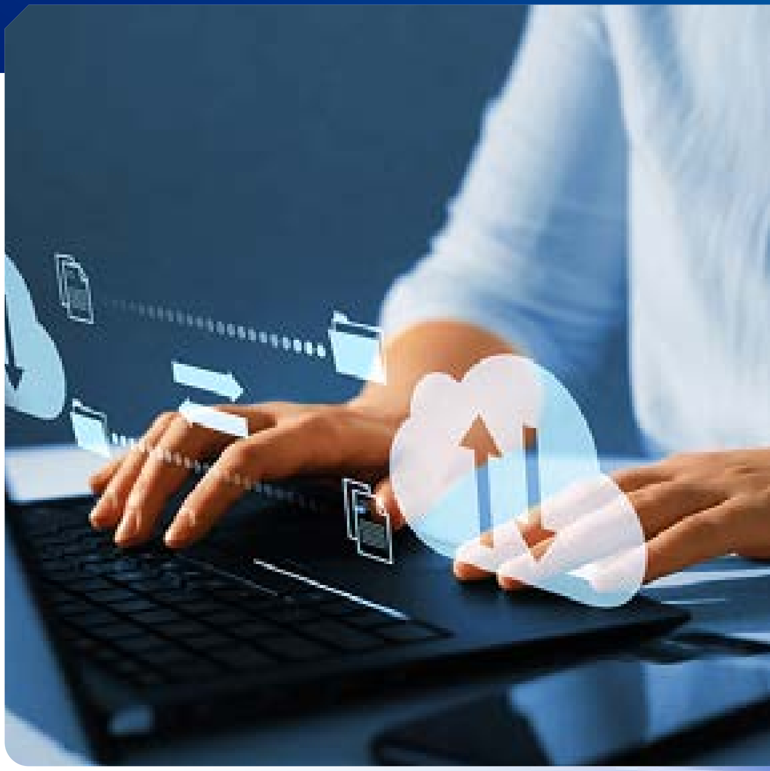
Explosive data growth is one of the biggest challenges to unified data management. How many data copies you have—and where they are stored—can be hard to track. Storage is another challenge, forcing you to decide which data needs to be stored and protected and which doesn't. Fortunately, available solutions can give you visibility across all locations where you have data—on-premises, in the cloud, or in backup locations. Unified data management eliminates data gaps and silos because you can view all your data from a single console or control panel.

Make Unified Data Management a Priority

With the average annual amount of data generated by organizations doubling, managing that data and leveraging it for business insights is challenging. Unified data management helps you solve those challenges. That explains why IDC predicts that half of all organizations will implement a plan to unify data storage, access, and governance by next year.

Find out how Arcserve products can help you achieve a consistent data experience, optimize the value of your data, and gain a competitive edge by choosing one of our expert technology partners.

3 Crucial Reasons Immutable Backups Are Your Best Defense Against Ransomware



Rampant ransomware attacks exploit vulnerabilities to breach companies, encrypt data, and extort painfully large ransom payouts. The SonicWall 2022 Cyber Threat Report mid-year update found that there were 236.1 million ransomware attacks through June of this year. Some industries suffered more than others, with ransomware attacks hitting 66 percent of healthcare organizations in 2021, almost doubling the previous year's total.

Here are three reasons immutable backups are your best defense against ransomware:

1. Immutable Backups Can't Be Altered or Deleted

Ransomware attackers are getting much more sophisticated, and their methods are becoming more ingenious each year. With IT organizations increasingly relying on backups to quickly recover from a ransomware attack without paying a ransom, attackers are targeting these backups first, deleting backup copies and then encrypting the primary production data. No backups can mean no recovery.

What can you do to stop the bad guys? One key to protecting your company is immutability. Immutable backups provide robust data protection because they are impervious to ransomware attacks. Backed-up data is converted to a write-once-read-many-times immutable format that can't be deleted or changed by hackers or admins.

There isn't any way to reverse this immutability, so you can rest assured that your backups are secure and accessible. Even if hackers get their hands on compromised admin credentials and gain full access to your network, immutability makes it harder for them to delete your copies or alter the data's state. The bottom line is that you won't have to pay a ransom to recover your data and get your business back up and running if you're attacked.

While immutability is still slowly being adopted, the good news is that cost-effective immutable solutions are now available that are a good fit for any size business. And these solutions can be deployed quickly and easily, adding a crucial layer of data protection.

2. Snapshots: The Key to Continuous Data Protection

There are several vital components within an immutable data backup solution. First is an immutable object store, with every object written only once and never modified. Any modification you make to the file system always creates a new object. By taking a snapshot every 90 seconds, the Continuous Data Protection feature further protects data. These snapshots are a view of the file system at the instant the snapshot is taken. Since the underlying objects are immutable, the snapshots inherit that immutability. Even better, snapshots let you go back to specific points in time and recover entire file systems in minutes.

Scalability is another critical piece of an immutable storage system. Many traditional systems fall short due to scalability and performance constraints, forcing the addition of more standalone arrays that require separate management or even a forklift upgrade. Object-based storage offers a seamless pool of capacity through a single namespace for dynamically scaled-out storage. That means you can effortlessly add drives and appliances while keeping your essential data safe.

3. Intelligent Tiering Saves Money

Intelligent data tiering is another critical component of an immutable storage solution. An ideal system uses analytics to identify frequently used data that should always be backed up and infrequently used data that doesn’t need to be backed up as often. That gives you an intelligent, tiered data architecture for fast access to mission-critical information. It also helps you save money on data storage while keeping your essential data safe.

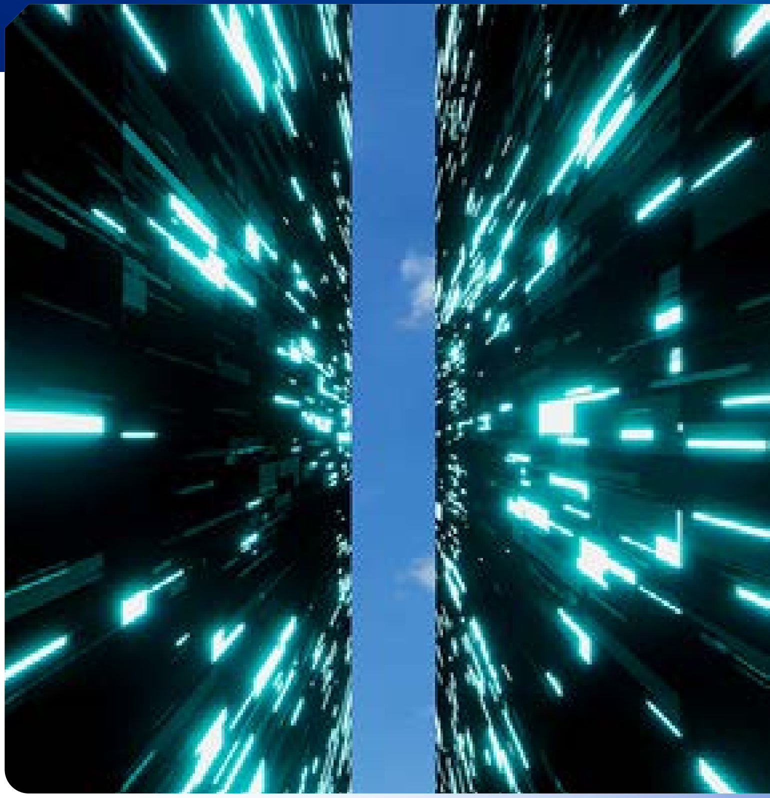
For example, law firms are required to keep legal documents in their original form without being altered. These firms’ backup solutions should automatically qualify which data fits those parameters. In financial services, journals and ledgers should automatically be classified as mission-critical. By setting these classifications in their backup and disaster recovery plan, these companies can ensure the point-in-time recovery of their priceless data.

Don’t Pay the Ransom; Solve the Problem

The cost of a ransomware attack can be astronomical. By investing in a solution that ensures your data is well-defended against these attacks, you can prevent ever facing the decision of whether or not to pay a ransom.

Learn more about Arcserve’s immutable backup options by finding an expert Arcserve technology partner or scheduling a demo.

Overcoming Challenges to Implementing Air-Gapped Technologies With Backup Software



Air gapping isolates your backups by eliminating any external connections—wired or wireless—to the device or devices where your backups are stored. Air gapping adds another layer of data protection to your data resilience and business continuity efforts. And it can be your last line of defense if all your other systems are taken down by ransomware, a natural disaster, or another calamity.

A survey of global IT professionals by Statista found that 71 percent said their companies were affected by ransomware in 2022. Even worse, the same study found that the victims paid the ransom in about two-thirds of those ransomware attacks.

Backups Are Being Targeted

We've previously written about how Conti ransomware can encrypt files and delete backups. But backups are still the most crucial component for ensuring recovery from ransomware—or any other data disaster, for that matter.

Safeguarding your backups demands adding another layer of data protection. That starts with a sound disaster recovery plan that includes a 3-2-1-1 backup strategy. But in a world where almost anything can—and does—happen, adding an air-gapped backup gives you one more layer of protection. And it can be a priceless but cost-effective addition to your data protection efforts.

That's why we found a post by DCIG's Jerome Wendt regarding the challenges of managing air-gapped technologies using backup software to be of particular interest. The post lists the five challenges of using air-gapped technologies to store backups, and it's well worth a read.

Arcserve provides logical and physical air-gapping solutions through its Arcserve UDP and tape backup software.

Unified Data Protection Includes Air Gapping

The DCIG post notes that properly implementing and managing your backup technologies—including air gapping—starts by selecting a backup software such as Arcserve UDP that addresses the critical management challenges listed. Arcserve UDP unifies data protection, prevents cyberattacks across on- and off-premises workloads, and even orchestrates recovery.

Arcserve UDP does more than support air gapping, of course. It protects against data loss and extended downtime across cloud, local, virtual, hyperconverged, and SaaS-based workloads from a single management interface.

Arcserve UDP also:

- Reduces downtime from days to minutes.
- Validates RTOs and RPOs, and service-level agreements.
- Deploys in minutes without the need for extensive training or professional services.
- Prevents ransomware attacks on critical disaster recovery infrastructure with available Sophos Intercept X Advanced for Server.
- Assures immutability of data backups with support for Amazon S3 Object Lock.
- Restores faster with instant VM and bare metal recovery (BMR), local and remote virtual standby, application-consistent backup, and granular restore.
- Includes hardware snapshot support and extensions that deliver high availability and tape support.
- Protects Microsoft 365 workloads on-premises with deep data reduction, granular recovery, and offsite replication.

Tape Backups Offer Affordable Air Gapping

While many storage technologies can hold air-gapped backups, tape—a vintage technology that Univac first introduced in 1951—is still an important and cost-effective option. Allied Market Research says the global tape storage market will reach $9.42 billion by 2030 at a CAGR of 7.8 percent. Tape isn’t leaving the marketplace anytime soon.

If you’re looking to upgrade your existing tape backup efforts, Arcserve Tape Backup software is a solution worth considering. A staple in global data centers for more than 28 years, Arcserve Tape Backup:

- Eliminates IT time wasted sifting through data with centralized management and storage resource manager (SRM) reporting.
- Monitors the status of all backup activities.
- Identifies nodes that are taking the longest to back up.

- Locates backed-up data quickly and tracks volume, disk, and media.
- Enables sophisticated functionality for VMware, Microsoft Hyper-V, and Citrix XenServer platforms.
- Simplifies system management of your entire environment and mitigates the risk of data loss on virtualized servers.
- Increases reliability with smart restore capabilities.
- Allows the redirection of restore jobs to other media containing the same data without any manual intervention.
- Quickly restores individual application objects from Active Directory, Microsoft Exchange, Microsoft SQL Server, and Microsoft SharePoint.
- Delivers faster, more efficient backups and restores UNIX and Linux data overs for SAN-based backups.
- Meets application-specific requirements with backup to disk, backup to tape, disk-to-disk-to-tape (D2D2T), disk-to-disk-to-cloud (D2D2CC), virtual tape library (VTL), hardware snapshot support, multiplexing, and multi-streaming.

That's quite a list. Add it all up, and it makes managing air-gapped tape backups easier than ever.

Get Answers About Air Gapping

Learn more about your air-gapped backup options by talking to an Arcserve technology partner.

Read the full DCIG post here.

Why Your Company Needs a Next-Gen Business Continuity Strategy

A recent survey of CEOs by the publication Chief Executive found that one-third expect their work model for the remainder of 2022 to be a mix of remote, hybrid, and onsite workers. Only 31 percent expect to have their people in the office, with the rest of the CEOs expecting their workforce to be either hybrid or fully remote, or they're undecided. The pandemic drove this move to a new work paradigm in which employees work from anywhere. Now, many companies are implementing infrastructure modernization initiatives as they journey through digital transformation.

These changes have brought on new challenges. These include increased complexity and new vulnerabilities. The most crucial question that companies need to answer is how will they keep their operations running smoothly if they're struck by a natural disaster, hardware failure, cyber attack, or downtime caused by human error?

IT teams need to reevaluate their approach to business continuity if they are going to overcome these challenges. The IT metrics used to measure business continuity don't change. What still matters is uptime, data and application availability, and data backup and recovery. But the transition to hybrid work demands a new business continuity strategy that acknowledges IT's growing responsibility to keep everything running all the time.

This change applies to every company that relies on technology, and today that's almost every business. Say the French restaurant down the street uses cloud-based software that lets customers order and pay with their phones. If this service is disrupted, the restaurant not only loses orders during the downtime, it also takes a hit to its reputation.

Business Continuity Is a Requirement

Due to businesses' increased reliance on data, pressure continues to mount to achieve 24/7 uptime. An independent global study commissioned by Arcserve found that 83 percent of IT decision-makers believe 12 hours is the maximum acceptable downtime for critical systems before there is a measurable negative impact on business. But for many businesses, even that is too much downtime.

A 2021 study by IBM found that just one hour of downtime for a single server can cost firms $100,000. If you're running 1,000 servers, that's a heart-stopping $10 million per hour.

Start With a Plan

Every organization should have a business continuity plan. This step-by-step plan will guide your response to a disruption when time and efficiency are essential. Your plan should address any contingency or type of disaster so you can quickly address the cause, minimize downtime, and control any damage.

Make sure your plan is comprehensive, listing the resources you'll need in a crisis, like data backups and storage locations. It should also include your team's steps to notify company leaders, communicate with customers, and sustain productivity.

You should test your plan regularly to ensure it will work when needed. Testing will help you identify and address vulnerabilities before they are exposed. With regular testing, you can also be confident that your data is safeguarded and can be restored no matter what.

Make Data Backups a Priority

Most companies will suffer a data loss at some point. In the recent survey commissioned by Arcserve, 74 percent of respondents in mid-sized companies said they had experienced a data loss in the past five years. And 52 percent said they couldn't recover all their data after a loss.

That's why you need to adopt a 3-2-1-1 data backup strategy to prevent data loss. The strategy calls for three backup copies of your data on two different media (disk and tape, for example), with one copy stored offsite for disaster recovery. The final "1" stands for immutable storage. Immutable backups convert your data to a write-once read-many-times format that can't be altered, deleted, or encrypted.

Establish Your RPOs and RTOs

Your plan also needs to include your recovery point objectives (RPOs) and recovery time objectives (RTOs) and how you will meet them. Your RPO is the amount of data your business can tolerate losing before it experiences severe damage. It's the determining factor behind how frequently you need to back up your data—and the technologies you'll need to support that schedule. You may set different RPOs for different business functions, with dynamic files like financial transactions requiring frequent backups for a minimal RPO. Static files that aren't crucial to operations can be backed up less frequently, allowing a longer RPO.

RTO is the amount of time before your operation can be up and running following a disaster. Once you've established your RTO, you can make informed decisions about your data resilience plan. If you decide your organization can only tolerate an hour of downtime, you'll need a recovery solution to meet that one-hour threshold.

Go Next-Gen

Businesses can’t tolerate digital disruptions anymore because the costs can be astronomical and even kill a company. So, go with a next-gen solution, test it in conjunction with your disaster recovery plan, and be ready for anything.

To learn more about Arcserve’s next-gen data protection, backup, and disaster recovery solutions, talk to an Arcserve technology partner or check out our free trial offers.

E-book

Need Answers?

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

arcserve®

+1 844 639-6792
arcserve.com