arcserve®

Business Continuity Planning and the Role of Air Gapping, Immutable Storage, and SaaS Backup in Data Protection and Ransomware Recovery

Table of Contents

6 Steps for Developing a Business Continuity Plan

Every minute that your business is offline is expensive. While every business differs, you'll find some guidelines for projecting your downtime costs in this post. But there are other costs beyond dollars. Your reputation, for example, is hard to repair if you're unavailable when your customers need you and your company name is front-page news. No company wants to be responsible for delivering a lesson in security to the rest of its industry, as noted in the headline of a Forbes article about the Colonial Pipeline hack.

The best way to avoid these costs is through business continuity planning, including data backup and disaster recovery plans. That way, if any disaster strikes—from a ransomware attack to a hurricane—you know what to do and have the tools to keep your business running. With that in mind, let's look at the specific areas you need to address as you develop your plan—and how you can ensure it will be effective if and when it is required.

1. Assess Your Risks

Regardless of your company's size or structure, you must understand where your risks lie to reduce or eliminate them. You'll want to list every potential threat to your business operations so you can consider how to mitigate those risks most effectively. Risk assessment should be a team effort, addressing every aspect of your operations and every kind of threat, including:

- Natural disasters
- Cyberattacks
- Ransomware
- Human error
- Unplanned downtime
- Power outages
- Data corruption
- System failures
- Hardware failures

2. Perform a Business Impact Analysis

As noted on Ready.gov, the business continuity planning process should include a business impact analysis that addresses lost revenues, increased expenses, regulatory impacts, and other factors. You'll also find a helpful business impact analysis worksheet on the Ready.gov site. As part of this analysis, you need to establish or update your recovery time objective (RTO)—the amount of downtime your business can tolerate—and your recovery point objective (RPO)—the amount of data your business can afford to lose before the impacts are just too significant.

3. Identify Critical Systems

With a clear understanding of your risks and the potential impacts on your business, the next step is identifying mission-critical systems and functions. This list will help you prioritize these systems for protection and recovery. As you build out your business continuity plan, mapping your network, hardware, and software topology and dependencies can be invaluable for locating and troubleshooting issues, thus accelerating recovery.

4. Back Up Your Data

While you are likely already backing up your data in some form, your risk assessment and business impact analysis should give you a solid foundation for choosing the most effective backup strategy and solution for your needs. At a minimum, your data backup solutions should adhere to Arcserve's recommended 3-2-1-1 backup rule: Keep three copies of your data in two media types, with at least one copy offsite in the cloud or secure storage and one copy in immutable storage.

5. Plan for Recovery

Every IT business continuity plan should include a disaster recovery (DR) plan. Your plan should account for procuring the technologies you need to meet your RPOs and RTOs. It should also designate your recovery strategy—from file-based recovery to virtual machine (VM) and cloud-based recovery.

6. Test Your Plan (Regularly)

If you need to implement your business continuity and disaster recovery plans, there's no time to waste. It is essential to test your IT business continuity plan to perform as expected if disaster strikes.

Conclusion

There's a lot to consider when developing your business continuity plan. And when it comes to business continuity technologies like backup and disaster recovery, it's worth talking to an expert. Choose an Arcserve technology partner and get the product information you need to make an informed decision.

Air Gapping: Offline Backups Ensure Recovery

The concept of air gapping has been around for decades. And thanks to our ever-growing ransomware risks, it's not going anywhere soon. That's really no wonder, given that hackers seem to find ways to overcome just about every obstacle IT teams can put in their path. Let's take a look at why air-gapped backups are worth considering.

What Does Air Gapping Mean?

TechTarget defines air gapping as "a security measure that involves isolating a computer or network and preventing it from establishing an external connection. An air-gapped computer is physically segregated and incapable of connecting wirelessly or physically with other computers or network devices."

Your backup device can't be remotely hacked or corrupted without an internet or other network connection or by using a virtual air gap for your backups. That leaves only a direct physical attack as a means to get to your data.

Air-Gapping and the 3-2-1-1 Backup Strategy

Traditionally, air gapping has been referred to in the context of tape backups, but today's options for backing up to the cloud offer a virtual equivalent of air-gapped tape. But, while the cloud's object-based defenses, like S3 Object Lock, offer immutable storage, a physically air-gapped backup gives you a final line of defense.

This ties back to our post about the updated 3-2-1-1 backup strategy. There we discuss how you should store one copy of your backups in an immutable format and another in a secure, offsite location. While your immutable backups should always be available, you may choose to backup and archive large volumes of data on tape because it's such a cost-effective option.

If that offsite copy is air-gapped, it's protected from malicious software, direct cyberattacks, and other threats. It also protects your backups even if ransomware compromises admin passwords or other data. If everything else fails, your air-gapped backups should be capable of restoring your entire network system.

Physical Air Gapping

Although air gapping is your ultimate defense against disaster, it can also be costly in terms of labor. When your backup device is completely disconnected from your network, the only way to access it is with direct physical contact. That limits your ability to automate backups, and even if you choose an automated solution, any device connected to a network could become compromised. That means going to the device and physically transferring data is a good choice if it can work within your infrastructure. That brings us to virtual air gapping, where software and processes replace physical separation.

Virtual Air Gapping

Arcserve Unified Data Protection (UDP) offers virtual air-gapping by replicating your primary recovery point server (RPS) to a secondary, remotely-managed RPS to create an air gap between the systems. This creates two autonomous systems with separate controls. The air gap results from using a secure connection to the secondary RPS using a regular, non-administrative user account and a data transfer via a block-based replication. If the primary RPS server is compromised, the block-based replication technology prevents any affected files from reaching the secondary RPS. You should take several other essential measures to protect the secondary RPS, which you can learn about by requesting an Arcserve UDP demo.

Tape Air Gapping Made Easy

One of the simplest ways to protect your air-gapped storage is with Arcserve Tape Backup Software. Tape offers an affordable, proven option for long-term storage of backed-up data. The software offers unique technologies that improve the economies of data protection by enabling more extended retention periods, reducing storage, and integrating powerful deduplication into your existing backup environment.

With Arcserve Tape Backup Software, you can store critical data on nearly any tape device, from a single tape drive to huge tape libraries. You can also manage more data in more locations and reduce the time spent managing backups, no matter how simple or complex your infrastructure is. And it’s perfect for air-gapped tape backups.

Conclusion

Ultimately, whether you choose to include air-gapped backups in your strategy depends on your unique situation. What matters most is that you have a solid backup and recovery plan in place and keep it up to date. By choosing an Arcserve Technology Partner, you gain access to the expertise and guidance you need to ensure your data is protected, backed up, and always recoverable.

A Deep Dive Into Immutable Storage: How It Works for Ensuring Data Protection and Ransomware Recovery

Immutable storage is recognized as one of the most effective data protection solutions for ensuring ransomware recovery. That's more important than ever, given that 66 percent of respondents to the Sophos State of Ransomware Report 2023 reported that their organization was hit by ransomware in the previous year. So, the odds are high that your organization will become hit if it hasn't already.

While most IT pros know about immutable storage, they may need help understanding how it functions. With that in mind, let's dive into the technical underpinning of immutable storage.

What Is Immutable Storage?

Think of immutable storage as your last line of defense for ransomware protection and data loss prevention. Data backed up to immutable storage is protected against any modifications or deletions.

At the heart of immutable storage systems is the write-once-read-many (WORM) technology. WORM technology prevents data from being overwritten or deleted once written to a storage medium.

Hardware-Based WORM

WORM was initially associated with physical storage media, such as optical discs, which use a laser to write data. Once written into the disc by the laser, data is physically prevented from being erased or modified. Modern implementations of WORM technology extend beyond physical media to software-defined storage systems, offering broader and more flexible applications of immutability principles.

Software-Defined WORM

Software-defined WORM solutions offer a more versatile approach to immutability, applying the principle at the file system or object storage level. In these systems, software controls enforce immutability by restricting write and delete operations on the files or backups saved as immutable, with the storage system modifying the file or object's metadata to mark it as unchangeable.

This metadata, a foundational file system component, acts as the gatekeeper, enforcing immutability rules. It also enables the dynamic application of WORM policies, where data can be immutable for a predetermined retention period without needing specialized hardware.

Locking Down Data: Set Retention Periods

In both hardware and software-defined WORM systems, data is “locked down” for a specified retention period when it is written. Defined by your policies and regulatory requirements, this retention period ensures the data can’t be altered or deleted until the set period expires. That gives you flexibility in managing retention periods, so you can apply policies based on the data type (see our post on data classification and tiering), compliance requirements, and business needs.

During the retention period, the storage system systematically blocks any attempts to modify or delete the data. This immutable data protection ensures data integrity, especially when historical accuracy, such as legal evidence or financial records, is paramount.

When the retention period expires, the data’s immutable protection status can be lifted so that it can be altered or deleted. This lets users delete outdated files and backups to save storage while ensuring compliance with required retention periods. Administrators can typically review and manage data as it approaches the end of its retention period and decide to extend the immutability, archive the data, or delete it if it is no longer needed.

Access Control Systems Enforce Immutability

File systems or object stores that support immutability implement rigorous access control mechanisms. These mechanisms are designed to restrict unauthorized access and operations on data, ensuring it remains unchanged once data is marked as immutable. Here are the common access control mechanisms in use today:

Discretionary Access Control (DAC)

In a DAC system, the data owner specifies who can access the data and what operations they can perform. While DAC is flexible, for immutable storage applications it is typically bolstered by additional controls to prevent data access for immutable storage applications.

Mandatory Access Control (MAC)

MAC systems offer tighter controls than DAC systems because they rely on fixed policies that system administrators define to control access. In the context of immutable storage, MAC can enforce immutability policies across different data tiers, ensuring that only authorized users and processes can access data based on their security clearance and the data classification level.

Role-Based Access Control (RBAC)

RBAC limits access and operations based on the roles of individual users within an organization. This method is effective in immutable storage environments because it can restrict who can mark data as immutable or alter immutability policies based on predefined roles, such as system admins or data managers.

Attribute-Based Access Control (ABAC)

ABAC provides a highly granular level of control by defining access permissions based on a wide range of attributes. These can include user attributes, such as department or role; environmental attributes, such as time of day; and data attributes, such as classification and immutability status. ABAC dynamically enforces access decisions based on complex policies considering multiple factors, making it highly adaptable to various security environments.

Cryptographic Access Control

Some immutable storage systems enforce access control using cryptographic means, such as digital signatures and encryption. Users must have the appropriate cryptographic keys to access or modify data, adding a solid layer of security. This approach ensures that even if a user technically has access to data, they can’t modify it without the correct cryptographic authorization.

Data and Ransomware Recovery from Immutable Backups

Data recovery is the most significant advantage of immutable storage. Since immutable backups are protected from threats, they provide a reliable recovery point following a cyber incident or data disaster. If ransomware strikes, you can revert to a pristine version of your production environment using an immutable backup.

Put Immutability to Work

With an understanding of WORM, you now know how immutable storage systems provide robust defenses against threats. For expert help implementing immutable onsite, offsite, and cloud data protection, backup, and disaster recovery, find an Arcserve technology partner.

Why SaaS Backup Should Be a Core Component of Your Business Continuity Plan

There are endless threats to your SaaS data. Only some IT professionals are fully aware of these threats, with the Thales 2023 Cloud Security Study finding that 38 percent of respondents rank SaaS applications as the top target for cyberattacks. In the same survey, 46 percent of respondents said they had experienced a data breach in their cloud environment.

While you may be able to fight back against many threats with today's cyber defenses, the same study found that 55 percent of breaches were caused by human error. That's a threat that isn't easy to combat.

What's worse, SaaS data breaches are more common than you may think, with AppOmni's SaaS Breach Info Center listing breaches to Microsoft 365, Okta, Equifax and Sony. That's why you need SaaS backup.

SaaS Data Backup and the Shared Responsibility Model

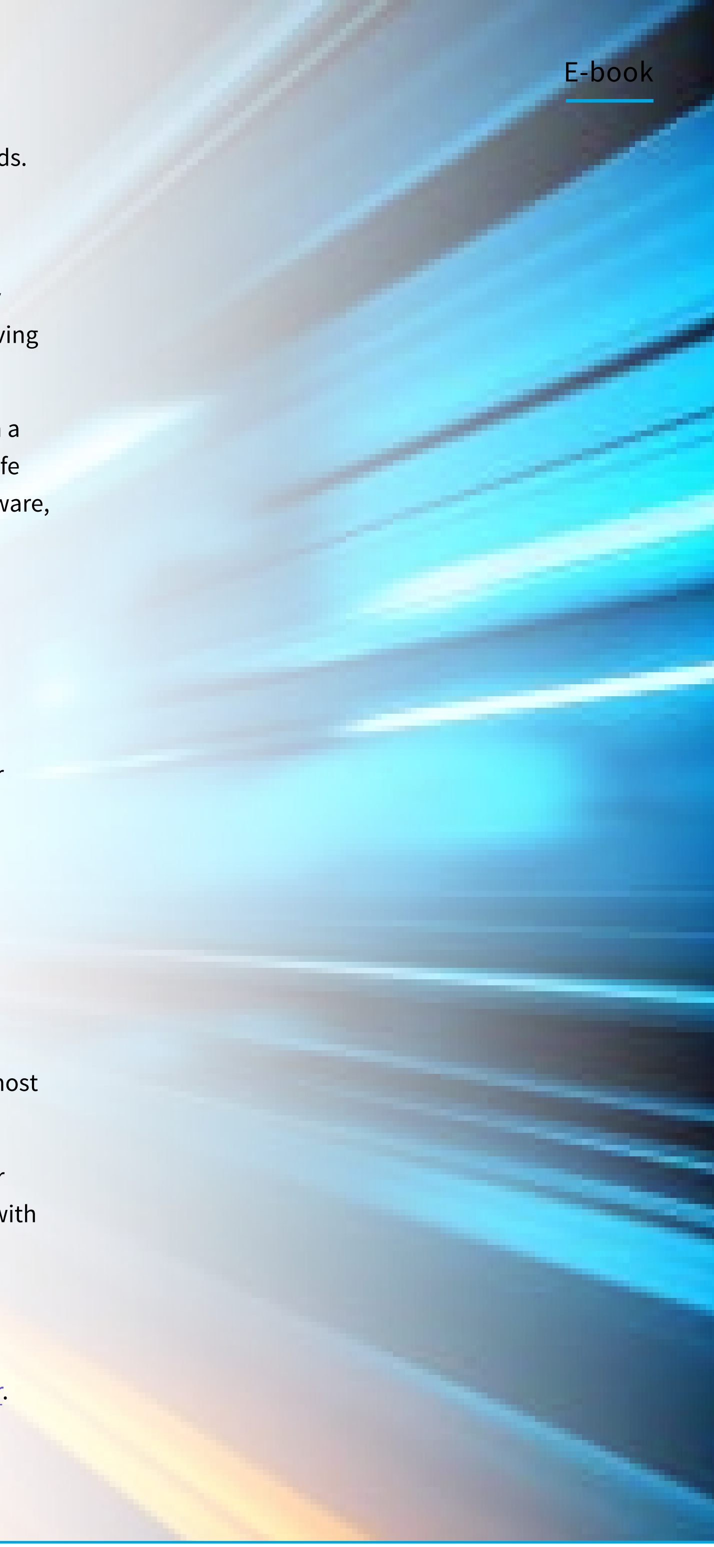
You may be aware of the shared responsibility model. But not everyone is. Arcserve's own global study finding that 43 percent of IT decision-makers believe cloud providers are responsible for data.

Microsoft says, "For all cloud deployment types, you own your data and identities. You're responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control." Translated into plain language, if your Microsoft SaaS data is lost due to a breach, ransomware, or other data disaster, it's your problem getting it back.

Why SaaS Backup?

If your company is like most, you depend on SaaS applications to drive your business. Without your SaaS data, your business will likely screech to a halt. That's why you must incorporate SaaS backup into your business continuity and disaster recovery plan.

The numbers bear this out, with the Thales survey also finding that the mean number of SaaS applications used at responding organizations was 97. However, most organizations use common SaaS apps like Salesforce, Microsoft 365, and Google Workspace too.



That’s a lot of precious SaaS data. And that’s why you need a cloud-native, cloud-to-cloud SaaS backup solution. Arcserve SaaS Backup is that solution, providing comprehensive protection for data hosted in SaaS application clouds.

Simple, Secure, and Scalable SaaS Backup and Recovery

Arcserve SaaS Backup is simple to set up. It takes just five minutes before protection starts, and management is easy with a single pane of glass that offers multi-tenant and role-based access controls (RBAC). Navigation is fast while giving you complete control over your protected data.

The solution also features immutable backups using a blockchain-based algorithm. Immutable backups are saved in a write-once-read-many-times (WORM) format that can’t be altered or deleted. You can be certain your backups are safe and that an unaltered copy of your data can be retrieved and restored, even if you’re the victim of ransomware, malware, or other form of attack. Think of immutable backups as your last line of defense.

With Arcserve SaaS Backup, your data is encrypted in transit and at rest, with a default 30-day delete retention. That makes it easy to restore files deleted in error.

Guaranteed Data Sovereignty

The Thales study found that 83 percent of respondents are concerned about the impacts of data sovereignty on their cloud deployments. And for good reasons, with the EU GDPR levying fines of up to $22 million or 4 percent of global annual turnover (whichever is greater) for non-compliance.

Arcserve SaaS Backup solves that problem by keeping four copies of your backup data in two different data centers within the same region. That guarantees both data sovereignty and backup redundancy.

The Most Cost-Effective SaaS Backup Solution

Ensuring business continuity with SaaS backup doesn’t have to cost an arm and a leg. Arcserve SaaS Backup is the most cost-effective solution available, with a single price per seat that includes all SaaS data protection functionalities.

These include custom backup retention settings to meet your compliance requirements and no additional charge for data traffic—ingress, egress, or transaction fees. Even better, you get unlimited data storage in our online cloud tier with Arcserve SaaS Backup, ensuring fast access and restores.

Learn More

Take a deeper dive into Arcserve SaaS Backup by requesting a demo or taking advantage of our 30-day free trial offer.

For expert help in putting the right solutions in place for your business, choose an Arcserve technology partner.

Need Answers?

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

arcserve®

+1 844 639-6792
arcserve.com