Acronis

WHITEPAPER

Hybrid solutions for sustainable, affordable backups

Like most small- or medium-sized businesses, you probably already have a backup solution in place. That said, even though you may no longer be relying on manual backups, your existing backup solution may not have kept up with the times.

There are a few common reasons SMBs start looking for a new backup solution:

- With more data to back up, you've outgrown your current platform.
- You're swamped by high data storage or transfer costs with your current platform.
- You've tested your solution and it isn't as effective for recovery as you need it to be.
- You're in an industry that requires your backups to comply with regulations.

As your data backup needs have evolved, so have the solutions that are out there. But it can feel overwhelming to weigh all the solutions available — especially on a budget. How can you know which features are absolutely essential?

This white paper will explore key concepts behind modern backup solutions, and in particular, the need for hybrid backup. It will also cover approaches for upgrading seamlessly while saving money.

Modern backup concepts

You may still remember when team members used to take backup tapes home with them. But the world of backups has changed dramatically since the days of manual tape backups and other removable storage media.

Today, backup is just one component hardening your organization's IT against both physical and cyberthreats. It's one important piece of the puzzle known as cyber risk management.

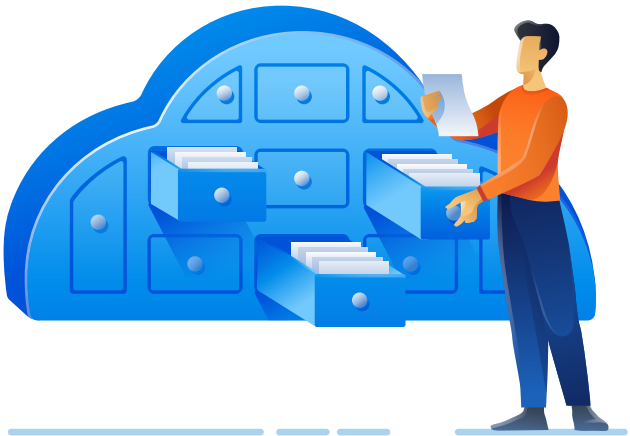
Beyond backup planning, you probably have these other components in place:

- Traditional antivirus scanning and remediation
- Vulnerability scanning and remediation
- DevSecOps: Building security into your development and release cycle
- Disaster recovery plans and protocols

However, even with all of these defenses, backup remains a critical part of your risk management plan.

An effective backup strategy ensures you'll be able to bounce back from the worst-case scenario.

But a backup program only works if you're capturing all of the information that's important to your business — and storing it in a way that you can easily access in a crisis. Here are some key concepts to evaluate when you're shifting to a more up-to-date backup approach:



Backing up distributed assets

Unlike older, on-premises data center models, your assets aren't all in one place. They're on-premises, but they're also virtual and highly distributed across the cloud (hyperconverged infrastructure). But your responsibility remains the same: You must back up all your company's assets, wherever they're located.You're also responsible for securing data in multiple locations; that is, everywhere your departments access and store it. This includes SaaS apps like Salesforce, Google Docs, Office 365, and more; data stored as part of big data and analytics; data associated with your remote workforce, DevOps, IoT, and more.

Plus, SMB backup needs are unpredictable: the volume of data you're backing up can increase dramatically with little warning — and come with a steep price tag for the sudden increase.

In short, today's data is …

- bigger than ever (taking up more space, costing more to move and store)
- changing faster than ever
- being stored on a more diverse range of devices than ever

And yet you still need to be able to back it all up and recover it in an emergency.

Backup scope

Doing a full backup is very complex, and takes a lot of time and storage space. Fortunately, it's not the only strategy available. All modern platforms offer a few primary backup methods:

- **Full backup:** This is exactly what it sounds like. All of your data is backed up and stored securely in a single destination.

Pros: A fast and simple recovery process, since the entire image is in one location.

Cons: Can take a long time and a lot of bandwidth and storage space.

- **Differential backup:** Backs up new versions of all files modified since the last full backup.

Pros: Offers fast backup and utilizes less space and bandwidth.

Cons: Requires a more complex restore process and access to the last full backup. It's also slower to restore, which means more downtime.

- **Incremental backup:** Stores new versions only for files modified since the last backup of any kind, whether full or differential.

Pros: Provides a very fast backup and requires the least storage space.

Cons: Restore requires access to all previous backups, including previous incremental backups. This is the slowest option in terms of restoration.

Backup type	What's backed up?	Backup time	Restore time	Space / bandwidth needed
Full	Everything	Slow	Fastest	High
Differential	Changes since last full backup	Medium	Medium	Medium
Incremental	Changes since last full or differential backup	Fastest	Slow	Low

Figure 1: Comparison of backup methods with relative time and bandwidth usage

Some backup platforms give you even more granularity. For instance, by letting you select a backup strategy for individual files or folders if they are particularly sensitive.

Most organizations use a rotating schedule of multiple backup types, such as performing a full backup once a week, followed by some pattern of differential and incremental backups in between.

Regulatory compliance

Before you choose a backup strategy going forward, it's important to be aware of regulatory issues that touch on backups: How often you perform them, how they're stored, and more. Certainly, regulations have affected every aspect of how IT is performed in today's world.

You may need to ensure that your backup strategy complies with regulations in one or more jurisdictions if you're:

- **Handling medical information** or payment card data (HIPAA, PCI DSS, GLBA)
- **Processing personally identifiable information** about customers, employees, or users (GDPR, CCPA)
- W**orking directly or indirectly with government** agencies, healthcare, or financial organizations (HIPAA, GLBA, NIST)

Some regulatory standards are not mandatory, but are highly advisable for building trust and hardening your security posture.

Most regulatory standards provide guidance for backup programs, including how often you need to back up your data, along with how often you need to perform full restore tests. Some have other specifications as well, such as PCI DSS, which specifies how backups are handled to protect cardholder data.

Obviously, failing to meet regulatory standards that apply to your business could result in fines. But more importantly, it opens you up to breaches that can destroy your business's reputation. That means that a lot more is riding on your backup program than ever before.

The 3-2-1 backup rule

This is easily the most important rule in modern backup planning, ensuring multiple types of redundancy and separation of storage location for maximum protection:

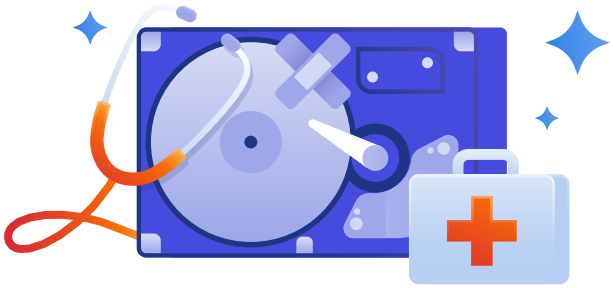
- 3 copies of your data (1 production copy and 2 backups)
- 2 physically independent devices storing your data (not the same physical server, RAID array, or cloud—for added security, this is often done to 2 different types of storage media)
- 1 copy in an offsite location (a different physical office or cloud-based data center)

Today, maintaining multiple copies of your data usually means a mix of cloud and on-premises — possibly involving a VM component.

With careful planning, you can also ensure that your 3-2-1 backup solution provides geo-redundancy, meaning that in the event of a power outage, network outage, or natural disaster in the primary region, your data is still safe.

However, storing a backup in a safe geographic location isn't enough. In fact, the 3-2-1 strategy, while extremely important, isn't enough on its own either. When you're restoring after a geographic or other major catastrophe, you're often doing it to bare metal, since the original device and location are unavailable.

Unless your backup platform lets you restore to different hardware, you may be left holding onto a backup you can't really use. That's why restore tests are important, and why they need to be planned to reproduce actual situations you could encounter in an emergency.



Challenges in modern backup operations

All of the concepts explored so far present specific backup challenges for a typical SMB IT department:

- Cost of on-premises or other physical backup [high capital expenditures (CAPEX) costs] and an inability to scale
- Cost of cloud (storage, transfer, download)
- Costs and optimization of cloud-to-cloud backup — protecting data from all your SaaS and other business-critical applications
- Restoring to bare metal or dissimilar hardware

Cloud costs are particularly difficult to estimate and rein in. Cloud provides you with the ability to scale, but it's very easy to lose track of costs, diminishing your ROI and making it difficult to leverage economies of scale. For instance, long-term, slower-access storage is generally less expensive; but your backup strategy may not give you the visibility and insight into data use that would let you take advantage of this.

Finally, recovery speed has also become critical, and bare-metal recovery time must be a major factor in planning. This is a problem in traditional disaster planning, yet it's obvious if you think about it. The exact hardware configuration you usually use might not be available in a crisis. In such a situation, can your backup platform still function?

It's not enough to get up and running eventually. Every minute your systems are down translates to lost productivity, reputational damage, and missed transactions.

What is hybrid backup?

Today, you'll find many backup solutions claiming to provide a full response to SMB needs exclusively in the cloud. It's tempting to go with that type of solution for simplicity; certainly, at a time when you are facing so many complex demands, you don't want two parallel solutions — one platform for local backup and another for cloud.

So why not transition to a cloud-only solution?

The short answer is that local backup still offers competitive advantages:

- Lightning-fast, super-simple backup and restore
- No clogging precious network bandwidth
- Uses hardware you own, preventing cloud cost spikes through inefficient usage

All in all, local backups still provide a highly effective, affordable backup solution.

However, cloud can still be an important part of your backup strategy. For one thing, any cyber-risk management strategy (along with some regulatory requirements) demands that you avoid a single point of failure (SPOF). A great example of SPOF is the Facebook outage in November of 2021, which also took down Instagram and WhatsApp because they were all housed on the same servers.

Your physical site doesn't offer enough protection against SPOF risk. That's why the 3-2-1 rule requires you to keep at least some of your backups off-site. That's where hybrid backup comes in.

Hybrid backup platforms merge the best features of cloud and local backup. In many ways, this offers the best of both worlds:

- Simple, fast recovery from local backup when original hardware is available
- Secure copy available in the cloud when you need to recover from a larger-scale event

Top reasons organizations turn to hybrid backup for a more comprehensive solution:

- Business continuity
- Not all clients want everything in the cloud (SPOF; vendor lock in; geographic security)
- Data sovereignty
- Regulatory compliance
- Portability
- Faster restores
- Disaster recovery scenarios

Fortunately, today's best risk management platforms combine the best of cloud and on-premises backup, saving you money and offering end-to-end protection.

Acronis Cyber Protect: A hybrid solution offering security and flexibility

Acronis Cyber Protect gives you a hybrid backup solution emphasizing speed, security, and flexibility — all while helping you keep costs under control by optimizing cloud and minimizing bandwidth.

Acronis single solution integrates email security, backup, disaster recovery, next-generation anti-malware, and cyber protection management — thus simplifying IT and making all your security responsibilities easier to manage.

Plus, Acronis Cyber Protect is fully integrated with other cyber protection products, meaning your backup tools work hand in hand with other security tools. For example, you can ensure that backups are automatically scanned for malware and other threats. You can also apply patches seamlessly to backups and live systems, so you can get up and running from backup more easily.

Acronis Cyber Protect makes sure you're covered for every possible outcome with comprehensive cyber protection. Trust Acronis to protect your data across all your platforms — locally and in the cloud.

Upgrade your backup and security posture with Acronis Cyber Protect

Get a demo

Acronis

Learn more at
www.acronis.com