



SECURE YOUR DATA,  
**PROTECT YOUR  
BUSINESS**

How to create a backup strategy  
fit for your needs



# TABLE OF CONTENTS

<b>BUILD REDUNDANCY INTO YOUR DATA PROTECTION .....</b>	<b>3</b>
<b>BACKUP REGULATIONS AND BEST PRACTICE .....</b>	<b>5</b>
<b>REGULATIONS TO KEEP AN EYE ON... ..</b>	<b>6</b>
<b>...BASED ON YOUR LOCATION .....</b>	<b>7</b>
<b>...BASED ON YOUR INDUSTRY .....</b>	<b>8</b>
<b>UNDERSTAND YOUR DATA AND RECOVERY GOALS .....</b>	<b>10</b>
<b>CREATING A BACKUP STRATEGY: WHAT ARE YOUR OPTIONS? .....</b>	<b>12</b>
<b>FILE, AND APPLICATION BACKUP, AND DISASTER RECOVERY .....</b>	<b>12</b>
<b>LOCAL, OFFSITE, AND HYBRID BACKUP .....</b>	<b>13</b>
<b>BACKUP METHODS .....</b>	<b>14</b>
<b>ADDITIONAL FEATURES TO CONSIDER .....</b>	<b>16</b>
<b>PLAN YOUR BACKUP STRATEGY .....</b>	<b>18</b>
<b>ABOUT NOVABACKUP .....</b>	<b>19</b>



# REDUNDANCY

## Build redundancy into your data protection

As the way you use your data becomes increasingly crucial to your company's success, so does the importance of protecting it. Your day-to-day operations rely on the data you hold and losing that data can spell disaster.

Almost 70% of small businesses close within a year of a large data loss. <sup>i</sup>

You need to protect yourself from data loss on three fronts:

- 1 External threats:** Ransomware and other malicious software are growing in frequency and maturity. Plus, non-cyber threats like natural disasters and extreme weather are also on the rise.
- 2 Internal threats:** Software and hardware failure can also cause you to lose your data. And human error could lead to accidental deletion.
- 3 Remote systems:** A rise in remote working means you may have more devices to keep track of on a variety of networks. This gives attackers more entry points to your system and makes it harder for you to keep track of security.

Prevention methods like keeping antivirus software up to date and increasing awareness across your team are an absolute must, as 68% of data breaches involved a human element (such as human error, misuse, phishing, and stolen credentials). <sup>ii</sup>

Unfortunately, even with the most diligent protection, data breaches do still happen. In fact, 73% of healthcare organizations reported that their data was encrypted in 2023—the highest rate in three years. <sup>iii</sup>



When human error or malicious attack cause you to lose your data, it disrupts operations and puts pressure on your finances. You can't operate fully, if at all, until you can restore your data. And that's where a good backup is invaluable.

"It took 31% of organizations between one and six months to recover from a ransomware attack after paying the ransom. Meanwhile, 45% of those using backups recovered within a week."

Sophos <sup>iv</sup>

This document will guide you through how to create the right backup strategy for your business and everything you need to consider along the way.



# BEST PRACTICES

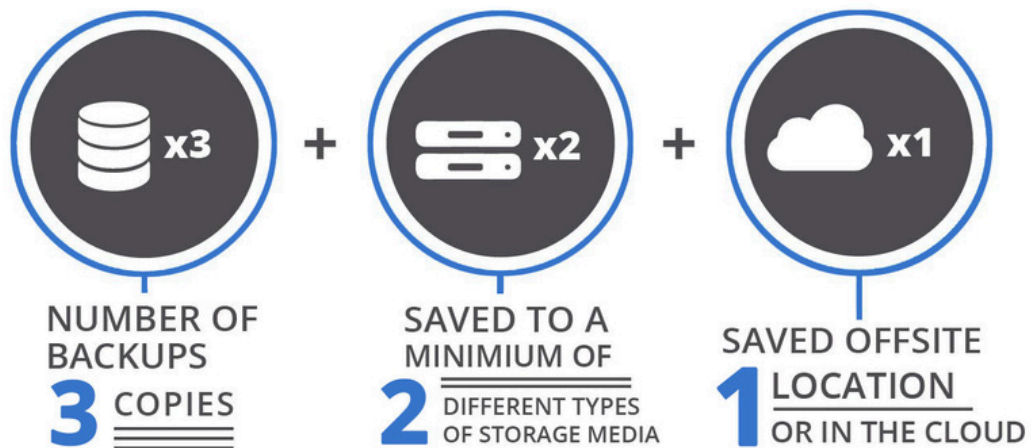
## Backup Regulation and Best Practice

Backup isn't just making a copy of important files or saving data to a company OneDrive. Those things are important, but the protection from a comprehensive backup strategy goes much further.

Backup is much more powerful than a simple copy of a file. It's a safety net for your business-critical data. Not only does it make copies of your files, it also keeps multiple versions over time in multiple locations. That means you can go back to any previous point in time if something goes wrong.

### The 3-2-1 Rules of Backup

One of the most simple and effective best practices to follow when backing up your data is the 3-2-1 rule:



Having multiple copies of your data on different storage media means that, even if one gets corrupted, you have redundancies to fall back on. Plus, keeping a copy of your backup offsite or in the cloud means that if data loss occurs due to physical damage to your site, like from natural disaster, you have a backup that's out of harm's way.

## Regulations to keep an eye on...

As businesses produce more data, regulation around the protection of sensitive information has become increasingly important. Governments worldwide are constantly creating new laws and updating existing ones to ensure organizations do everything they can to keep private data protected.

Organizations of all sizes must comply with data protection and privacy laws to ensure the security of their own and their customers' information, protect their reputation, and avoid the heavy fines that can be imposed for non-compliance. However, compliance can be a challenge when IT resources are already spread thin and are often working with a limited budget.



74% of managed service providers' clients struggle to comply with regulations like HIPAA, GDPR, and PCI-DSS. <sup>v</sup>

Backup strategies and solutions can be customized to meet your needs and the specific standards and security regulations for your location and industry.

## ...Based on Location

### North America

Requirements are ever-evolving due to constant changes in technology, so here are some crucial regulations to look out for in North America.



**California Privacy Rights Act (CPRA):** This amendment to the California Consumer Privacy Act (CCPA) came into effect on January 1, 2023, with the goal of giving consumers more say in how their personal information is used by businesses that gather it.

This law limits what information can be collected, how consumers are notified of collection, and how data is shared with other businesses. It also gives the consumer a right to know what specific information a company has about them, and request that information be corrected, limited, and even deleted.

California was the first state to launch a data protection law, and there are now similar laws in Virginia, Connecticut, Colorado, Utah, Michigan, Ohio, New Jersey, and Pennsylvania to regulate how data is collected and protected. While the laws are similar, there are specifics that companies working with personal information in these states should be aware of.



**Quebec's Law 25:** All businesses that collect personal information and operate in Quebec are required to receive consent before using, transferring, and disclosing data. The law has been amended many times over the years, and major changes came into effect on September 22, 2023.

## Europe



**General Data Protection Regulation (GDPR):** GDPR governs the protection of personal data of EU citizens. It requires companies to take adequate measures to protect personal data—including using secure methods for backup—and notify authorities in case of data loss or theft.

GDPR is a broad law that regulates the use and storage of information for all of the EU, so many countries have added their own regulations to align with country-specific requirements.



**Federal Data Protection Act (BDSG) in Germany:** BDSG complements GDPR in Germany and contains additional rules for data processing and security. In particular, security agencies must adhere to BDSG regulations, as GDPR rules do not apply to them.

### **...Based on your industry**

If you're in an industry that deals with sensitive data, you're likely to face an additional regulatory burden.

#### Healthcare

Healthcare organizations, and especially medical practices, are a common target for cyber criminals. What's more, the healthcare industry holds people's most sensitive data in patient records, so it's vital to stay on top of compliance regulations and the latest technological advancements.



More than 60% of cybersecurity incidents adversely impact patient care.<sup>vi</sup>

**Health Insurance Portability and Accountability Act (HIPAA):** HIPAA is a US law that governs the protection of healthcare data. It's designed to implement safeguards for data protection along with appropriate access and use of that information.

Guidelines are in place to ensure that all entities that handle medical data take the necessary measures to securely store patient information, with backup being a critical component.



### Ecommerce

Payments and transfers are also targets for malicious actors, so it's crucial for any business that holds payment information to maintain robust data security. In fact, any system that might affect the credit card data environment, even managed service providers (MSPs) that may not be processing the data themselves, will have security requirements to maintain.

**Payment Card Industry Data Security Standard (PCI-DSS):** Companies processing credit card data must ensure the secure storage and transmission of this information, often including secure backup methods. Organizations need to identify and document all web assets and ensure applications and system components are securely configured, and that vulnerabilities can be identified.



# GOALS

## Understand your data and recovery goals

Backup isn't just making a copy of important files or saving data to a company OneDrive. Those things are important, but the protection from a comprehensive backup strategy goes much further.

Backup is much more powerful than a simple copy of a file. It's a safety net for your business-critical data. Not only does it make copies of your files, it also keeps multiple versions over time in multiple locations. That means you can go back to any previous point in time if something goes wrong.

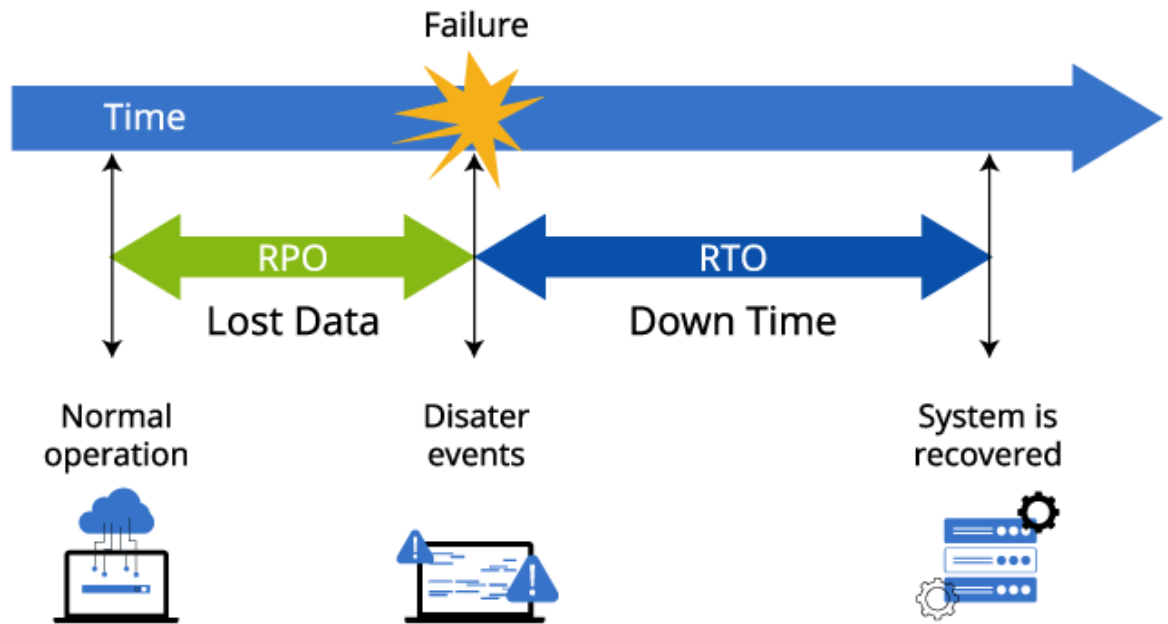
- ✓ Take inventory of existing IT systems, applications, and data, as well as remote locations and at-home employees, to identify key systems, data, and potential future needs.
- ✓ Establish your data dependencies and the information your business relies on to function. As part of this process, consider how financial and customer data interacts and affects decision-making, as well as any contractual obligations you must uphold.
- ✓ Consider how much your data changes. Some data you hold will change every day as information is added or adapted. This will benefit from a more frequent backup than data that doesn't change much over time.

Every organization is obliged to keep business records for a certain period of time—often ranging from six to ten years depending on location and industry. Classifying your data into critical, operational, business, and personal categories will help you determine its retention period. Establishing retention policies also helps you use your storage media more efficiently by ensuring you remove older or unnecessary backups.

Understanding your data dependencies will help you assess how long you can keep your business up and running if that data is lost, or how much of it could be lost in a worst-case scenario. With this insight, you can establish the goals a backup strategy must meet.

Your recovery goals are another a key element to any backup strategy, and are split into two components:

- 1 **Recovery Time Objective (RTO):** The RTO is the maximum tolerable length of time that a computer, IT system, network, or application may remain out of operation.
- 2 **Recovery Point Objective (RPO):** The RPO is the maximum amount of data that an organization can tolerate losing or having to recreate in the event of data loss, and still be able proceed with normal operations.



Determining your RTO and RPO helps you understand your organization's requirements to perform necessary business functions, so you can define an appropriate backup strategy.

Understanding RTO helps you build prioritization into your backup strategy. You need to understand your bandwidth limitations, which can directly impact your backup strategy. Plus, you'll need to consider where you hold your backups, especially your offsite copy, which will be quicker to recover if it's in the cloud rather than at a physical location you need to travel to.

Your RPO will help define the intervals between backups. Typically, business-critical data is backed up once a day (or more) and scheduled to run at a specific time to avoid any infrastructure performance impact. For most organizations, evenings are the most common off-peak hours of availability for backups.

# BACKUP STRATEGY

## Creating a backup strategy: What are your options?

When establishing your backup strategy, it's important to consider all your options before working out which is the right fit for your business. Choosing the right solution is critical to ensure that business-critical data is available after any type of data loss scenario.

### File and application backup, and disaster recovery



**File backup:** The purpose of a file backup is to be able to restore individual files and folders quickly and easily. No matter if a single file was lost or the internal hard drive stopped working, a file backup is the most efficient method to get business-critical (or not-so-critical) information back.



**Application backup:** An application backup ensures all data associated with the application, including its configuration and dependencies, is preserved. They extend the concept of file backups to more complex data such as databases, entire applications, or even snapshots of virtual machines.



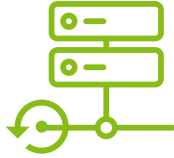
**Disaster recovery:** With disaster recovery, you are able to restore your entire operating system and its data. This means, in the event of disaster, you can recreate your entire system to existing or new hardware—or mount it as a virtual machine—in one go.

File, and application backups, as well as disaster recovery all have a role to play in a comprehensive backup strategy and can be scheduled at different frequencies. For example, you may backup business-critical files more often than your applications.



## Local, offsite, and hybrid backup

As part of the 3-2-1 rule, you need to keep backup both on and offsite. That means having a:

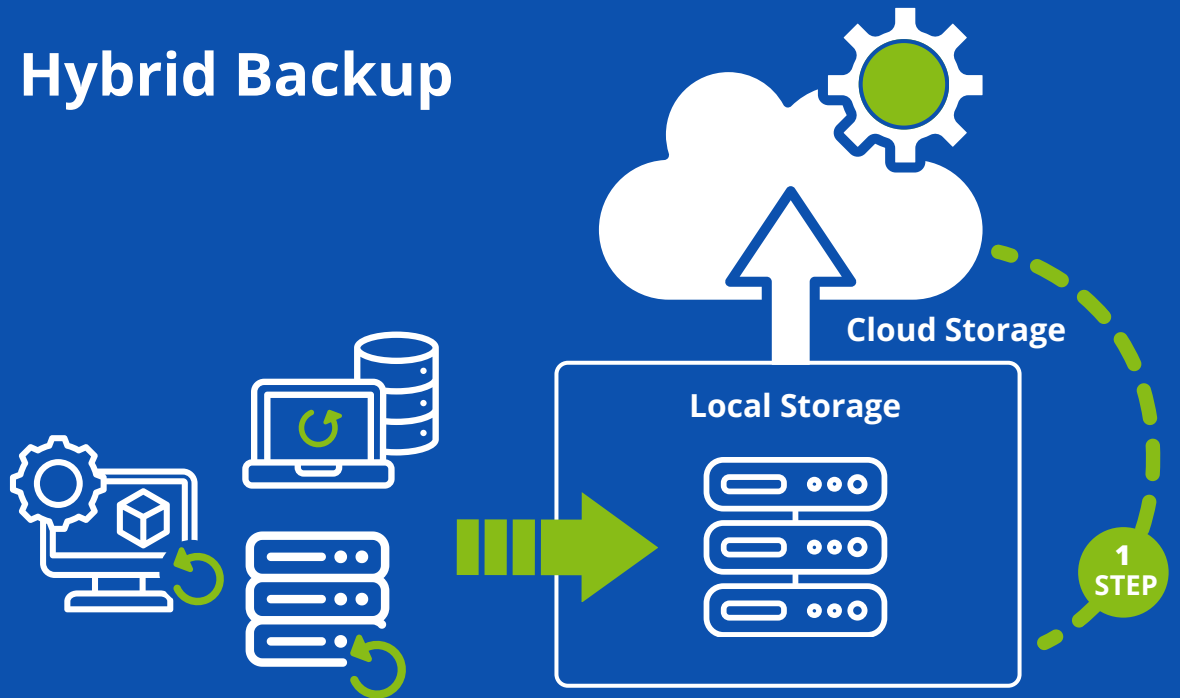


**Local backup:** A backup stored on a device located in the same office or area is usually referred to as a local or onsite backup. Because it's directly connected, it provides the fastest file and system recovery.



**Offsite backup:** An offsite backup is the only way to recover data if the local backup is corrupted or otherwise inaccessible. Today, it's common for businesses to use cloud storage as their offsite location.

## Hybrid Backup



But keeping track of two backup locations doesn't need to be complicated. With a **hybrid backup solution** you can combine local and cloud backup in one backup job, sending all data first to the selected local storage device and then from there to the cloud.

## Backup Methods

Traditionally, there are three main backup methods you can use, each with its own advantages and drawbacks. However there's now another way that takes the best of all worlds: Incremental Forever backup.



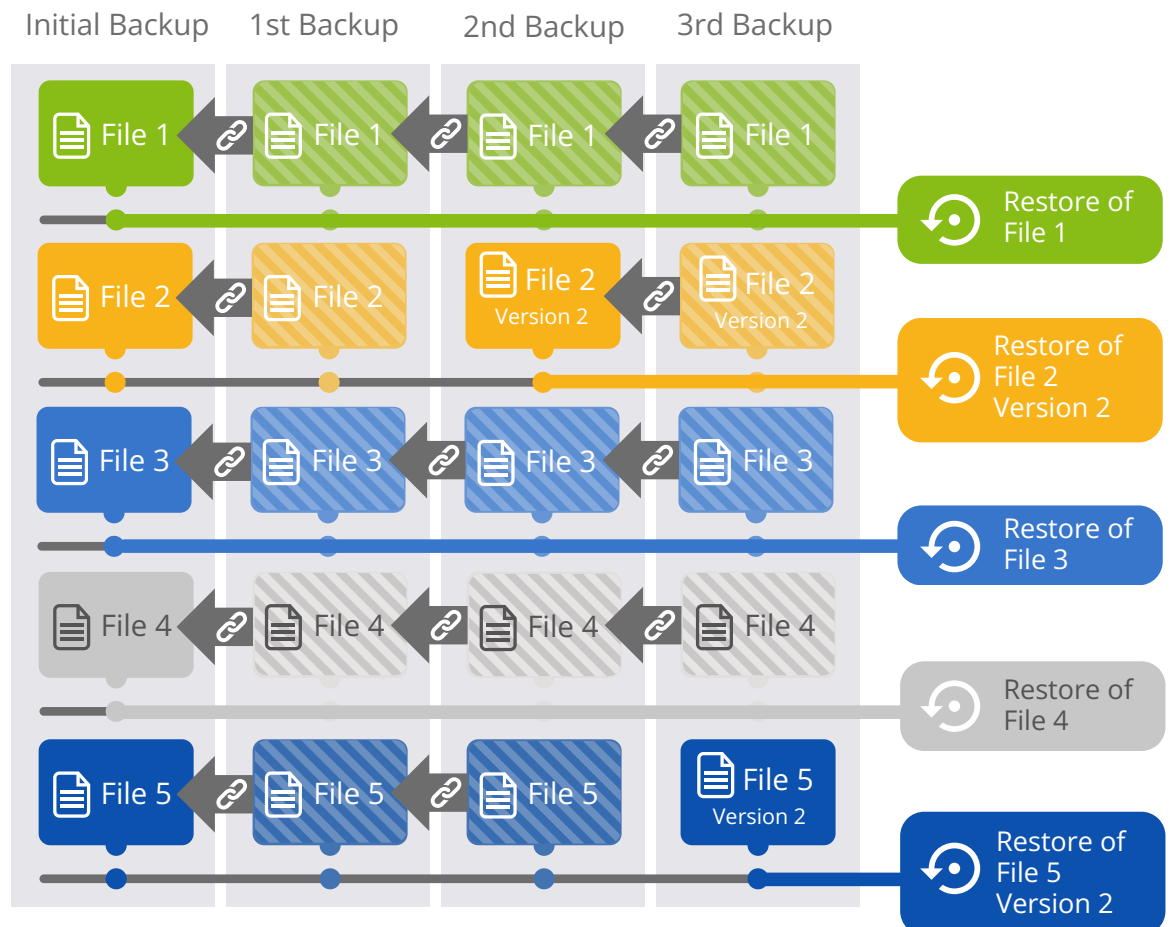
### Traditional Backup Methods

- ✓ **Full backups** include all data at a given point in time, which makes restores straightforward. However, they are storage-intensive and time-consuming, making them impractical for regular use—especially for small or medium businesses with growing data sets or MSPs that need to look after multiple clients.
- ✓ **Incremental backups** only capture changes made since the last backup, so they're much faster and more storage-efficient. However, restores can be cumbersome, as they require the initial backup and each incremental backup to rebuild a full picture of your data—and this can be unreliable.
- ✓ **Differential backups** include every change made to your data since your last full backup. This simplifies restore, as you only need your full backup and your most recent differential backup to capture everything. However, it creates a lot of redundant data, adding to your storage footprint.

## Incremental Forever Backup

Incremental Forever backup takes ideas from traditional incremental and differential backups while eliminating their weaknesses. It uses the following process:

- ✓ **Initial full backup:** The process starts with a single, complete backup of all selected files.
- ✓ **Incremental backups only:** Subsequent backups capture only the changes since the last backup.
- ✓ **Efficient data linking:** Each increment contains links to all previous versions of a file or folder, even if it hasn't changed. Similarly to differential backup, each increment retains all information, but without data redundancy between backup files.



The main advantages of Incremental Forever backups are that they significantly reduce backup times after the initial full backup, and by eliminating data redundancy, they lower storage costs, too. You also get simplified restores, with automated links between incremental backups and flexible retention that ensures critical data is always available as old files are removed.

## Additional features to consider

### Storage Media

Having multiple copies of your backups in multiple locations requires a mix of backup storage. When choosing the best storage media for you, you should be able to choose those that make the most sense for your environment. This could be a mix of:

- ✓ **External hard drives (HDD), solid state drives (SSD), USB drives:** These are easy to use, have a high storage capacity, are relatively cost-effective, and transfer data quickly. However, they're vulnerable to physical damage and theft.
- ✓ **Network Attached Storage (NAS):** This delivers centralized data storage with options for built-in redundancy. However, it comes with a high initial purchase cost and requires some technical knowledge for setup and management.
- ✓ **Cloud storage:** This provides easy access from anywhere, is immediately scalable, and comes with vendor-managed security. However, it requires an internet connection to back up and restore your data.



### Compression

By using software to compress your data when it's stored on your backup media, you can save a significant amount of storage space and time.



## Encryption

Encryption keeps your data secure and only accessible by trusted parties—which is particularly important for data stored offsite. There are two main types of data encryption:



**Data-at-rest encryption:** This protects your data when it's on your computer or another storage medium, such as the cloud, and ensures no one can access it without the right encryption key.



**Data-in-transit encryption:** This additional encryption mechanism protects your data from unauthorized access while it's in transit to the storage medium.



## Automatic Backups

A good backup solution should perform backups automatically without requiring constant manual intervention. You can set your backup schedule, and leave the software to reliably carry it out for you. Even better, you can include a holiday schedule to pause backups when your customers or colleagues take a well-deserved vacation.

## Notifications, reports, and alerts

Regular reporting on the status of your backups and any problems that may have occurred is critical to ensuring your backup can restore files and systems when you need them.

## Versioning

A good backup solution should allow you to store multiple versions of your files and systems in case you need to revert to previous versions.



# PLANNING

## Plan your backup strategy

Now you have:

- Understood regulations and best practice
- Identified your business-critical data
- Defined your recovery goals
- Considered the right backup options for your business

...it's finally time to map out your backup plan.

### An example backup plan

Protecting business-critical data that needs to be recovered quickly:

- Run a disaster recovery backup of your system **monthly**
- Run backups of data and applications **daily**, with 30-day retention locally and 90-day retention in the cloud

Protecting data that rarely changes:

- Run a disaster recovery backup of your system monthly
- Run backups of data and applications weekly with 30-day retention locally and in the cloud

For a well-rounded strategy, we recommend using a combination of backup types that keep your data in multiple locations. Backup your business-critical data files most frequently, especially if they often change, while also keeping regular disaster recovery and application backups. With the right backup solution, you can schedule backups to run automatically and set appropriate retention times for your data.

Good backup solutions offer comprehensive support from experts in backup. So if you're not sure what the right strategy is for your business, you can talk it through and get the answers you need.



## Document your backup plan

When you've established your backup strategy, you need to document it. Having your strategy established and written down will help you keep on top of your backups and ensure you know where your data is held if you need to recover it.

Document:

- What's backed up, to where, and when
- Data retention rules
- Who's responsible for what
- Who's going to check the backup regularly
- How often backups will be reviewed
- How often new data, applications, and systems will be added to the backup schedule

If you work with a Managed Service Provider, discuss these backup plan documentation requirements with them so you know they're doing everything they can to protect your data.

## Test your strategy to ensure data recovery

Probably the most important aspect of your backup solution is its ability to recover your information. It's vital that the backup software actually works in the worst-case scenario.

That's why, in addition to a well-planned backup strategy and regular backups, it's important to test those backups periodically.

- Test your backups and verify that they can recover your data and systems.
- Check the backup is working and sending your data to the NAS or cloud.
- Make sure the storage media is still working and doesn't have any bad blocks.
- Ensure you have all the passwords and encryption keys to quickly unpack your backups.



test

## Backup specialists to help you secure your data

At NovaBACKUP, we're dedicated to helping you find the right solution for your business needs. Every IT environment is different and has unique data requirements. Our goal is to meet your backup and recovery needs and to be an extension of your IT team for the long haul.

[Schedule a call](#) with one of our backup experts to discuss your backup needs and goals, and we'll help you find your perfect solution.



# ABOUT NOVABACKUP

For more than a decade, NovaBACKUP has been a trusted provider of flexible, all-inclusive data protection solutions for Managed Service Providers (MSPs) and professional offices worldwide. As industry leaders in Backup and Disaster Recovery, we bring extensive experience in helping specialized industries meet strict data protection goals.

At NovaBACKUP, our primary goal is to simplify and enhance data protection for our clients. More than just powerful backup technology, our team of backup experts is dedicated to providing unparalleled support. We take a people-first approach to backup, understanding that every unique environment requires a personalized approach to data protection.


With NovaBACKUP, our commitment to exceptional support ensures that you have a reliable partner in data protection. Learn more about NovaBACKUP and explore our comprehensive range of data protection solutions by visiting our website at [www.novabackup.com](http://www.novabackup.com).


[Schedule a call](#) with one of our backup experts today!





Sources:

- i Consoltech
- ii 2024 Data Breach Investigations Report – Verizon
- iii The State of Ransomware in Healthcare 2023 – Sophos (Aug 2023)
- iv The State of Ransomware 2023 – Sophos (May 2023)
- v Kaseya's 2022 Global Benchmark Survey Report
- vi The Global Healthcare Cybersecurity Study – Claroty (2023)

 NovaBACKUP  
29209 Canwood Street  
Agoura Hills, California  
91301

 Tel.: (805) 579-6700  
Fax: (805) 579-6710  
M-F 9am-5pm PT

 Email: [ols@novabackup.com](mailto:ols@novabackup.com)  
 [www.novabackup.com](http://www.novabackup.com)