STRATEGY GUIDE

NOVABACKUP

HOW TO BUILD A BETTER BACKUP STRATEGY

A guide to preventing data loss, and reducing downtime.

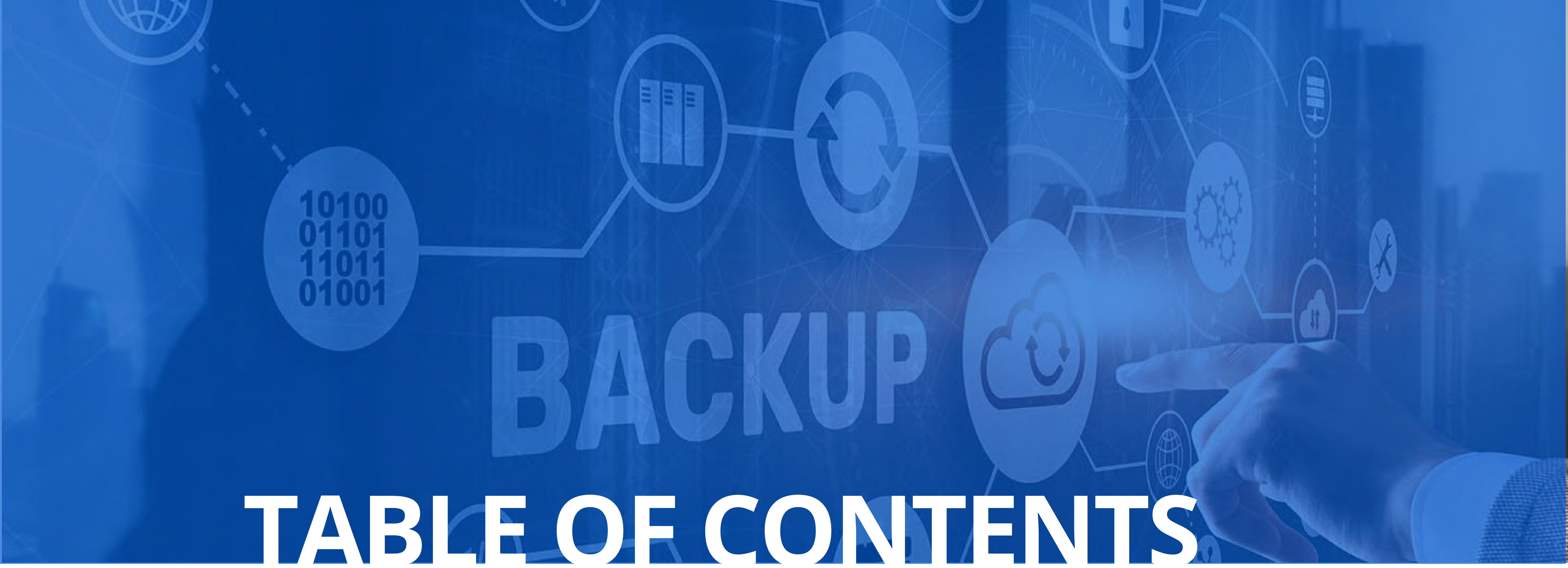


TABLE OF CONTENTS

INTRODUCTION

Most business-critical information is maintained primarily in digital form, often stored in multiple locations. The loss of specific information, or even an entire data set, has serious consequences for productivity and sometimes even an organization's survival.

And there are many ways an organization's data can be lost, for example:

External threats: The frequency of attacks, such as ransomware and other malicious software that holds all your data for ransom and denies access until payment is made for decryption, has raised global awareness. But let's not forget "non-cyber attacks," such as natural disasters, which can be just as devastating.

Internal threats: While cybercrime is the most headline-grabbing threat, there are more mundane causes of data loss - from the common mishaps caused by human error to software corruption, and hardware failure.

Remote systems: The modern business landscape includes remote and offsite employees. This presents system administrators with increased security challenges as they work to defend an expanded attack surface and a diverse range of roaming devices.

No matter the reason, data loss is a potentially business-ending event.

But what can be done about it?

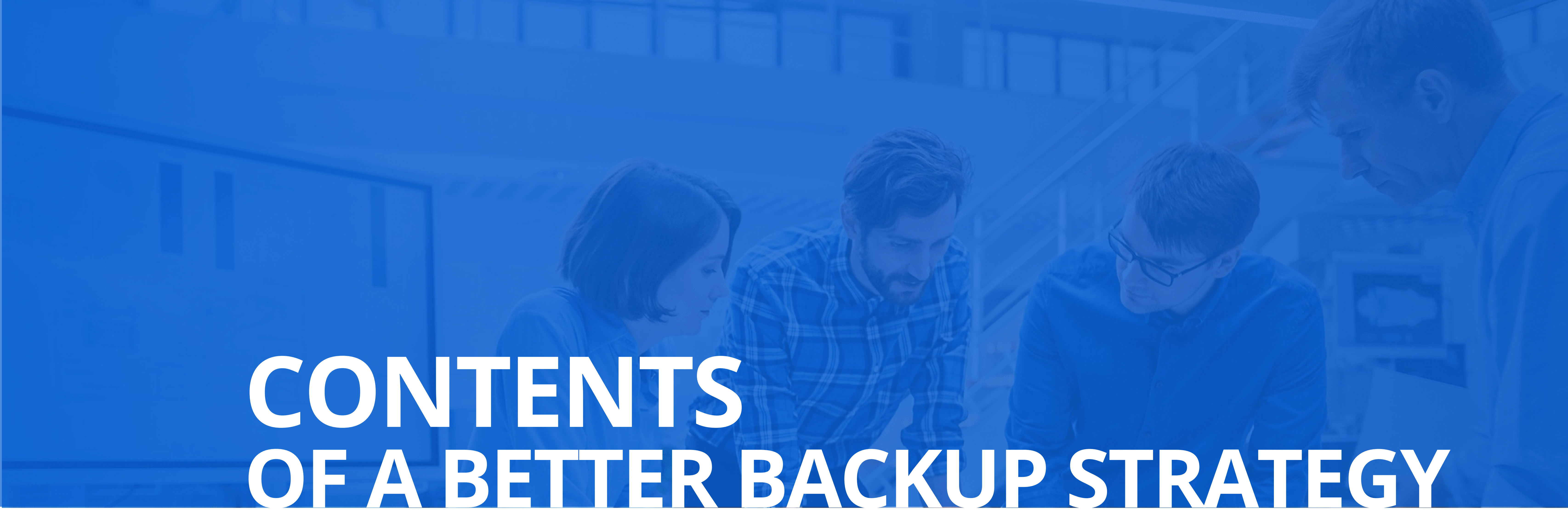
Preventive measures such as antivirus and vulnerability scanners, password management systems, and even security awareness training improve the ability to detect problems early and are an absolute must.

> "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 – The State of Ransomware 2023

However, when other methods fail, only a current and recoverable backup of all critical data and/or systems will enable a timely return to business as usual.

The good news is that a comprehensive data protection strategy and clear documentation of policies can not only ensure that your data can be recovered in the event of a disaster but can also satisfy a significant portion of your regulatory requirements when compliance auditors are at the door.

This document will guide you through the important environmental factors in building a comprehensive backup and recovery strategy that meets your business needs.



CONTENTS OF A BETTER BACKUP STRATEGY

To create the most effective backup strategy, you must first gather some important information that will help you lay the groundwork for planning and then consolidate it to create a strategy that is designed for your specific needs.

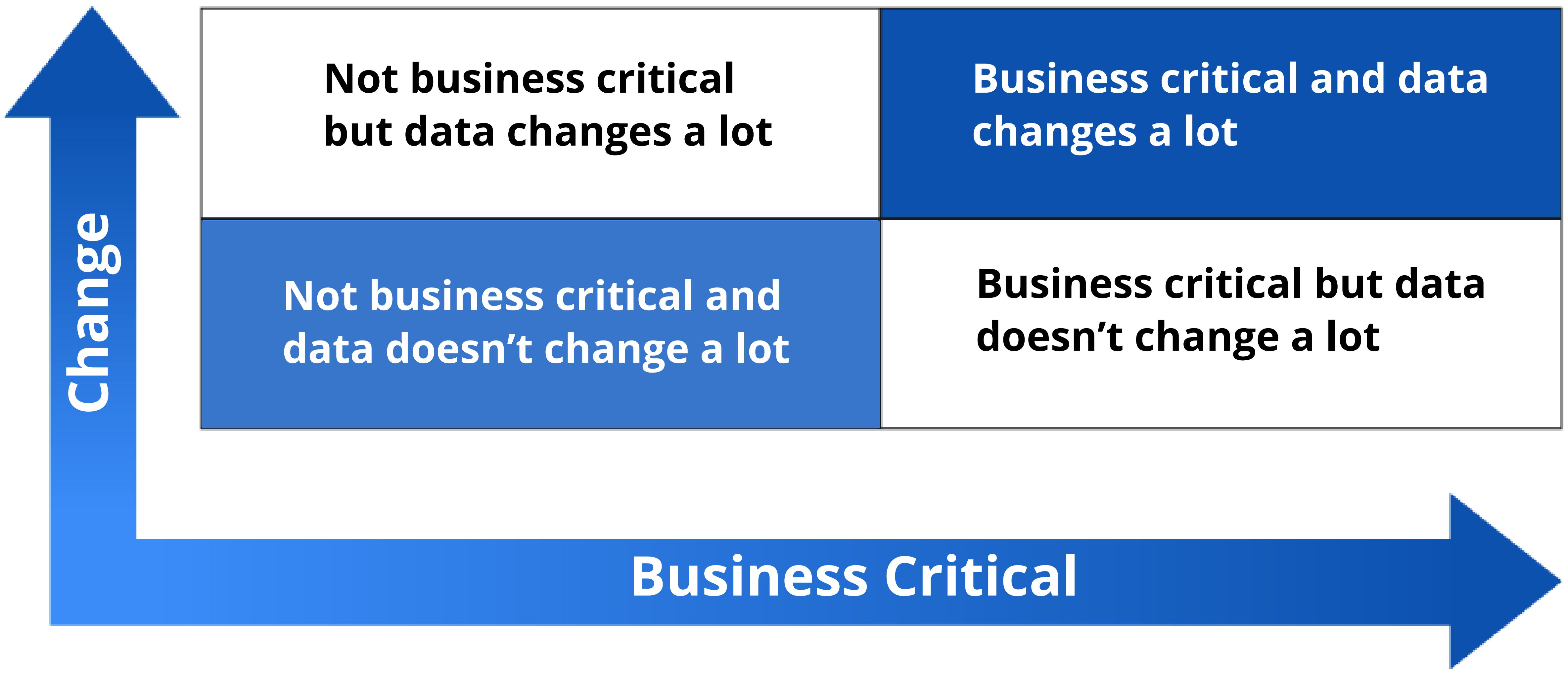
This can be done in the following four steps that we will explore together.

Know your data and setup | **Understand your recovery goals** | **Backup building blocks** | **Document everything**

In the end, you will have the kind of personalized strategy that inspires confidence, leverages the resources you have, and operates efficiently without disruption.

1 Know Your Data and Setup

Begin with an inventory of existing IT systems, applications, and data, as well as remote locations and at-home employees. This will help you identify key systems, data, and future needs. You can use the following classification to categorize business data as you prepare to define your backup strategy.



Not business critical but data changes a lot	**Business critical and data changes a lot**
Not business critical and data doesn't change a lot	**Business critical but data doesn't change a lot**

To analyze which classification your data and systems might fall into, consider the following:

Data dependencies: The company is most dependent on the data that could lead to the greatest loss - that is, the essential data without which the business cannot function. Consider how financial and customer data interact and affect decision-making. Contractual obligations and regulatory requirements must also be taken into account.

Legal Requirements: The demands of the latest laws and privacy regulations add an entirely different set of requirements to your own personal needs. Regulations such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) outline requirements for organizations that collect personal information.

Other standards, such as the Health Insurance Portability and Accountability Act (HIPAA) or the Payment Card Industry Data Security Standard (PCI DSS), define that ALL companies that accept, process, store, or transmit personal information must maintain a secure environment.

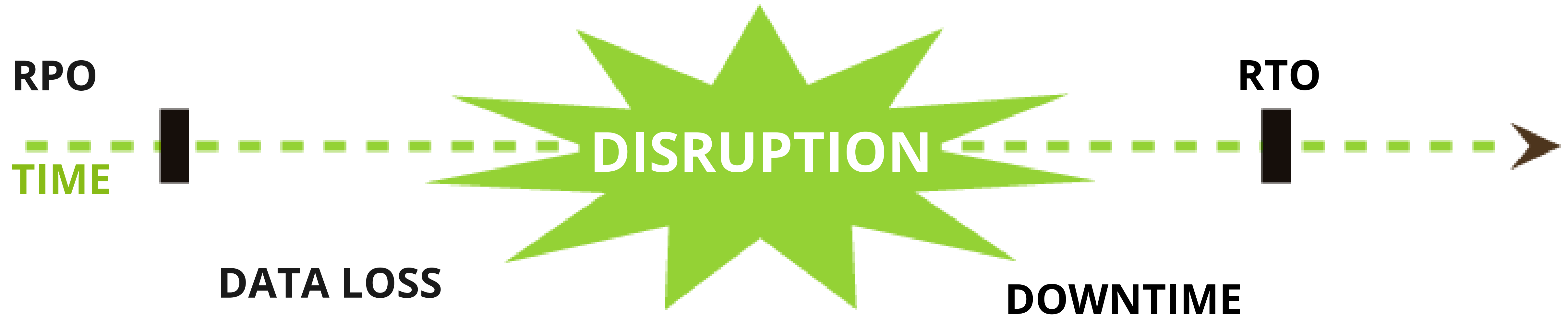
QUICK TIPS

A future-proof backup strategy should include short- and medium-term planning, not just the current state. This will also help you avoid unnecessary follow-up costs.

Retention Periods: Every organization is obliged to keep business records for a certain period of time, depending on location and industry. This often ranges from six to ten years. Classifying your data into critical, operational, business, and personal categories will help you later determine its retention period - or how long backup data is kept before unnecessary data is purged. If you are considering long-term storage of large amounts of data, additional archival technologies may be required.

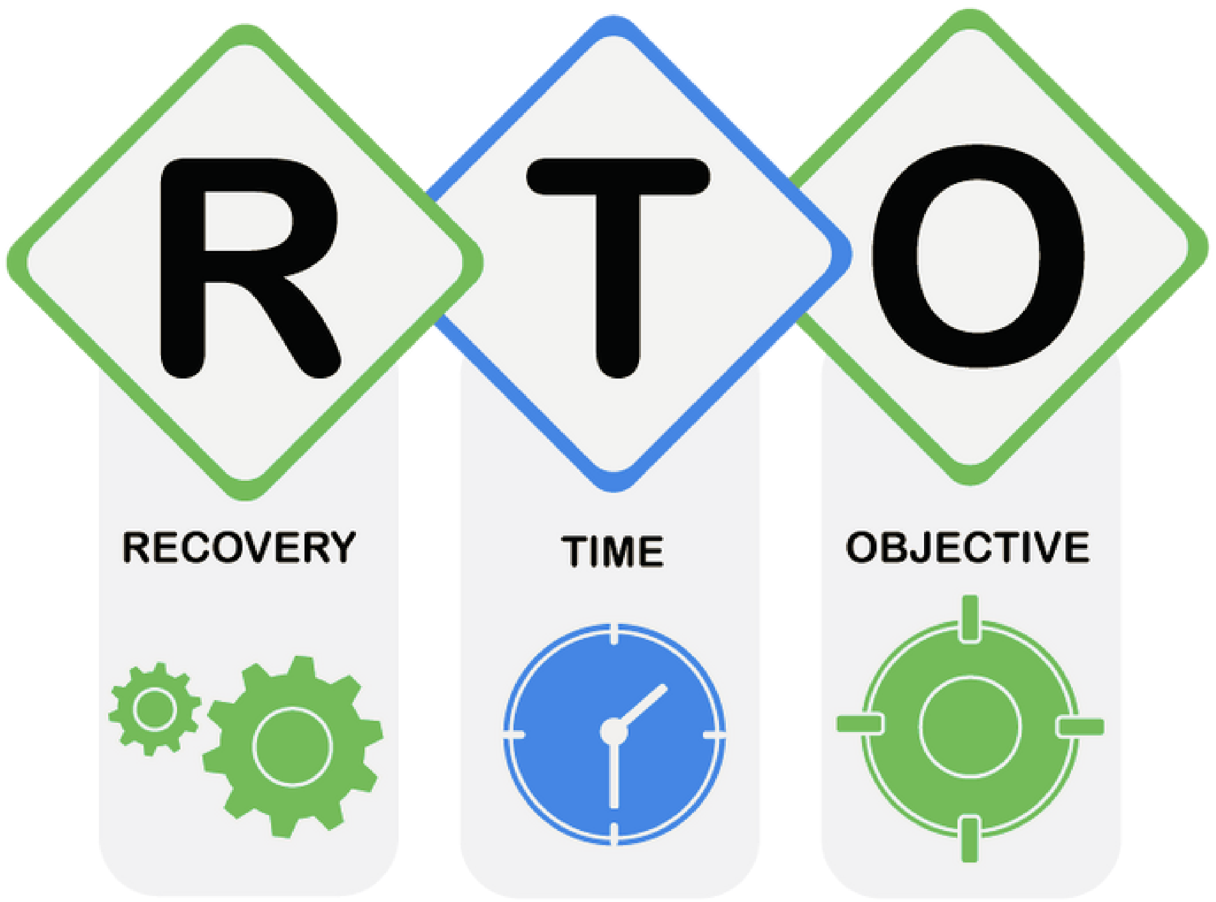
2 Understand Your Recovery Goals

Understanding what kind of data you have, what data is critical to your business, and what data may be less critical 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. This is defined by two metrics: Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Let us take a closer look at these two important metrics for your backup - and therefore recovery - strategy.



When should your last successful backup have completed?

How soon must you restore and resume operations?



RTO (Recovery Time Objective)

"The RTO is the maximum tolerable length of a period that a computer, IT system, network, or application may remain out of operation."

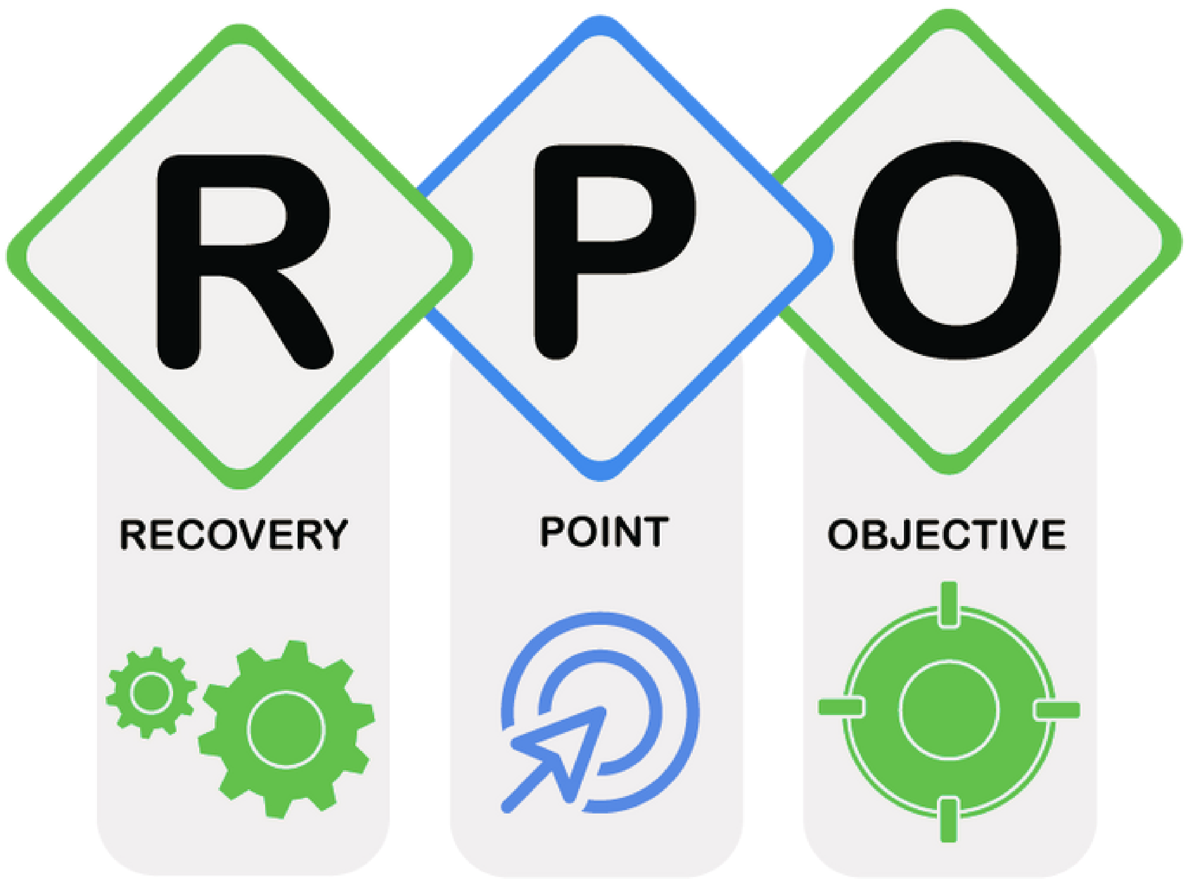
What is the maximum amount of downtime which your organization can tolerate before the disruption seriously impacts operations and revenue? How long should your restore take to make the needed data available? Different data types will of course have different availability requirements. And for example, higher availability requirements will impact the backups, dictating a smaller (or even continuous) backup interval. Your answer may be that certain functions or systems are more important than others, therefore understanding RTO helps you to build prioritization into your backup strategy.

Consider onsite or offsite backup locations

A backup of the business-critical data held outside of the local premises, and therefore separated from the production environment, is a must for most, if not all, industries. Experts recommend that you at least follow the 3-2-1 backup rule (backup in at least 3 locations, on at least 2 different storage media, 1 of which is offsite).

But to keep your RTO in mind, you need to understand your bandwidth limitations, which can directly impact your backup strategy. Bandwidth constraints between devices can not only impact network performance when large backups are performed during production hours, but can also cause unnecessary downtime as the organization waits for a restore to complete.

Tip: Researching the maximum bandwidth of removable drives, network connections, and cloud connections can help you estimate recovery times.



RPO (Recovery Point Objective)

"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."

We are talking about the point in time that your backup solution must be able to recover to in order to meet your business needs. For example, if your RPO is two hours, you need to be able to recover data that was created no more than two hours before the data loss event. Understanding this metric will help you think about how your data is structured and how often it needs to be backed up.

Consider your backup window

Backups should be scheduled to avoid any performance impact on your infrastructure. For most organizations, evenings are the most common off-peak hours of availability for backups to commence. Companies operating 24/7 must adapt their production processes to accommodate the backup window, and to load the production systems as little as possible.

In order to keep your RPO short, those backup windows shouldn't be too far apart. Your RPO will help define the intervals between backups. Typically, business-critical data is backed up once a day or more. It is often advisable to increase the backup interval. For example, it makes sense to back up an SQL database several times a day, because if you need to recover from a disaster, the only way to reconstruct the missing data is from the most recent backup.

Determining your Recovery Time Objective (RTO) and Recovery Point Objective (RPO) means understanding your organizations requirements to perform necessary business functions. Identify your critical systems and applications and define (in minutes or hours) how much downtime is acceptable for each component.

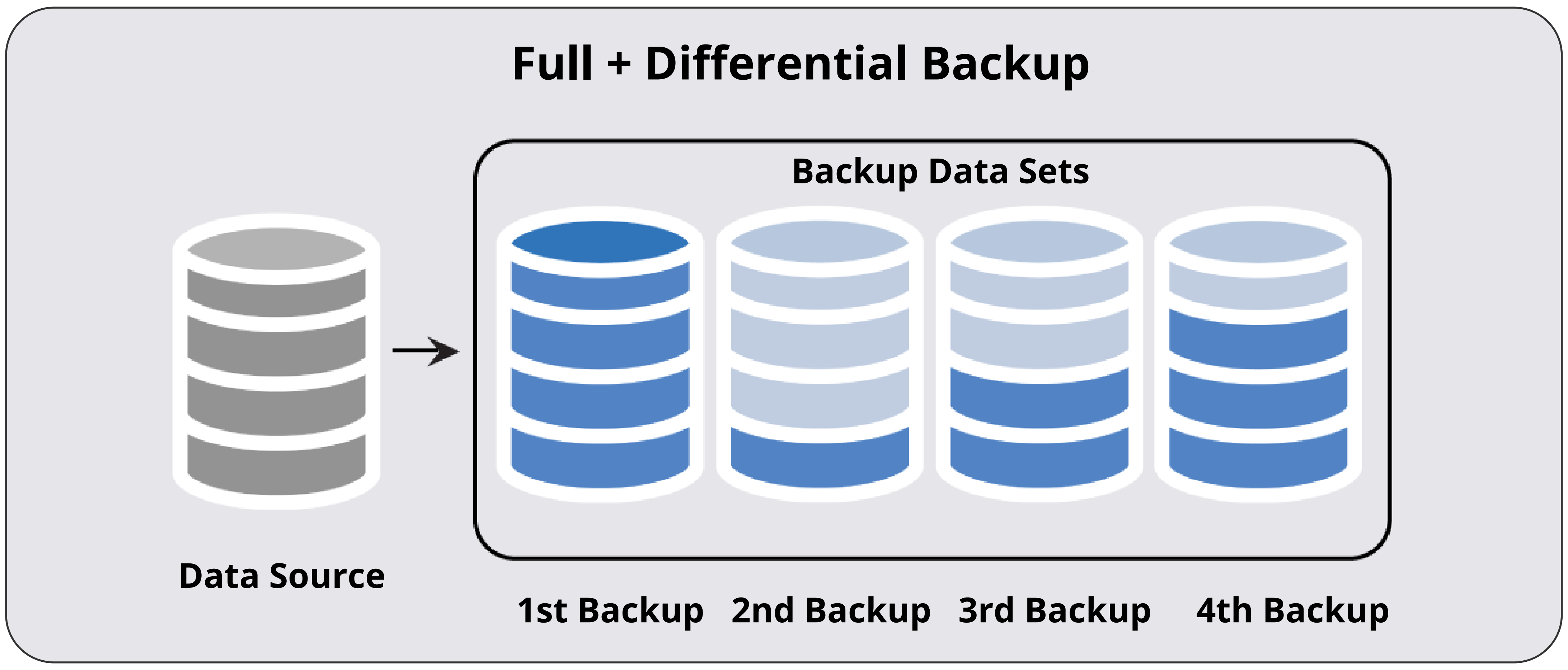
3 Backup Building Blocks

Every backup solution offers different ways to perform your backup and keep your data safe. Over the years, these solutions have added new and flashy features that promise to keep your data safer. But for probably more than 90% of organizations, the familiar and proven backup methods are all that's needed to ensure a fast recovery.

The Backup Basics

Full Backup: Each time the backup is run, all selected data is saved. This type of backup is the basis for all file, application, and system backups.

Differential Backup: Only data that has changed or that has been added since the last full backup will be saved. When performing a restore, both the full and the most recent differential backup of the selected restore point are required.



Incremental Backup: Only data is saved that has changed or has been newly added since the last incremental backup. These backups are often smaller and more frequent than differential backups. A restore requires the full backup and all incremental backups to the selected recovery point.

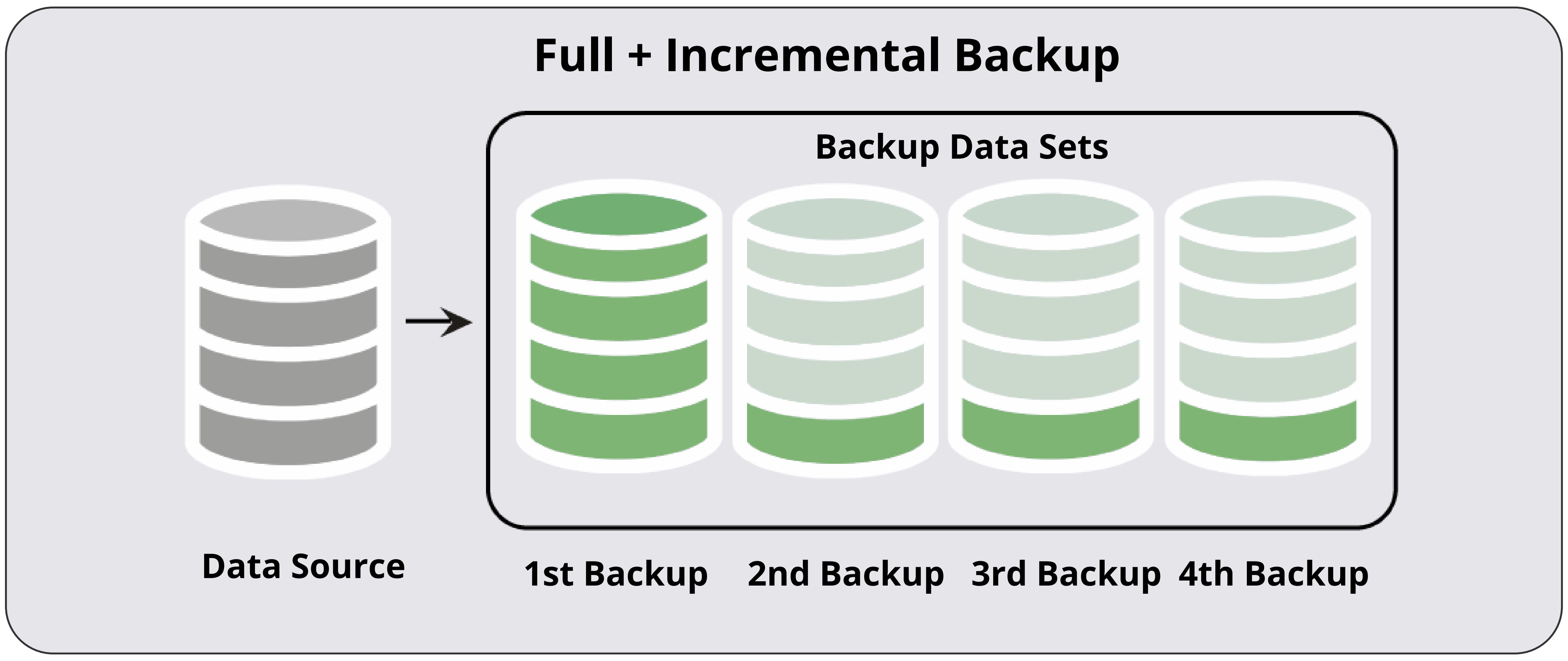


Image Backup

System Image / Disaster Recovery Backup: All system data, including file system, applications, and operating system is backed up to a single image, which is a special format that may also contain system specific configuration data. These images can be virtual hard disks (VHD/ VHDx) which may be mounted as virtual machines. These backups are often conducted periodically in addition to regular file backups.

Other Options

Continuous Backup: Some software or cloud services may offer continuous backup as an option where all new or changed data is immediately secured. Many SaaS backup solutions that backup to the cloud, i.e., for service such as Microsoft 365, now include this capability.

Additional features for consideration:

Encryption method: An algorithm or technology (such as AES 256) that allows you to encrypt your data. This is especially important for data stored offsite.

Compression: Software that compresses the data stored on the backup media can save storage space and time (because less data needs to be written).

Open file backup: Files and applications that are open are backed up using Volume Snapshot Service (VSS).

Scripting: The ability to run pre- and post-backup scripts gives system administrators a level of flexibility and customization to perform maintenance tasks.

BACKUP PLAN

Finally, you are ready to map out your backup plan. Combine your documented requirements with the typical features of a backup solution to create a comprehensive backup strategy for each of the data classifications from the **Know Your Data and Setup** chapter.

The exact cadence of your backup jobs depends on the industry you are in. For a highly regulated industry such as Healthcare, you would want to increase the number of daily and weekly jobs (if your bandwidth can handle it) to reduce your RPO. But if you run, for example, a small store, you may not need as many. Therefore, the following examples are intended to give you a few options on how to approach your exact backup schedule and strategy.

Business-Critical Data that Changes Frequently

For the data that is essential to your business, a good suggestion would be to run:

1 One full backup per week, ideally on the weekend, and keep a month's worth of these full backups.

5 Five differential backups per week, as these will shorten your RTO, which allows you to recover quickly in the event of a data loss.

1 One Image backup per week for the recoverability of an entire system at once with a monthly retention.

The full and differential backups should be sent to local storage, such as a NAS, for rapid recovery of individual files (RTO). Adding cloud storage for offsite backup enables recovery from anywhere. This is especially important for organizations with remote and/or home employees. Your image backup is best stored on a local device for quick access, as well as an additional removable media that is taken to a safe somewhere outside the office.

Non-Business-Critical Data that Rarely Changes

For the data that is still needed but wouldn't ruin your business if it would be gone, you could setup your backup jobs as followed:

1 **One full backup**

once a month, with a 4-6 month retention schedule.

1 **One differential backup**

run once per week, with a quarterly retention schedule.

1 **One Image backup**

every 6 months with a yearly retention schedule.

If your bandwidth allows, all files and applications could be stored in a cloud for long-term storage. Since there probably won't be a need for a quick rollback and not many changes will be made, the company would be fine if the restore took a few days.

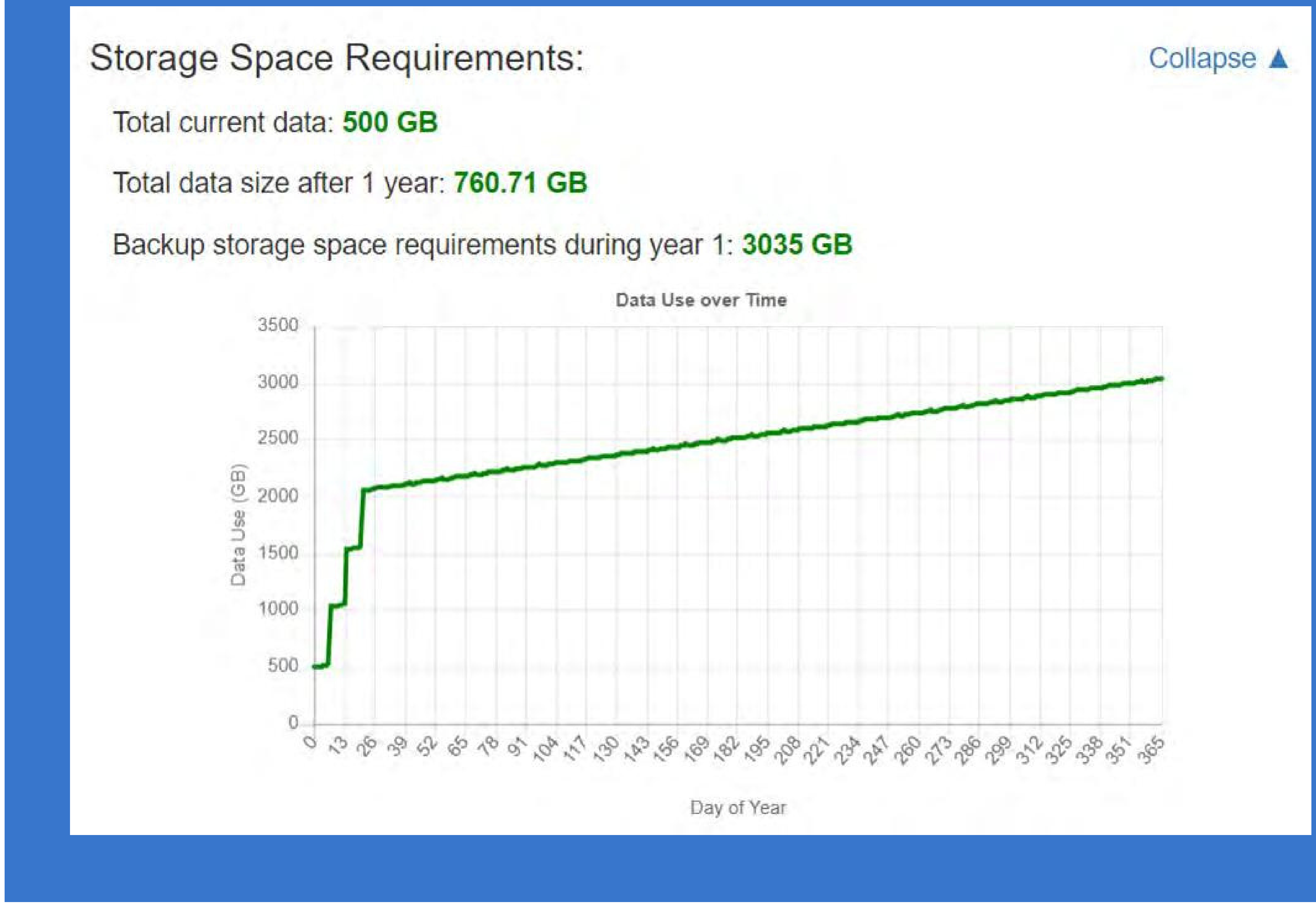
STORAGE EXAMPLE

A Note Regarding the Amount of Data Storage Required

For a well-rounded strategy, it is recommended that you use a combination of backup methods that keep your data in multiple locations. Before choosing which methods to include, it is important to consider the amount of data that will be backed up so that you can determine the size of your backup storage. And not just for the first backup, but for all the backups you perform on an ongoing basis as part of your data retention cycle.

Here is an example of a file server with a current data set of 500GB that plans to back up its data on a weekly full and daily differential schedule. To estimate how much additional data will be generated over a given period of time, it may be useful to use a calculation tool such as:

www.BackupCalculator.com



Storage Space Requirements:

Total current data: **500 GB**

Total data size after 1 year: **760.71 GB**

Backup storage space requirements during year 1: **3035 GB**

Current Data Per Server: 500GB

Existing data changing per/week: 5GB

New data added per/week: 5GB

Using Backup Compression: No

4 Document Everything

The ability to quickly recover files and systems in the event of a data loss depends not only on a functioning backup, but also on well-documented processes so that everyone knows what to do, where to find everything, in what order to restore, and so on. It's also important to clearly define processes so that information is preserved for your own team, or perhaps a successor or outside party who may take over your backup responsibilities.

Document Your Backup Plan

First, document the backup plan you created based on the previous paragraph.

- What is backed up, to where, and when
- Data retention rules (for example, for legal requirements, accounting rules, etc.)
- Who is responsible for what, i.e., who takes the USB drive and puts it in the safe?
- Who is going to check the backup regularly?

And so on...

Define a Schedule

Your schedule should define the following:

- How often will backups be reviewed?
- How often are new data, applications, and systems added to the backup schedule?

Backup Plan	Restore Plan	Testing
What data is secured and where?	Restore Objectives (RTO & RPO)	Testing Schedule / Frequency
Backup Roles & Responsibilities	Restore / Recovery Scenarios	How is success defined?
Storage Sites / Devices / Rules	Define File Restore Procedure	What did you restore?
Media Management Details	Disaster Recovery Procedure	From where?
Monitoring & Reporting Details	Special Scripts / Tools to Use	How long did it take?
Data Retention Policy	Restore Training & Awareness	
Backup software contact and contract information	Restore Roles & Responsibilities	
License keys, Encryption keys, etc.	Process for Updating This Restore Documentation	

VERY IMPORTANT

Test your backups regularly! Nothing is worse than a corrupted or otherwise inoperable backup that cannot be restored. Also, the recovery plan should not just be created once, but should be updated with the latest changes as part of your regular recovery testing.

Transfer Protocol Documentation

If you are an IT Service Provider or run an IT department for a large organization, you will want to create and document a transfer protocol for handing over backup and restore responsibilities to another party.

QUICK TIPS

Tip for IT Service Providers

In case you have to hand off a customer to another Service Provider, the relevant company should sign the transfer protocol as a means of protecting your liability.

CONCLUSION

A backup is only valuable if it is restorable, reliable in disaster scenarios, and meets recovery objectives. That's why secure, reliable backup begins not with choosing a storage location, but with planning a backup strategy that works for your unique environment.

By conducting a comprehensive assessment of your environment (including an analysis of data files, hardware, software storage devices, and applications), you can easily identify the most critical systems and potential vulnerabilities when developing your strategy. And by understanding business and regulatory requirements, as well as the limitations and vulnerabilities of the environment, you can create an effective backup strategy that prevents data loss and reduces downtime.

To avoid falling behind, it is also key to remain adaptable and make changes to the strategy over time. Therefore, it is important to consider various common (and less common) threat scenarios, schedule regular recovery tests, and reevaluate recovery requirements as they relate to business needs.

When a backup strategy is carefully planned, supported by flexible technology, and properly managed, the only thing separating organizations from returning to business after a data loss event is the time it takes to complete a recovery.

"NovaBACKUP has proven to be a superior product and their customer support is consistently the best and most experienced that I've dealt with from any vendor."

Lori Simmons
Support Services Engineer, Mytec Services

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.

Schedule a call with one of our backup experts today!

Our Service Promise

We promise to treat the protection and safety of your data like we do our own. Our job it to make data protection as simple and reliable as possible. You can count on us to provide professional, knowledgeable support that meets your data protection needs. Feel free to reach out to our team if you need assistance with your backup and recovery needs.

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

www.novabackup.com