Backblaze

Server Backup

A Comprehensive Guide to Protecting
The Data on Your Servers

Contents

Overview

In business, data loss is unavoidable unless you have good server backups. Files get deleted accidentally, servers crash, computers fail, and employees make mistakes.

However, those aren't the only dangers. You could also lose your company data in a natural disaster or cybersecurity attack. Ransomware is a serious concern for small to medium-sized businesses (SMBs) as well as large enterprises. Smart companies plan ahead to avoid data loss.

This ebook will discuss:

- Why it's critical to keep your data backed up.
- Server backup basics.
- The different types of server backup.
- How to create a solid backup strategy for your company.
- How to create a recovery plan if you ever need to use your server backups.

Read on to learn everything you ever wanted to know about server backups.

Why Backup?

If you're in charge of backups for your company, you know backing up your server is a critical task to protect important business data from data disasters like fires, floods, and ransomware attacks. Data disasters can easily cost a business thousands of dollars in recovery expenses. Did you know that roughly 40% of SMBs will be hacked within a year, and 61% of all SMBs have already been attacked? Additionally, statistics show that 93% of companies that lost data for more than 10 days were forced into bankruptcy within a year. More than half of them filed immediately, and most shut down.

61%

of SMBs have suffered a ransomware attack.

40%

of SMBs will be hacked within a year.

93%

of companies that lost data for 10+ days filed for bankruptcy.

As an IT leader or business owner, establishing a solid, working backup strategy is one of the most important tasks on your plate. Server backups are an essential part of a good security and disaster recovery stance. When company data is vulnerable to fire, theft, natural disasters, hardware failure, and cybercrime, simply put, backups are an essential prevention tool.

What is Server Backup?

A server is a virtual or physical device that performs a function to support other computers and users. Sometimes servers are dedicated machines used for a single purpose, and sometimes they serve multiple functions. Other computers or devices that connect to the server are called “clients.” Typically, clients use special software to communicate with the server and reply to requests. This communication is referred to as the server/client model.

A server backup is a copy of the data on a given server. This could include files, folders, configuration files, and applications stored on it. The backup copy can be used to restore the data on a given server in the event it’s needed.

Common Uses for Servers

- **Web Server:** Hosts web pages and online applications.
- **Email Server:** Manages email for a company.
- **Database Server:** Hosts various databases and controls access.
- **Application Server:** Allows users to share applications.
- **File Server:** Used to host files shared on a network.
- **DNS Server:** Used to decode web addresses and deliver the user to the correct address.
- **FTP Server:** Used specifically for hosting files for shared use.
- **Proxy Server:** Adds a layer of security between client and server.

Types of Servers

Within the realm of servers, there are many different types for virtually any purpose and environment. However, the primary function of most servers is data storage and processing. Some examples of servers include:

Physical Servers

These are hardware devices (usually computers) that connect users, share resources, and control access.

Cloud Servers

Cloud servers exist in a virtual online environment, and you can access them through web portals, applications, and specialized software.

Virtual Servers

Using special software (called a hypervisor), you can set up multiple virtual servers on one physical machine. Each server acts like a physical server while the hypervisor manages memory and allocates other system resources as needed.

NAS Devices

Network attached storage (NAS) devices store data and are accessed directly through the network without first connecting to a computer. These hardware devices contain a storage drive, processor, and operating system (OS) and can be accessed remotely.

SAN Servers

Although not technically a server, a storage area network (SAN) connects multiple storage devices to multiple servers expanding the network and controlling connections.

Hybrid Servers

Hybrids are servers combining physical servers and virtual servers. They offer the speed and efficiency of a physical server combined with the flexibility of cloud-hosted resources.

Servers also run on many operating systems such as Windows, Linux, Mac, Apache, Unix, NetWare, and FreeBSD. The OS handles access control, user connections, memory allocation, and network functions. Each OS offers varying degrees of control, security, flexibility, and scalability.

Regardless of what types of servers you have, backups are essential to protecting yourself from loss.

Where to Back Up Servers

You have options for backing up data, and the methods vary. In this section, we'll explain some of the fundamentals of backing up servers, including:

- Backup destinations
- On-premises vs. cloud-only vs. hybrid backups
- Creating a backup strategy

But first, let's talk about terminology. We'll define the following terms to help you understand all of the moving parts of a server backup strategy:

- Backup vs. Archive
- Backup vs. Sync

Backup vs. Archive

Backing up is copying your data, whereas an archive is a historical copy that you keep for retention purposes, often for long periods. Archives are often used to save old, inactive data for compliance reasons.

An example of a backup vs. an archive is when your mobile phone backs up to the cloud, and if you factory reset the phone, you can restore all your applications, settings, and data from the backup copy. An example of an archive is a tape backup of old HR files that have long since been deleted from the server.

Backup vs. Sync

Sometimes people confuse the word backup with sync. They are not the same thing. A backup is a copy of your data you can use to restore lost files. Syncing is the automatic updating and merging of two file sources. Cloud computing often uses syncing to keep files in one location identical to files in another.

To prevent data loss, backups are the process to use. Syncing overwrites files with the latest version; a backup can restore back to a single point in time, so you don't lose anything valuable.

Backup Destinations

When selecting a backup destination, you have many mediums to choose from. There are pros and cons for each type. Some popular backup destinations and their pros and cons are outlined below.

On-premises Solutions

Air-gapped tape backups provide excellent protection from ransomware and hackers. For this reason, the use of tapes has increased as ransomware proliferates, but it's not without drawbacks—namely, cost and maintenance.

LTO/Tape

Linear Tape-Open (LTO) backup is the process of copying data from primary storage to a tape cartridge. If the hard disk crashes, the tapes will still hold a copy of the data.

Pros

- High capacity.
- Tapes can last a long time.
- Provides a physical air gap between backups and the network to protect against threats like ransomware.

Cons

- Up-front capital expense.
- Tape drives must be monitored and maintained to ensure they are functioning properly.
- Tapes take up considerable physical space.
- Tape is susceptible to degradation over time.
- The process of backing up to tape can be time consuming for high volumes of data.

NAS

Network attached storage enables multiple users and devices to store and back up data through a secure server. Anyone connected to a local area network can access the storage through a browser-based utility. It’s essentially an extra network strictly for storing data that users can access via its attached network device.

Pros

- Faster to restore files and access backups than tape backups.
- More digitally intuitive and straightforward to navigate.
- Comes with built-in backup and sync features.
- Can connect and back up multiple computers and endpoints via the network.

Cons

- Requires physical maintenance and periodic drive replacement.
- Each appliance has a limited storage capacity.
- Because it’s connected to your network, it is also vulnerable to network attacks.

Including these specific backup destinations, there are some pros to using on-premises backup solutions in general. For example, you might still be able to access backup files without an internet connection using on-premises solutions. And you can expect a fast restore if you have large amounts of data to recover.

However, all on-premises backup storage solutions are vulnerable to natural disasters, fires, and water damage despite your best efforts. While some methods like tape are naturally air gapped, solutions like NAS are not. Even with a layered approach to data protection, NAS backup leaves a business susceptible to attacks.

To summarize, we've pulled various on-premises solutions discussed previously plus a few others and their pros and cons into the following table.

On-premises Solutions

Destination	Pros	Cons
LTO/Tape	High capacity, can be kept for years, air gapped, low OpEx ongoing.	High initial setup costs, limited scalability, potential media corruption over time, space hungry, time consuming to manage.
NAS	Always available on the network, fast access, easier to navigate than tape, small size, backup and sync built in, can connect and backup multiple endpoints.	Requires physical maintenance and drive replacement, vulnerable to on-premises threats, non-scalable due to limits.
Local Servers	Highly local, fast access.	Less secure due to network connectivity and localized data storage, capacity limited, vulnerable to attacks.
Network or SAN Storage	High speed, view connected drives as local, good security, failover protection, excellent disk utilization, high-end disaster recovery options.	Can be expensive, doesn't work with all types of servers, vulnerable to attacks on the network.
FTP	Excellent for large files, copy multiple files at once, can resume if the connection is lost, schedule backups and recover lost data.	No security, vendors vary widely, not all solutions include encryption, vulnerable to attacks.
External Media (USB, CD, Removable Hard Drives, Flash Drives, etc.)	Quick, easy, affordable.	Fragile if dropped, crushed, or exposed to magnets; very small capacity.

Cloud Solutions

Many organizations choose a cloud-based server for backup storage instead of or in addition to an on-premises solution as they continue to integrate modern digital tools. While an on-premises system refers to data hardware and physical storage solutions, cloud storage lives "in the cloud."

A cloud server is a virtual server that is hosted in a cloud provider's data center. "The cloud" refers to the virtual servers users access through web browsers, APIs, CLIs, and SaaS applications and the databases that run on the servers themselves.

Because cloud providers manage the server's physical location and hardware, organizations aren't responsible for managing costly data centers. Even small businesses that can't afford internal infrastructure can outsource data management, backup, and cloud storage from providers.

Pros

- Highly scalable since companies can add as much storage as needed without ever running out of space.
- Typically far less expensive than on-premises backup solutions because there's no need to pay for dedicated IT staff, hardware upgrades or repair, or the space and electricity needed to run an on-premises system.
- Builds resilience from natural disasters with off-site storage.
- Virtual air-gapped protection may be available.
- Fast recovery times in most cases.

Cons

- Cloud storage fees can add up depending on the amount of storage your organization requires and the company you choose. Things like egress fees, minimum retention policies, and complicated pricing tiers can cause headaches later, so much so that there are companies dedicated to helping you decipher your Amazon Web Services bill, for example.
- Can require high bandwidth for initial deployment, however effective migration solutions from various cloud vendors are making deployment and migrations easier.
- Since backups can be accessed via API, they can be vulnerable to attacks without a feature like Object Lock.

When it comes to cloud backup solutions, there are two main types: all-in-one and integrated solutions. Let's talk about the differences between the two:

All-in-one Tools

All-in-one tools are cloud backup solutions that include both the backup application software and the cloud storage where backups will be stored. Instead of purchasing multiple products and deploying them separately, all-in-one tools allow users to deploy cloud storage with backup features together.

Depending on the tool you choose, you may be able to back up an unlimited number of devices, or you may have limits. However, most of these all-in-one solutions are expensive and can be complex to learn, or, conversely, they are lacking important functionality you might need. All those bells and whistles often come at a price—a steep learning curve.

Pros

- No need for additional software.
- Simple, out-of-the-box deployment.
- Creates a seamless native environment.

Cons

- Some all-in-one tools sacrifice granularity for convenience, meaning they may not fit every use case.
- They can be more costly than pairing cloud storage with backup software.

Integrated Solutions

Integrated solutions are pure cloud storage providers that offer cloud storage infrastructure without built-in backup software. An integrated solution means that organizations have to bring their own backup application that integrates with their chosen cloud provider.

Integrated solutions however can combine the best of both worlds. They allow users to choose the software they want with the features they need paired with fast, reliable cloud storage. Cloud storage is scalable, so you will never run out of space as your business grows. Using your chosen software, it's fast and easy to restore your files.

Although it may seem counterintuitive, it's often more affordable to use two integrated solutions—backup software plus cloud storage—versus an all-in-one tool. Pure cloud storage providers like Backblaze often integrate with many popular software options. For example, Backblaze works seamlessly with:

- MSP360
- Veeam
- Catalogic
- Veritas
- And many more

Pros

- Mix and match your cloud storage and backup vendors to create a tailored server backup solution.
- More control over your environment.
- More control over your spending.

Cons

- Requires identifying and contracting with more than one provider.
- Can require more technical expertise than with an all-in-one solution, but many cloud storage providers and backup software providers have engineered existing integrations to make onboarding seamless.

On-premises vs. Cloud-only vs. Hybrid Server Backups

Now that you're aware of the different destinations where you can store server backups, the next step is deciding which you'll use. A big part of setting up your backup strategy is where and how you'll store server backups: on-premises, in the cloud, or in some mix of the two.

It can be tough to choose between cloud storage vs. on-premises storage for backing up critical data. Many companies choose a hybrid cloud backup solution that involves both on-premises and cloud storage backup processes. Cloud backup providers often work with companies that want to build a hybrid cloud environment to run business applications and store data backups in case of a cyber-attack, natural disaster, or hardware failure.

If you're stuck between choosing an on-premises or cloud storage backup solution, a hybrid cloud option might be a good fit. And if you're confused about how to set up a hybrid cloud strategy for backups, you're not alone. There are as many ways to approach it as there are companies backing up to the cloud.

This section explores the benefits and drawbacks of on-premises, cloud-only, and hybrid server backups.

Here are some examples of different server backup strategies according to where your data is located:

On-premises Backups

On-premises backup, also known as a local backup, is a process of backing up your system, applications, and other data to a local device. As explained in the previous section, tape, servers, and NAS are examples of common local backup solutions.

Pros

- A major benefit to using a local backup strategy is that organizations have fast access to data backups in case of emergencies. Backing up to NAS can also be faster locally depending on the size of your data set.

Cons

- Maintaining on-premises hardware can be costly, but more important, your data is at a higher risk of loss from local disasters like floods, fires, or theft.

Cloud-only Backups

Cloud-only backup strategies are becoming more commonplace as startups take a cloud-native approach and existing companies undergo digital transformations. A cloud-only backup strategy involves eliminating local, on-premises backups and sending files and databases to the cloud vendor for storage.

Pros

- With a cloud-only backup strategy, there is no need for on-site hardware, and backup and recovery can be initiated from any location. Cloud resources are inherently scalable, so the stress of budgeting for and provisioning hardware is gone.

Cons

- A cloud-only strategy is susceptible to outages if your data is consolidated with one vendor, however this risk can be mitigated by diversifying vendors and regions within the same vendor. Similarly, if your network goes down, then you won’t have access to your data.

Hybrid Cloud Backups

When you hear the term hybrid when it comes to servers, you might initially think about a combination of on-premises and cloud data. That's typically what people think of when they imagine a hybrid cloud, but as mentioned earlier, a hybrid cloud is a combination of a public cloud and a private cloud. Today, private clouds can live off-premises, but for our purposes, we'll consider private clouds as being on-premises.

Private Cloud

Is dedicated to a single tenant. Private clouds are traditionally thought of as on-premises. Your company provisions and maintains the infrastructure needed to run the cloud at your office. Now, though, you can rent rackspace or even private, dedicated servers in a data center, so a private cloud can be off-premises, but it's still dedicated only to your company.

Public Cloud

A data center that's used by many different tenants and maintained by a third-party company. Tenants share the same physical hardware, and their data is virtually separated so one tenant can't access another tenant's data.

As the cloud has become more secure, affordable, and accessible, more organizations are using a hybrid cloud strategy for their cloud computing needs, and server backups are particularly well suited to this strategy. It allows you to maintain existing on-premises infrastructure while taking advantage of the scalability, affordability, and geographic separation offered by the cloud. A hybrid server backup strategy is an easy way to accomplish a 3-2-1 backup strategy, generally considered the gold standard when it comes to backups.

Pros

- Hybrid cloud server backup strategies combine the best features of public and private clouds: You have fast access to your data locally while protecting your data from disaster by adding an off-site location to your backup strategy.

Cons

- Setting up and running a private cloud server can be very costly. Businesses also need to plan their backup strategy a bit more thoughtfully because they must decide what to keep in a public cloud versus a private cloud or on local storage.

It’s still a great idea to keep a local copy of your backup so you comply with a 3-2-1 backup strategy.

Refresher: What is the 3-2-1 Backup Strategy?

The 3-2-1 backup strategy is a tried and tested way to keep your data accessible, yet safe. It includes:

3 Keep three copies of any important file—one primary and two backups.

2 Keep the files on two different media types to protect against different types of hazards.

1 Store one copy off-site , preferably in a geographically distanced location like a public cloud provider’s data center.

A hybrid server backup strategy can be helpful for fulfilling this sage backup advice as it provides two backup locations, one in the private cloud and one in the public cloud.

To achieve a 3-2-1 compliant, cloud-only backup strategy, you could also utilize multiple cloud vendors or multiple regions with the same vendor to ensure redundancy. In the event of an outage, your data is stored safely in a separate cloud or a different cloud region and can easily be restored.

How Backblaze Can Help: Cloud Replication

With services like Backblaze Cloud Replication, companies can easily achieve a solid cloud-only server backup solution within the same cloud vendor’s infrastructure. Cloud Replication allows you to automatically store to different locations—across regions, across accounts, or in different buckets within the same account.

How to Choose Between Hybrid, Cloud-only, and On-prem

Choosing a backup arrangement that is right for you involves carefully evaluating your existing systems and your future goals. Can you get there with your current backup strategy? What if a ransomware or distributed denial of service attack affected your organization tomorrow? Decide what gaps need to be filled and take into consideration a few more crucial points:

- **Evaluate Your Vulnerabilities:** Is your location susceptible to a local data disaster? How often do you think you might need to access your backups? How quickly would you need them?
- **Price:** Various backup strategies will incur costs for hardware, service, expansions, and more. Carefully evaluate your organization's finances to decide on a budget. And keep in mind that monthly fees and service charges may go up over time as you add more storage or use enhanced backup tools.
- **Storage Capacity:** How much storage capacity do you have on-site? How much data does your business generate over a given period of time? Do you have IT personnel to manage on-premises systems?
- **Access to Hardware:** Provisioning a private cloud on-premises involves purchasing hardware. Increasing supply chain issues can slow down factories, so be mindful of shortages and increased delivery times.
- **Scalability:** As your organization grows, it's likely that your data backup needs will grow, too. If you're projecting growth, choose a data backup strategy that can keep up with rapidly expanding backup needs.

Structuring Hybrid Server Backup Strategies

Once you've decided a hybrid server backup strategy is right for you, there are many ways you can structure it. Here are just a few examples:

- Keep backups of active working files on-premises and move all archives to the cloud.
- Choose a cutover date if your business is ready to move mostly to the cloud going forward. All backups and archives prior to the cutover date could remain on-premises and everything after the cutover date gets stored in cloud storage.
- Store monthly full backups in local storage and keep more recent weekly full backups and incremental backups in cloud storage. This provides multiple access points for recovery.

As you're structuring your server backup strategy, consider any GDPR, HIPAA, or cybersecurity insurance requirements. Does it call for off-site, air-gapped backups? If so, you may want to move that data (like customer or patient records) to the cloud and keep other, non-regulated data local. Some industries, particularly government and heavily regulated industries, may require you to keep some data in a private cloud.

How to Back Up Servers:

Creating a Server Backup Strategy

By this point, you have a solid understanding of the different backup destinations you can choose from, and how you might want to structure your backup approach between them. Now, it's time to iron out some remaining details to complete your backup strategy, including:

- How often to back up.
- What kinds of backups to run and when.
- How long you should keep backups.
- How you will monitor your backups.

This section covers the above. Keep in mind, a solid backup strategy plan is the best way to protect your company against data loss. Again, you have options. As mentioned in the last section, the 3-2-1 strategy is the gold standard, but some companies are choosing options like a 3-2-1-1-0 option or even a 4-3-2 scheme.

What is a 3-2-1-1-0 Backup Strategy?

A 3-2-1-1-0 strategy stipulates that you:

- Maintain at least three copies of business data.
- Store data on at least two different types of storage media.
- Keep one copy of the backups in an off-site location.
- Keep one copy of the media offline or air gapped.
- Ensure all recoverability solutions have zero errors.

Whatis a 4-3-2 Backup Strategy?

The 4-3-2 rule stipulates that you keep:

- Four copies of your data.
- Data in three locations (on-prem with you, stored in a second off-site location, for example, at a secondary office or with a managed service provider (MSP), and stored with a cloud provider).
- Two locations for your data are off-site.

Before determining your strategy, you must consider what data you need to back up. For example, will you be backing up just servers or also workstations and dedicated servers, such as email servers, or SaaS data devices?

Another concern is how you will get your data into the cloud. You need to figure out which method will work best for you.

How Backblaze Can Help: Universal Data Migration

Migrating your data can seem like an insurmountable task. We launched our Universal Data Migration service to make migrating to Backblaze just as easy as it is to use Backblaze. You can migrate from virtually any source to Backblaze B2 Cloud Storage, and it's free to new customers who have 10TB of data or more to migrate with a one-year commitment.

How Often Should You Back Up Your Data?

Should you run full backups regularly? Or rely on incremental backups? The answer is that both have their place.

Specifically, there are four different types of backups that you need to consider:

- Full backups
- Incremental backups
- Synthetic full backups
- Differential backups

Full vs. Incremental vs. Synthetic Full vs. Differential Backups

The cadence of full versus incremental backups might look different for each organization, so it’s important to understand the difference. Choosing the right backup type also means maximizing efficiency, as simply performing a full backup of your data on a daily basis would take up too much bandwidth and storage, resulting in unnecessary extra costs.

Not sure what kind of backup you need to do? We explain the differences below.

Full Backups

A full backup is the very first backup you create of your data. You start with nothing—no backup—and then you make a complete copy of your data. It will probably take a while, because you're starting from nothing, making this your longest backup job.

Pros

- Full backups are the best option for recovery, because they contain all the files you need. Because your full backup is a clone of your data, it's very important to encrypt them. Don't forget this essential step!

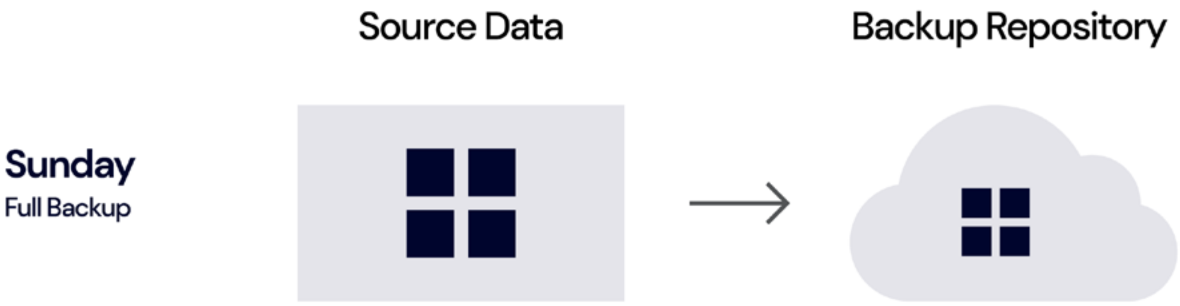
Cons

- You can see how it would be time-consuming to do a full backup each time. Additionally, you would likely need a lot of extra bandwidth and storage to be able to run a full backup everyday.

How Backblaze Can Help: Encryption

Backblaze B2 Cloud Storage stores the data you put in it. You can choose to upload only encrypted data or use a third-party integration to encrypt data before transmission to Backblaze B2. We also support server-side encryption using the 256-bit Advanced Encryption Standard, with multiple key management options.

Full Backup



You should think about how often to do your full backups, given that they are the safest recovery option but also the most time-consuming and expensive to complete. Some people do full backups daily; some do them weekly; and some complete them monthly, or even less often. It all depends on your backup strategy plan and how you balance your needs for data security vs. your resources, like time, funds, etc. For example, in the image above, this person has decided to do their full backup on a Sunday. Their source data is copied exactly as is into the cloud. This provides them the security of a 100% true copy of their data.

Incremental Backups

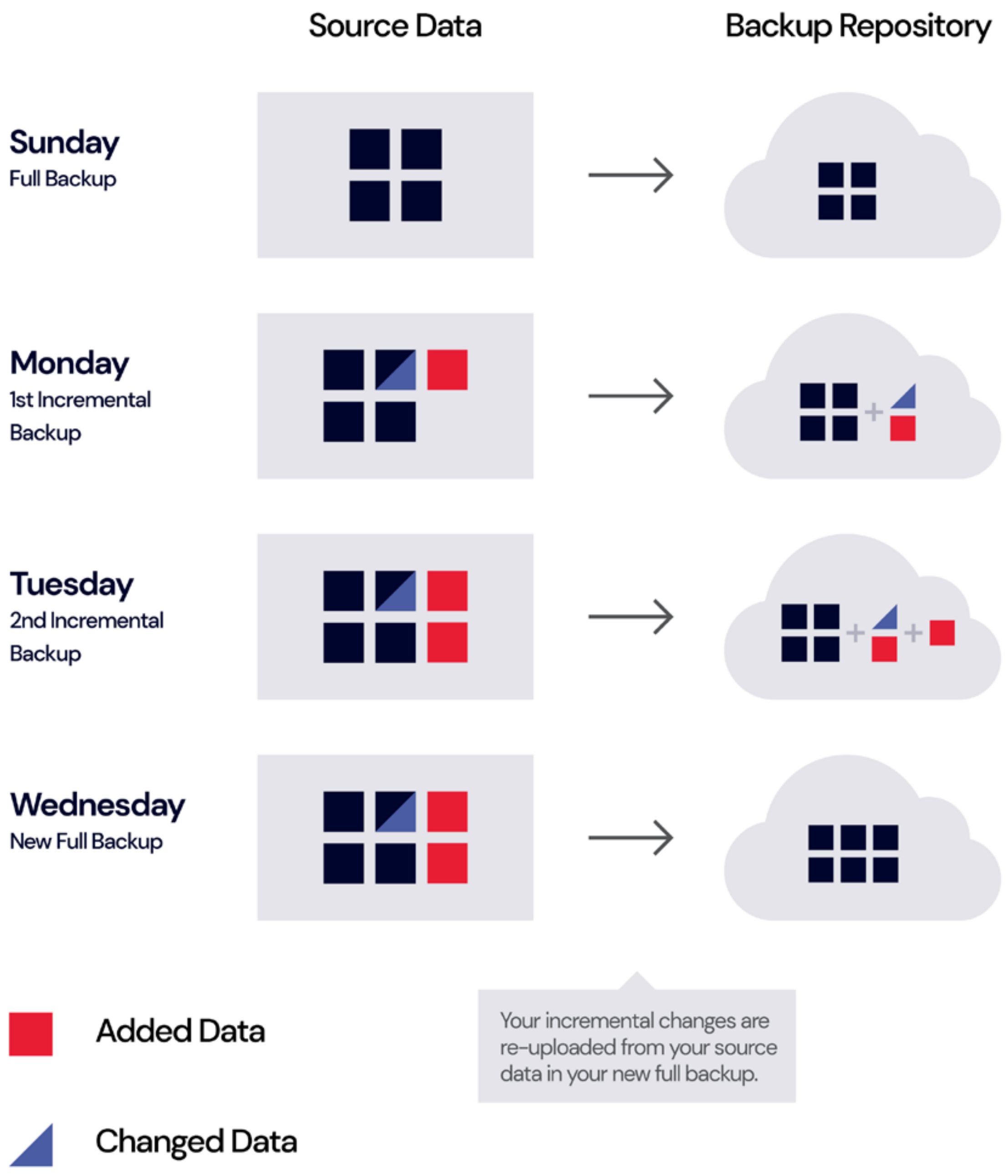
Once you have your full backup, you have a baseline for any subsequent backups. For reasons already explained, it's probably not efficient for you to do a full backup each time. That's where incremental backups come in.

Incremental backups copy the data that has changed or has been added since your last full backup and then, any newly changed or added data since the previous incremental backup.

Let's take a look at the image on the next page. This person performs their full backups on Sundays and Wednesdays so that they always have a fairly recent complete copy of their data. Then, on the other days of the week, they perform incremental backups. (To be clear, we're not recommending this cadence—it's just for demonstration purposes.) Here's a step-by-step overview of the process:

- **Sunday:** A full backup is created.
- **Monday:** After the full backup on Sunday, one file is changed (the purple triangle) and one new file is added (the red square). Both of these changes are uploaded to the backup repository in the cloud.
- **Tuesday:** An additional new file is created (the second red square). This one piece of new data is sent to the cloud. You can see how incremental backups are backing up only new or changed data one piece at a time.
- **Wednesday:** A new full backup is run, which creates a complete copy of the source data (including all previously changed and added data) and stores that in the cloud. This starts the cycle of full backups to incremental backups over again.

Incremental Backup



Your incremental changes are re-uploaded from your source data in your new full backup.

Note that there is another consideration here—whether you want your full backups to overwrite your existing backup repository or whether you would like to keep the previous versions of your files for extra security. Keeping an archive of your previous versions takes up more space (and therefore costs more) but it can be helpful to have an archive for some length of time (called your retention period). On the other hand, some backup providers charge retention minimums where they continue to bill you for data deleted before a certain time frame—make sure to read the terms and conditions carefully so you're not stuck paying for deleted backups. Again, this all differs according to your data security needs. Some people keep archives going back a month. Some may keep an archive for a full year's worth of previous versions. It's all up to you.

Determining how often and when to do your full backups, as well as deciding how many previous versions of your backups you want to keep, is a strategic decision that should take into consideration your typical operating conditions, your risk factors, your budget, and your time. For instance, you could perform a full backup on Sundays and incremental backups Monday through Saturday. Or, you may not even perform full backups as often as that; it's important to think about your data and how often it changes.

Pros

- In a disaster recovery scenario, your restore will consist of your full backup and all of the incremental backups you've made.

Cons

- If you've made a lot of changes to your data since your last full backup, your restore could take some time, as it progresses through this chain of incremental changes. In other words, if you are only doing full backups monthly or less often and you add or change a lot of data in between, your recovery will take a long time because the restore will first process your last full backup and then each piece of incrementally changed or added data.
- Another downside is that your recovery could be compromised by any missing or damaged files, which would break your chain of backups and would make recovery of those files impossible. For this reason (and because having a fairly recent full backup is always a good idea), it's important to do full backups regularly so you have a fresh full copy of your data to work from.

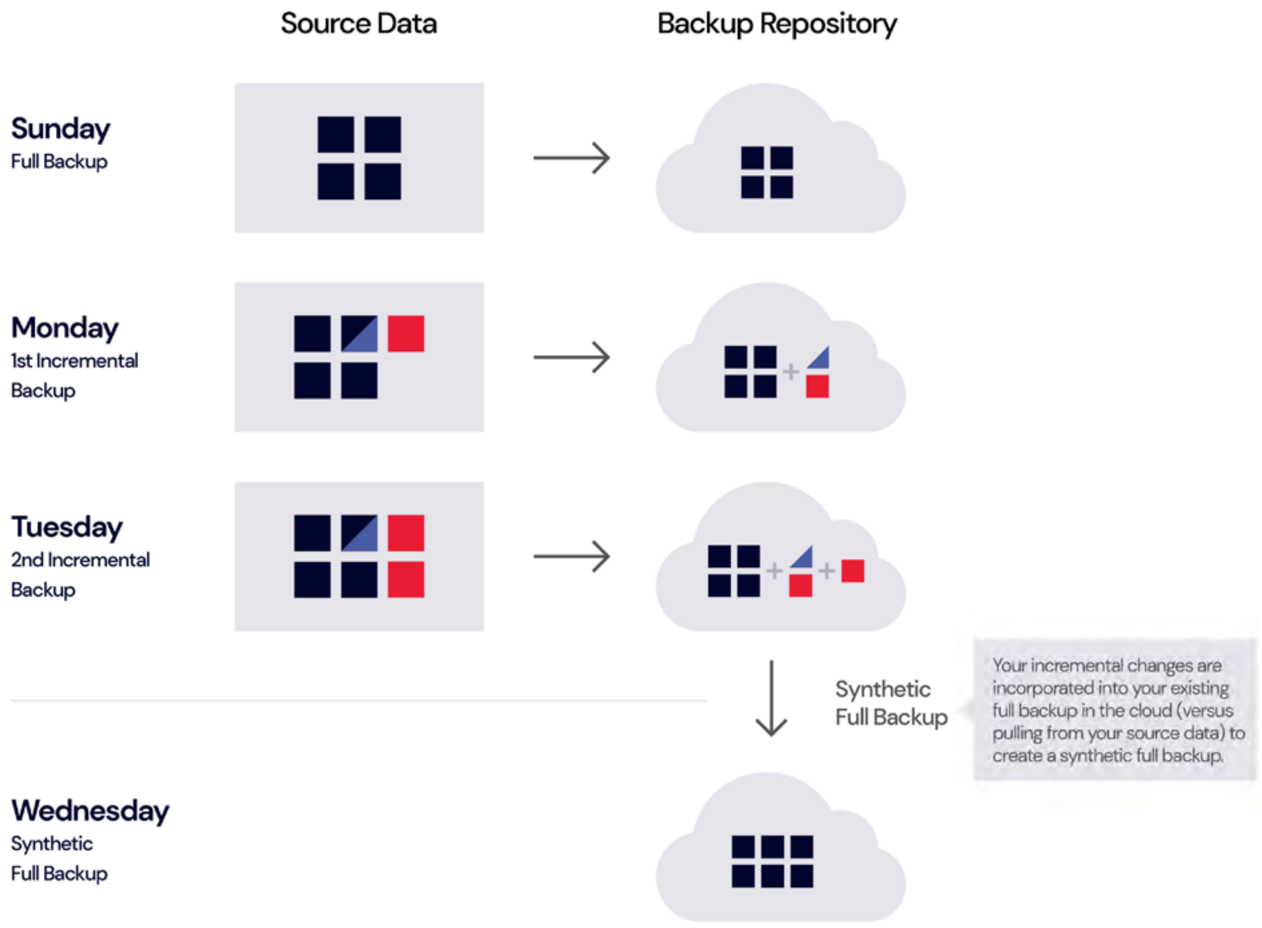
Synthetic Full Backups

We’ve already talked about the need to perform regular full backups, even if (and especially if) you’re using incremental backups. We’ve also discussed how regular full backups can be time-consuming. Synthetic full backups may give you the best of all worlds. They make use of incremental backups to create a more efficient full backup experience.

In a synthetic full backup, your backup software takes your previous full backup and all the incremental backups you’ve created over a set period of time and combines them into a new full, synthesized backup. Your new synthetic backup contains the same data as an active full backup. The only difference is how the new backup is created. Instead of copying your source data to create a new, full backup, the synthetic full backup includes the unchanged data from the source plus all the incremental backups of changed data.

In the diagram on the next page, our hypothetical person performed a full backup on Sunday and an incremental backup on Monday and Tuesday. On Wednesday, their backup software performed a synthetic full backup by taking the previous backups from the backup repository and forging them into a new data set that is also a faithful copy of the source data. In other words, the synthetic full backup is completed in the cloud by merging the backups in the cloud, rather than referring to the source data.

Synthetic Backup



Your incremental changes are incorporated into your existing full backup in the cloud (versus pulling from your source data) to create a synthetic full backup.

🟥 Added Data

◢ Changed Data

Pros

- Synthetic full backups are much faster than normal, active full backups. And because they contain a 100% copy of your data, they serve as the starting point for any subsequent incremental backups, thus resetting your backup chain.
- Your backup software may have an option in your settings that needs to be turned on to enable synthetic full backups, so be sure to check out your tool's help resources to locate this option. You will also be able to define when that synthetic full backup should be created. Put some thought into this, considering when and how often your data gets changed. Because your synthetic full backup is based on the interim incremental backups, it's still somewhat at risk of being corrupted if one of the incremental backups is damaged.

Cons

- Since synthetic backups are much faster to create, you can regularly create new synthetic full backups to reduce that risk. For instance, let's say you create your first full backup on Sunday. Then, Monday through Saturday you create incremental backups of your changed data. On the next Sunday, your system creates a synthetic full backup by combining the unchanged data from the first full backup plus all of the incremental backups completed during the week.

Ultimately, synthetic full backups allow you to create full backups more often, without hogging up precious bandwidth or storage space. And, having a full backup of your data is always the best way to protect your business from a data disaster.

Some of Backblaze's partners support synthetic full backups, including MSP360 and Veeam, so be sure to check your backup tool's help articles to see if this option is available to you.

Differential Backups

There's another kind of backup to be aware of. Differential backups are popular for database applications like Microsoft SQL but not used frequently otherwise. Differential backups look at the last full backup only, and they collect the changes from the full backup. As you make changes to your original data set (the one in the full backup), your differential backup grows.

In our visual on the next page, the full backup takes place on a Sunday. Each time the differential backup runs, it looks back to the full backup to see what has changed from the original source data. Again, changes can be modified files (like our purple triangle) or new files (like our red squares). It adds these changes to the backup repository in a cumulative way, which means differential backups can grow to be quite large.

Pros

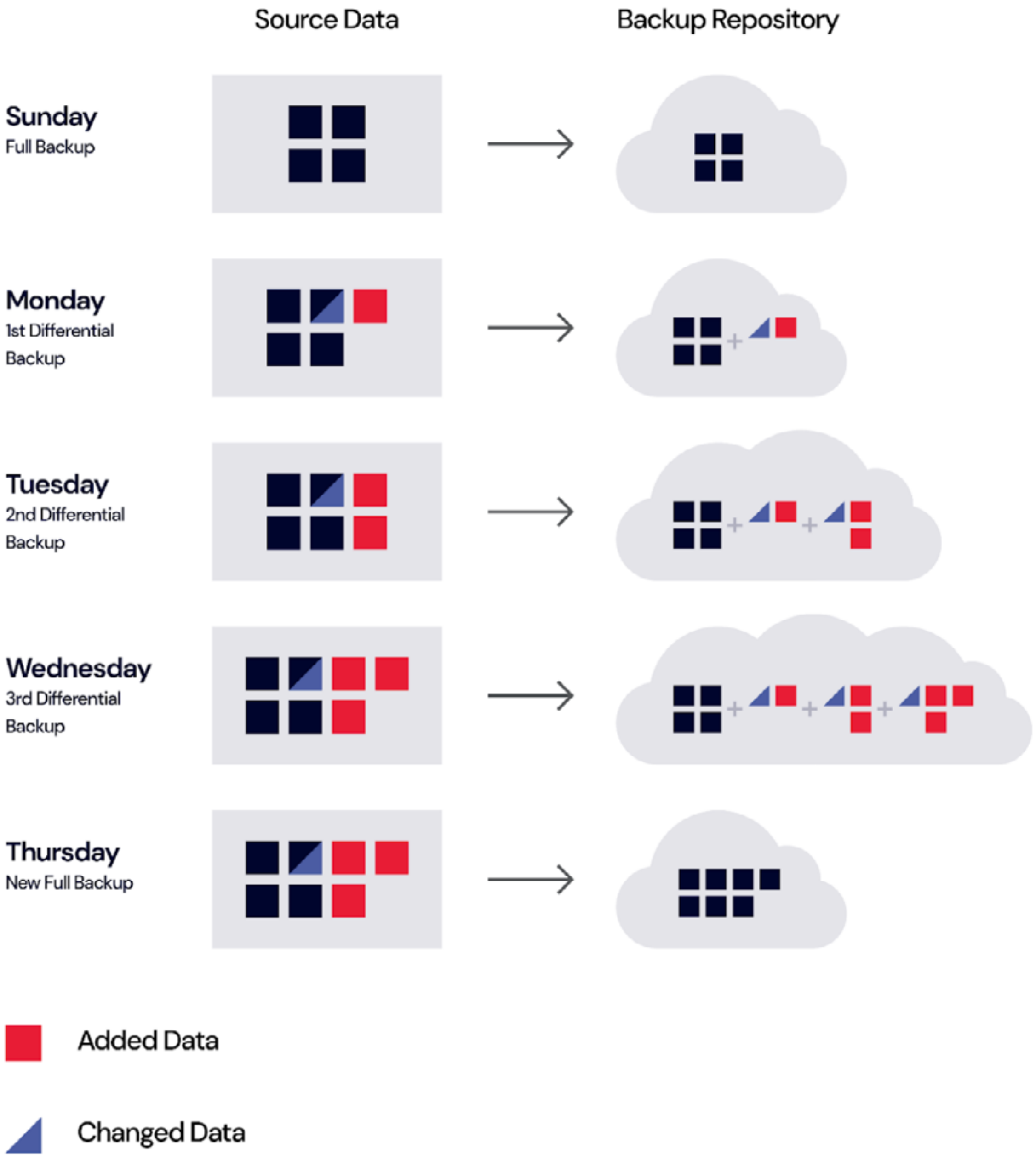
- Like incremental backups, differential backups are much faster to perform than a full backup. To perform a recovery from a differential backup, you just need the full backup and the latest differential backup. So differential backup restores can be quite fast.

Cons

- The overall differential backup can take up a large amount of storage space, as the changed files are uploaded to the backup repository until a new full backup is done. Hence, they don't necessarily offer cost savings in the way of storage.

While differential backups are uncommon, they are included here to ensure a full scope of the various types of backups that exist.

Differential Backup



File-level vs. Block-level Incremental Backups

To add another level of complexity to your decision-making, within the category of incremental backups, there are two standard options: file-level and block-level incremental backups.

Many backup tools offer these options in the configuration settings, so it's important to understand the difference. After you decide which type of incremental backup is best for you, check your backup software's support articles to see if you can configure this setting for yourself.

File-level Incremental Backups

When a file-level incremental backup is performed and a file has been modified, the entire file is copied to your backup repository. This takes longer than performing a block-level backup because your backup software will scan all your files to see which ones have changed since the last full backup and will then back up the entire modified file again.

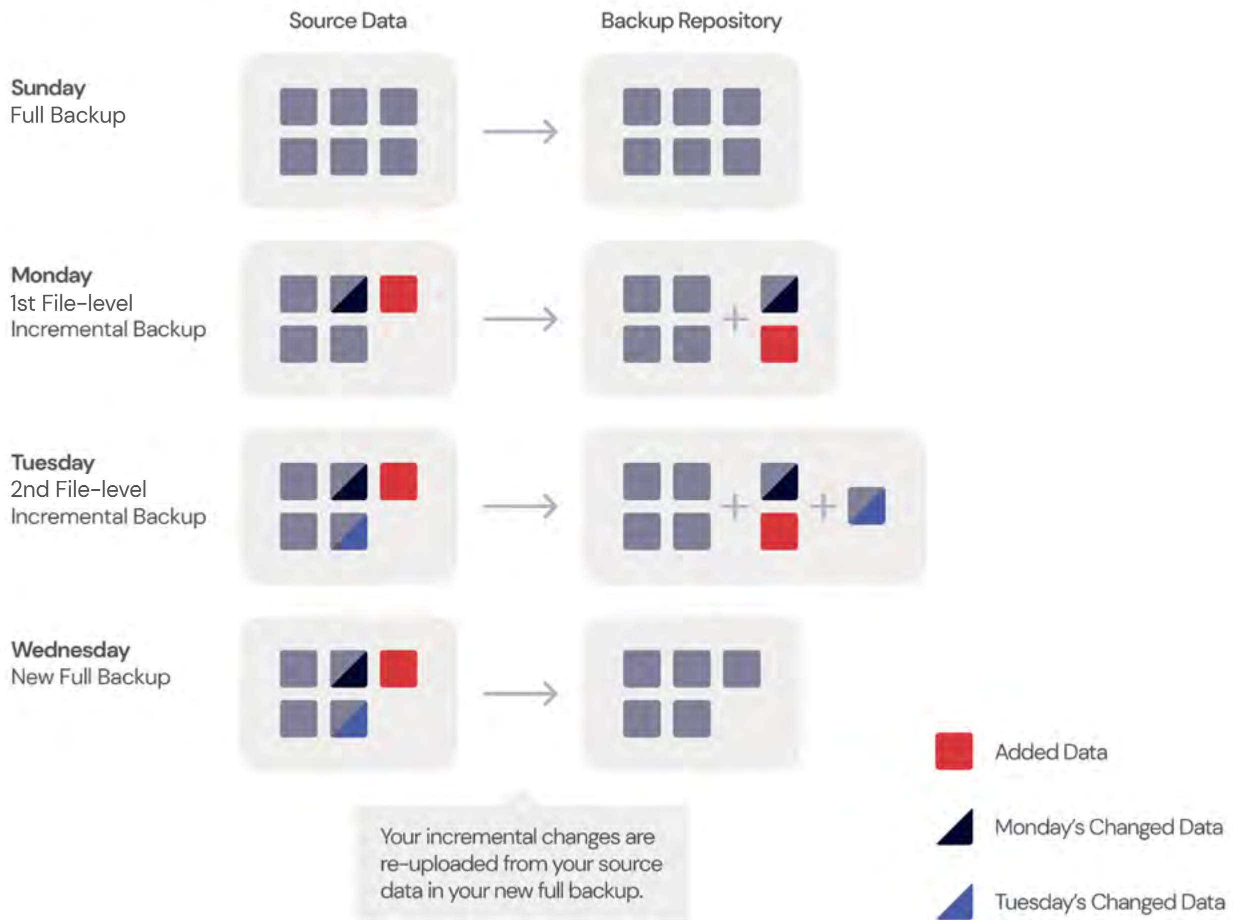
Imagine that you have a really big file and you make one small change to that file; with file-level backups, the whole file is re-uploaded. This likely sounds pretty inefficient, but there are some advantages to a file-level backup:

- It's simple and straightforward.
- It allows you to pick and choose the files you want backed up.
- You can include or exclude certain file types or easily back up specific directories.

File-level backups might be the right choice for a small business with a small amount of data that isn't frequently modified.

The diagram below illustrates this concept. This person performs their full backup on Sundays and Wednesdays. (Again, to be clear, we're not recommending this cadence—it's just for demonstration purposes.) This results in a 100% copy of their data to a backup repository like Backblaze B2. On Monday, part of a file is changed (the black triangle) and a new file is added (the red square). The file-level incremental backup uploads the new file (the red square) and the entire file that has changed (the gray square with the black triangle). On Tuesday, another file is changed (the purple triangle). When the file-level incremental backup is performed, it adds the entire file (the gray square with the purple triangle) to the backup repository. On Wednesday, a new full backup is run, which creates a complete copy of the source data (including all your previously changed and added data) and stores that in the cloud. This starts the cycle of full backups to incremental backups over again.

File-level Incremental Backup



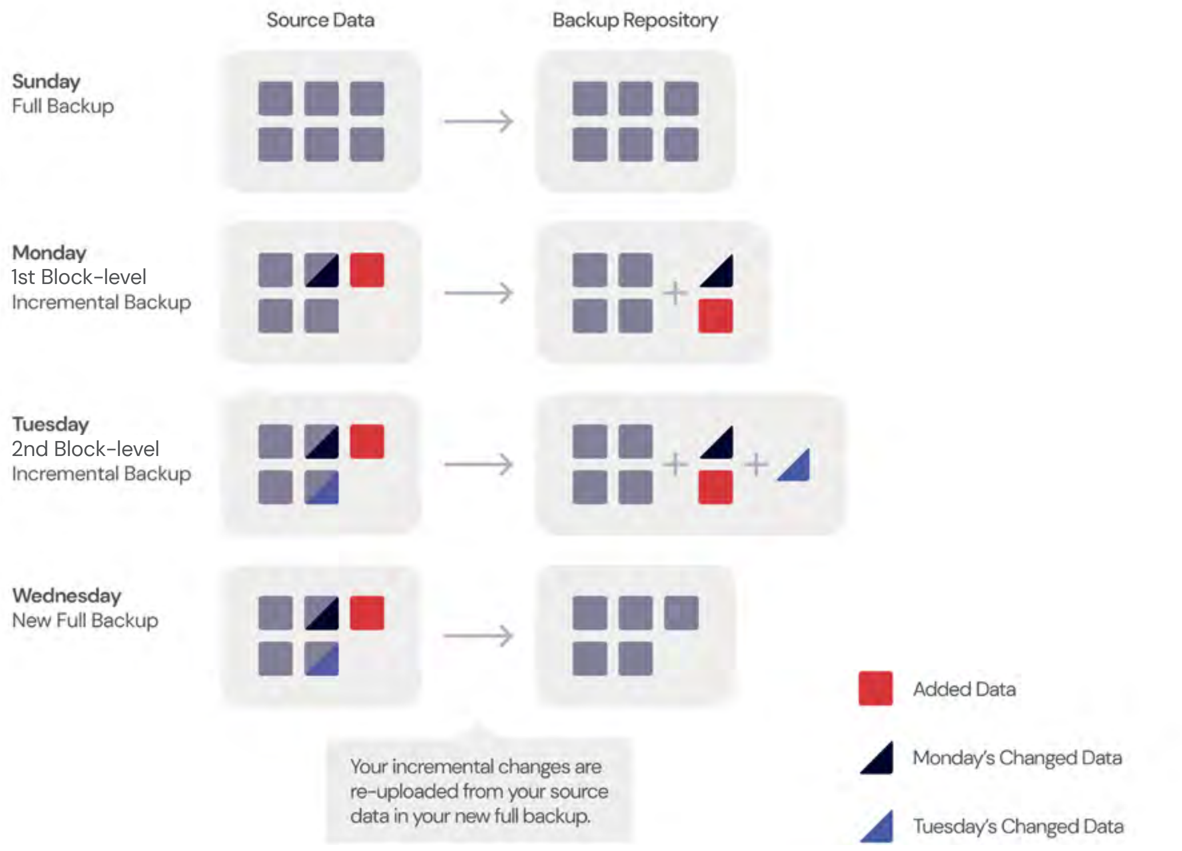
Your incremental changes are re-uploaded from your source data in your new full backup.

Block-level Incremental Backups

Block-level incremental backups do not copy the entire file if only a portion of it has changed. With this option, only the changed part of the file is sent to the backup repository. Because of this, block-level backups are faster and require less storage space. If you're backing up to cloud storage, obviously this will help you save on storage costs.

Let's return to our scenario where full backups are performed on Sundays and Wednesdays, but this time, block-level incrementals are being run in between. When the first block-level incremental backup is run on Monday, the backup software copies just the changed piece of data in the file (the black triangle) and the new data (the red square). In the Tuesday backup, the additional modified data in another file (the purple triangle) is also added to the backup repository. On Wednesday, the new full backup results in a fresh copy of the full data set to the cloud.

Block-level Incremental Backup



Your incremental changes are re-uploaded from your source data in your new full backup.

Block-level incremental backups take a snapshot of the running volume and data is read from the snapshot. This allows files to be copied even if they're currently in use in a running software program, and it also reduces the impact on your machine's performance while the backup is running.

This backup type works better than file-level incremental backups when you have a large number of files or files that often change. If you don't need to pick and choose which files to specifically include or exclude in your backup, it's generally best to use block-level incremental backups, as they're more efficient.

The only drawbacks to block-level incremental backups are that recovery may take longer, since your backup software will need to recover each piece of modified data and rebuild the file. And, because this style of incremental backup uploads modified data in pieces and parts, if one of those pieces becomes corrupted or is unable to be recovered, it could affect your ability to recover the whole file. For this reason (and plenty of other good reasons), it's important to regularly include full backups in your backup strategy and not just count on incremental backups perpetually.

Grandfather-Father-Son Backups

Now you understand the difference between full, incremental, synthetic full, and differential backups, the next part of your strategy is to consider how often to perform full backups, with the assumption that you'll fill the gap between full backups with incremental (or differential) backups.

One way to simplify your decision-making around backup strategy, including when to perform full vs. incremental backups, is to follow the grandfather-father-son (GFS) backup scheme. GFS provides recommended, but flexible, rotation cycles for full and incremental backups and has the added benefit of providing layers of data protection in a manageable framework.

How do GFS Backups Work?

In the traditional GFS approach, a full backup is completed on the same day of each month (for example, the last day of each month or the fourth Friday of each month—however you want to define it). This is the grandfather cycle. It's best practice to store this backup off-site or in the cloud. This also helps satisfy the off-site requirement of a 3-2-1 strategy.

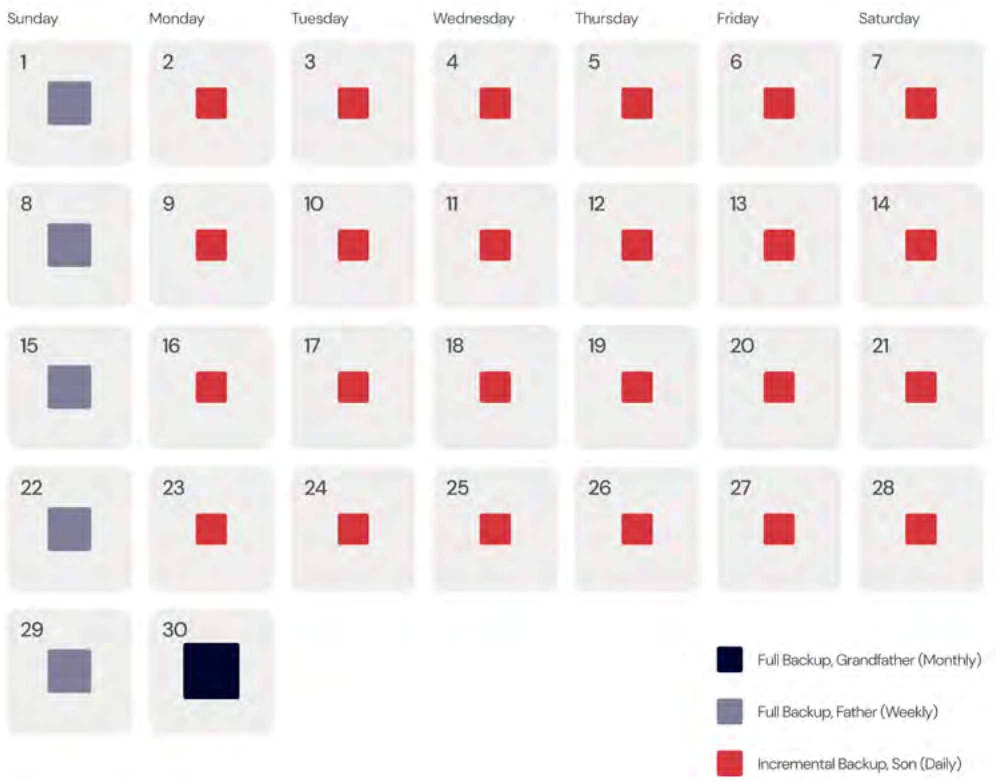
Next, another full backup is set to run on a more frequent basis, like weekly. Again, you can define when exactly this full backup should take place, keeping in mind your business's bandwidth requirements. (Because full backups will most definitely tie up your network for a while!) This is the father cycle, and, ideally, your backup should be stored locally and/or in hot cloud storage, like Backblaze B2, where it can be quickly and easily accessed if needed.

Last, plan to cover your bases with daily incremental backups. These are the son backups, and they should be stored in the same location as your father backups.

GFS Backups: An Example

In the example month shown below, the grandfather backup is completed on the last day of each month. Father full backups run every Sunday, and incremental son backups run Monday through Saturday.

Sample GFS Schedule



Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1 ▨	2 🟥	3 🟥	4 🟥	5 🟥	6 🟥	7 🟥
8 ▨	9 🟥	10 🟥	11 🟥	12 🟥	13 🟥	14 🟥
15 ▨	16 🟥	17 🟥	18 🟥	19 🟥	20 🟥	21 🟥
22 ▨	23 🟥	24 🟥	25 🟥	26 🟥	27 🟥	28 🟥
29 ▨	30 ■					

■ Full Backup, Grandfather (Monthly)

▨ Full Backup, Father (Weekly)

🟥 Incremental Backup, Son (Daily)

It's important to note that the daily-weekly-monthly cadence is a common approach, but you could perform your incremental son backups even more often than daily (Like hourly!) or you could set your grandfather backups to run yearly instead of monthly. Some choose to run grandfather backups monthly and great-grandfather backups yearly. Essentially, you just want to create three regular backup cycles (one full backup to off-site storage; one full backup to local or hot storage; and incremental backups to fill the gaps) with your grandfather full backup cycle being performed less often than your father full backup cycle.

How Long Should You Retain GFS Backups?

Last, it's important to also consider your retention policy for each backup cycle. In other words, how long do you want to keep your monthly grandfather backups, in case you need to restore data from one? How long do you want to keep your father and son backups? Are you in an industry that has strict data retention requirements? You'll want to think about how to balance regulatory requirements with storage costs.

Ultimately, you'll find that grandfather-father-son is an organized approach to creating and retaining full and incremental backups. It takes some planning to set up but is fairly straightforward to follow once you have a system in place. You have multiple fallback options in case your business is impacted by ransomware or a natural disaster, and you still have the flexibility to set backup cycles that meet your business needs and storage requirements.

How Long Should You Keep Your Previous Backups?

When planning your backup strategy, you also must consider how long you want to keep your previous backups. Will you keep them for a specific amount of time and overwrite older backups?

By overwriting the files, you can save space, but you may not have an old enough backup when you need it. Also, keep in mind that many cloud storage vendors have minimum retention policies for deleted files. While retention sounds like a good thing, in this case it's not. They might be charging you for data storage for 30, 60, or even 90 days even if you deleted it after storing it for just one day. That may also factor into your decision about how long you should keep your previous backup files. Some experts recommend three months, but that may not be enough in some situations.

You need to keep full backups for as long as you might need to recover from various issues. If, for example, you are infiltrated by a cybercriminal and don't discover it for two months, will your oldest backup be enough to restore your system back to a clean state?

Another question to think about is if you'll keep an archive. As a refresher, an archive is a backup of historical data that you keep long term even if the files have already been deleted from the server. Most sources say you should plan to keep archives forever unless you have no use for the data in the future, but your company might have a different appetite for retention timeframes. Keep in mind that the security of having those files available may be worth it.

How Will You Monitor Your Backup?

It’s not enough to just schedule your backups and walk away. You need to monitor them to ensure they are occurring on schedule. You should also test your ability to restore and fully understand the options you have for restoring your data. A backup is only as good as its ability to restore. You must test this out periodically to ensure you have a solid disaster recovery plan in place.

Special Considerations for Backing Up Servers

When backing up servers with different operating systems, you need to consider the constraints of that system. For example, SQL servers can handle differential backups, whereas other servers cannot. Some backup software integrates easily with all the major operating systems and therefore supports backups of multiple servers using different platforms.

If you are backing up a single server, things are easy. You have only one OS to worry about. However, if you are backing up multiple servers with different platforms and applications running on them, things could get more complex. Be sure to research all your options and use a vendor that can easily handle groups management and SaaS-managed backup services so that you can view all your data through a single pane of glass. You want consolidation and easy delineation if you need to pinpoint a single system to restore. You can use groups to easily manage different servers with similar operating systems to keep things organized and streamline your backup strategy.

Choosing a Server Backup Solution

This section explains some best practices and decision criteria for choosing the right backup solution for you.

How to Evaluate a Server Backup Solution

An important factor to consider when choosing the right backup software and cloud storage is compatibility. Research which platforms your software will back up comfortably and what types of backups it offers (file, image, system, etc.). You also need to think about the restore process and your options (e.g., file, folder, bare metal/image, virtual, etc.). User friendliness is important when deciding. Some programs like rclone require a working knowledge of command line. Choose a software program that is best for you.

Think about scalability and how much storage it can handle now and in the future as your business grows. A few other things to consider are pricing, security, and support. Your backup files are no good if they are vulnerable to attack. Compare prices and check out the support options before making your final decision.

Choosing the best cloud storage solution for your organization involves careful consideration. There are several types of solutions available, each with unique capabilities. You don't need the most expensive solution with bells and whistles. All you need to do is find the solution that fits your business model and future goals.

However, there are five main features that every organization seeking object storage in the cloud should look out for:

Cost

Cost is always a top concern for adopting new processes and tools in any business setting. Before choosing a cloud storage solution, take note of any fees or file size requirements for retention, egress, and data retrieval. Costs can vary significantly between storage providers, so be sure to check pricing details.

Ease of Use and Onboarding Support

Adopting a new digital tool may also require a bit of a learning curve. Choosing a solution that supports your OS and is easy to use can help speed up the adoption rate. Check to see if there are data transfer options or services that can help you migrate more effectively. Not only should cloud storage be simple to use, but easy to deploy as well.

Security and Recovery Capabilities

Most object storage cloud solutions come with security and recovery capabilities. For example, you may be looking for a provider with Object Lock capabilities to protect data from ransomware or a simple way to implement disaster recovery protocols with a single command. Otherwise, you should check if the security specs meet your needs.

How Backblaze Can Help: Object Lock

Object Lock allows you to store objects using a Write Once, Read Many model, meaning after it's written, data cannot be modified or deleted for a defined period of time. Any attempts to manipulate, copy, encrypt, change, or delete the file will fail during that time. The files may be accessed, but no one can change them, including the file owner or whoever set the Object Lock. Backblaze offers Object Lock functionality via API and third-party integrations.

Integrations

All organizations seeking cloud storage solutions need to make sure that they choose a compatible solution with their existing systems and software. For example, if your applications speak the S3 API language, your storage systems must also speak the same language.

Many organizations use software-based backup tools to get things done. To take advantage of the benefits of cloud storage, these digital tools should also integrate with your storage solution. Popular backup solutions such as MSP360 and Veeam are built with native integrations for ease of use.

Support Models

The level of support you want and need should factor into your decision-making when choosing a cloud provider. If you know your team needs fast access to support personnel, make sure the cloud provider you choose offers a support SLA or the opportunity to purchase elevated levels of support.

Buyer’s Guide to Cloud Storage Solutions

Use the worksheet below as you’re evaluating cloud storage solutions. Complete the column “Other Cloud Storage Vendor” to compare them to Backblaze B2 Cloud Storage.

Pricing

	Backblaze B2	Other Cloud Storage Vendor
Cost per TB per month	$6/TB/month	
Egress/Download Charges	Free, up to 3x of data stored and unlimited through many CDN and Compute partners.	
Free Trial Option	Yes, 10GB free	
Minimum Monthly Storage Requirement?	No	
Minimum Storage Retention Policy?	No	
Minimum File Size Requirement?	No	

Data Services

	Backblaze B2	Other Cloud Storage Vendor
Rapid ingestion device available?	Yes, the B2 Fireball	
Data migration services available?	Yes, Universal Data Migration	
Snapshot recovery option?	Yes, sent via FedEx	

Security and Accessibility

	Backblaze B2	Other Cloud Storage Vendor
Supports immutability via Object Lock at no extra cost?	✓	○
Server-side encryption?	✓	○
Uptime SLA of 99.9%?	✓	○
Supports HIPAA requirements (if relevant for your business)?	✓	○
SSAE 18 SOC 2 data centers	✓	○
Durability up to 11 nines	✓	○
Two-factor authentication available	✓	○

Ease of Use

	Backblaze B2	Other Cloud Storage Vendor
S3 Compatible API	✓	○
Integrates with leading backup software/ the application your business uses	✓	○

Additional Considerations

	Backblaze B2	Other Cloud Storage Vendor
Customer Support Included?	✓	○

Questions to Ask Before Deciding on a Cloud Storage Solution

Of course, there are other considerations to take into account. For example, managed service providers will likely need a cloud storage solution to manage multiple servers. Small business owners may only need a set amount of storage for now but with the ability to easily scale with pay-as-you-go pricing as the business grows. IT professionals might be looking for a simplified interface and centralized management to make monitoring and reporting more efficient.

When comparing different cloud solutions for object storage, there are a few more questions to ask before making a purchase:

- **Is there a web-based admin console?** A web-based admin console makes it easy to view backups from multiple servers. You can manage all your storage from one single location and download or recover files from anywhere in the world with a network connection.
- **Are there multiple ways to interact with the storage?** Does the provider offer different ways to access your data, for example, via a web console, APIs, CLI, etc.? If your infrastructure is configured to work with the S3 API, does the provider offer S3 compatibility?
- **Can you set retention?** Some industries are more highly regulated than others. Consider whether your company needs a certain retention policy and ensure that your cloud storage provider doesn't unnecessarily charge minimum file retention fees.
- **Is there native application support?** A native environment can be helpful to back up an Exchange and SQL Server appropriately, especially for team members who are less experienced in cloud storage.
- **What types of restores does it offer?** Another crucial factor to consider is how you can recover your data from cloud storage, if necessary.

Making a Buying Decision: The Intangibles

Lastly, don't just consider the individual software and cloud storage solutions you're buying. You should also consider the company you're buying from. It's worth doing your due diligence when vetting a cloud storage provider. Here are some areas to consider:

Stability

When it comes to crucial business data, you need to choose a company with a long-standing reputation for stability.

Data loss can happen if a not-so-well-known cloud provider suddenly goes down for good. And some lesser-known providers may not offer the same quality of uptime, storage, and other security and customer support options.

Find out how long the company has been providing cloud storage services, and do a little research to find out how popular its cloud services are.

Customers

Next, take a look at the organizations that use their cloud storage backup solutions. Do they work with companies similar to yours? Are there industry-specific features that can boost your business?

Choosing a cloud storage company that can provide the specs that your business requires plays an important role in the overall success of your organization. By looking at the other customers that a cloud storage company works with, you can better understand whether or not the solution will meet your needs.

Reviews

Online reviews are a great way to see how users respond to a cloud storage product's features and benefits before trying it out yourself.

Many software review websites such as G2, Gartner Peer Insights, and Capterra offer a comprehensive overview of different cloud storage products and reviews from real customers. You can also take a look at the company's website for case studies with companies like yours.

Values

Another area to investigate when choosing a cloud storage provider is the company values.

Organizations typically work with other companies that mirror their values and enhance their ability to put them into action. Choosing a cloud storage provider with the correct values can help you reach new clients. But choosing a provider with values that don't align with your organization can turn customers away.

Many tech companies are proud of their values, so it's easy to get a feel for what they stand for by checking out their social media feeds, about pages, and reviews from people who work there.

Continuous Improvement

An organization's ability to improve over time shows resiliency, an eye for innovation, and the ability to deliver high-quality products to users like you. You can find out if a cloud storage provider has a good track record for improving and innovating their products by performing a search query for new products and features, new offerings, additional options, and industry recognition.

Cloud Storage Solution Evaluation Matrix

You can find out if a cloud storage provider has a good track record for improving and innovating their products by performing a search query for new products and features, new offerings, additional options, and industry recognition.

The Solution

Criteria	Yes/No	Notes
Is there a web-based admin console?		
Are there multiple ways to interact with the storage (i.e., via API, web UI, CLI, etc.)?		
Can you set retention?		
Is there native application support?		
Can you easily restore? What types of restores does it offer?		

The Company

Criteria	Yes/No	Notes
Does the company have a long-standing reputation for stability?		
Does the company serve customers like us?		
Are the reviews generally good?		
Does the company align with our values?		
Does the company have a track record of improving and innovating?		

Recovering From Disaster Using Backups

In any business, time is money. What may shock you is how much money that time is actually worth. According to Gartner, the average cost of one hour of downtime is roughly $300,000. That's $5,600 a minute. Multiply that out by the amount of time it takes to recover from data theft, sabotage, or a natural disaster, and you could easily be looking at millions of dollars in lost revenue. That is, unless you've planned ahead with an effective disaster recovery plan.

This section covers how to develop an effective disaster recovery plan so you can quickly rebound no matter what happens, including:

- Knowing what a disaster recovery plan is and why you need it.
- Developing an effective strategy.
- Identifying key roles.
- Prioritizing business operations and objectives.
- Deploying backups.

What Is a Disaster Recovery Plan?

A disaster recovery plan is made up of resources and processes that a business can use to restore apps, data, digital assets, equipment, and network operations in the event of any unplanned disruption.

Events such as natural disasters (floods, fires, earthquakes, etc.), theft, and cybercrime often interrupt business operations or restrict access to data. The goal of a disaster recovery plan is to get back up and running as quickly and smoothly as possible.

Some companies will choose to write their own disaster recovery plans, while others may contract with a MSP specializing in disaster recovery as a service. Either way, crafting a disaster recovery plan that covers you for any contingency is crucial.

Why Do You Need a Disaster Recovery Plan?

A disaster recovery plan is not just a good idea, it is an essential component of your business. Cybercrime is on the rise, targeting SMBs just as often as large corporations. According to Cybersecurity Magazine, 43% of recent data breaches affected SMBs. Additionally, you could be cut off from your data by power outages, hardware failure, data corruption, and natural occurrences that restrict IT workflows. So, why do you need a disaster recovery plan? A few key benefits rise to the top:

- Your disaster recovery plan will ensure business continuity in the case of a disaster. Imagine the confidence of knowing that no matter what happens, your business is prepared and can continue operations seamlessly.
- An effective disaster recovery plan will help you get back up and running faster and more efficiently.
- The plan also helps to communicate to your entire team, from top to bottom, what to do in the event of an emergency.

Writing a Disaster Recovery Plan: What Should Your Plan Include?

A solid disaster recovery plan should include five main elements, which we'll detail below:

1. An effective strategy.
2. Key team members who can carry out the plan.
3. Clear objectives and priorities.
4. Solid backups.
5. Testing protocols.

Develop an Effective Strategy

One of the most critical aspects of your disaster recovery plan should be your strategy. Typically, the details of a disaster recovery plan include steps for prevention, preparation, mitigation, and recovery. Think about both the big picture and fine details when putting together the pieces. Some tips for creating an effective strategy include:

- **Identify possible disasters.** Consider the types of disasters your business may encounter and design your plan around those. Every business is susceptible to cybercrime, which should be a significant component of your plan. If your business is located in a disaster prone location, let that dictate your plan objectives.
- **Plan for minor disasters.** A major disaster like an earthquake could take out the entire office and on-premises infrastructure, but minor disasters can also be disruptive. Good employees make mistakes and delete things, and bad employees sometimes make worse mistakes. A disaster recovery plan protects you from those minor disasters as well.

- **Create multiple disaster recovery plans.** You may need to create different versions of your disaster recovery plan based on specific scenarios and the severity of the disaster. For example, you may need a plan that responds to a cyberattack and restores data quickly, while another plan may deal with hardware destruction and replacement rather than data restoration.
- **Plan from your recovery backward.** Think about what you need to accomplish with your disaster recovery and plan your backup routine to support it. Then, after your plan is written, go back and ensure that your backup routine follows the plan initiatives and accomplishes the goals in an acceptable time frame.
- **Develop KPIs.** Include critical key performance indicators (KPIs) in the plan, such as a recovery time objective (RTO) and recovery point objective (RPO). RTO refers to how quickly you intend to restore your systems after a disaster, and RPO is the maximum amount of data loss you can safely incur.

Establish the Key Team Members and Their Roles and Hierarchy

Another crucial component of your disaster recovery plan is identifying key team members to carry out the instructions. You must clearly define roles and hierarchy for effectiveness. Consider the following when building your disaster recovery team:

- **Communicate roles and hierarchy.** Ensure that each team member knows their role in the plan and understands where they land in the hierarchy. Build in redundancy if a major player is unavailable.
- **Develop a master contact list.** Create a master list with updated contact information for each team member and update it regularly as things change. Be sure the list includes everyone's cell phone and landline numbers (if applicable) and emergency contacts for each person. Don't assume you will have working internet and consider alternative ways to reach critical team members in the middle of the night.
- **Plan on how to manage your team.** Think about how you will stay organized and manage your team to function 24/7 until you resolve the disaster.

Prioritize Business Operations and Objectives

Another important aspect of your disaster recovery plan is prioritizing business operations and objectives and crafting your plan around those.

Identify the most critical aspects of the business that need to be restored first. Then, focus on those and leave the less essential things until later. Understand that it is not feasible to restore everything at once. Instead, you must prioritize the most critical business areas and get those up and running and then, other, less crucial parts of the system. Detail these priorities in your plan so that no one wastes time on nonessential operations.

Know How to Deploy Your Backups

Backups should be a routine function for your organization, and you should know them inside and out. Be sure to familiarize yourself with every aspect of the backup process, where data is stored, how recent it is, and how to restore it at a moment's notice.

Having a reliable backup plan could save your business. You don't want to waste precious time figuring out where the latest backup is, where it's stored (whether that's locally or on the cloud), or how to access it. Off-site cloud storage is a safe, reliable way to store and retrieve your data, especially in the event of a disaster.

Practice restoring your backups regularly to test their viability. Document the process for restoring in case you are unavailable and someone else has to take over. Data restoration should be a central part of your disaster recovery plan. Remember, backups are not your entire disaster recovery plan but only a piece of the overall system.

Foolproof Your Plan With Disaster Recovery Testing

The best-laid plans don't always work out. Therefore, it's essential that you foolproof your disaster recovery plan by testing it regularly (once a year, or every six months, whatever works for you). You don't have to experience a real catastrophe; you can simulate what a disaster would look like and run through the entire process to ensure everything works as expected. Some disaster recovery testing best practices include:

- **Planning for the worst-case scenario.** Think about things like access to a car, how you will get to the office, and how you will access your backups if they are stored online and you don't have internet? Prepare by having multiple alternate plans (A, B, C, etc.). Remember, disasters come in all shapes and sizes so, be prepared to think outside the box. When the COVID-19 pandemic started, businesses had to scramble to adjust. Prepare for anything, even minor disruptions or cut-offs from resources you rely on.
- **Securing resources in advance.** If you need resources to make it work, such as budgetary funds, software, hardware, or services, get those approved now so you're not stuck provisioning necessary resources in the middle of a disaster.
- **Regularly reviewing and updating your disaster recovery plan** as things change. Team members come and go, so schedule routine updates every three to six months to ensure that everything is up to date and viable.
- **Distributing copies of your disaster recovery plan.** All staff members, including executives, should have a copy of your plan, and you should clearly communicate how it works and what everyone's responsibility is.
- **Conducting post mortems** after training and simulations (or a real disaster) to determine what works and what doesn't. Make changes to your plan accordingly.

Don't wait until a disaster occurs before writing your disaster recovery plan. A disaster recovery plan is an ever-evolving process you must maintain as the business changes and grows so you can face anything that the future brings.

How Backblaze Can Help: Disaster Recovery, Done

Ready to check disaster recovery off your list? Check out our Instant Recovery in Any Cloud solution that you can use as part of your disaster recovery plan. You can run a single command to instantly see your servers, data, firewalls, and network storage. Get back up and running as soon as possible with minimal disruption and expense to your business.

Key Takeaways

With this guide, you can approach backing up your servers with confidence, including understanding how to create a server backup strategy, choose server backup solutions, and recover from disaster using your backups. To summarize, here are the major takeaways to remember when approaching server backups:

- **You have many options for where to back up servers**, including on-premises solutions like NAS and LTO/tape, as well as cloud solutions like cloud storage. Remember a strong 3-2-1 strategy includes both.
- **Make sure to follow the 3-2-1 strategy**, with three copies of your server data, in two locations, with one off-site.
- **Establish a cadence between full, incremental, and synthetic backups** that works best for your needs.
- **Consider using the grandfather-father-son approach** to organize your backup frequency.
- **Evaluate server backup solutions** using our checklist and worksheet to make sure they meet your needs.
- **Finally, create a disaster recovery plan** so you're prepared should you ever need to recover from your backups.

About Backblaze

Backblaze makes it astonishingly easy to store, use, and protect data. The Backblaze Storage Cloud provides a foundation for businesses, developers, IT professionals, and individuals to build applications, host content, manage media, back up and archive data, and more. With over two billion gigabytes of data storage under management, the company currently works with close to 500,000 customers in over 175 countries. Founded in 2007, the company is based in San Mateo, California.

For more information, please go to www.backblaze.com.