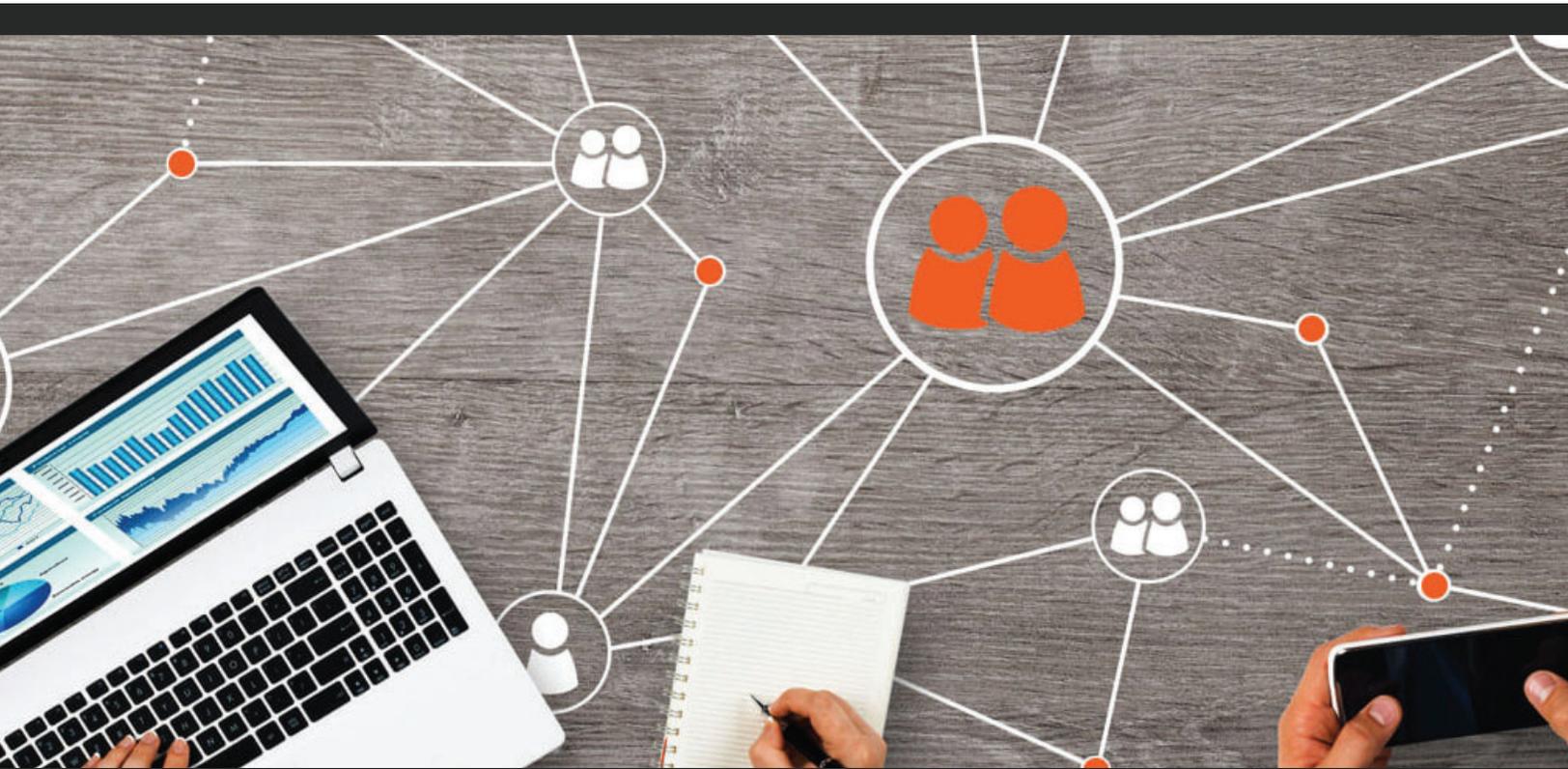


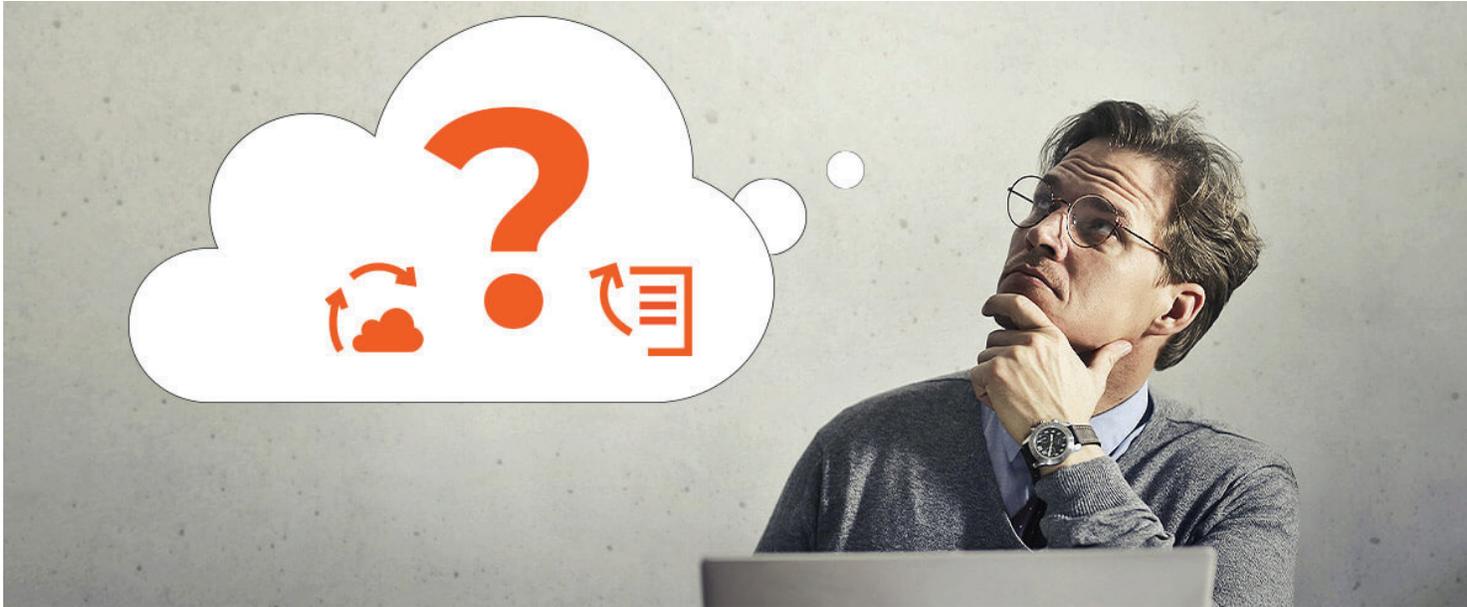
How to select the right Microsoft 365 backup solution



...and why you need to have one in the first place.

Microsoft 365 is in the cloud

Do you really need a backup?



As organizations adapt IT infrastructure to address the changes in how we work, Microsoft 365 has become the go-to cloud productivity and collaboration tool. That means it's also the main repository of emails, documents, meetings, conversations, project plans, and more.

But what if you lost that data? Even a small portion of it?

Some folks disagree that SaaS backups are needed. They point to the Recycle Bin and multiple synchronous copies of the data being automatically stored in multiple locations. While this might seem good in theory, in practice Recycle Bin provides insufficient data protection, and if data gets corrupted, synchronization simply creates more copies of corrupted data.

Microsoft 365's native capabilities for data protection include:

- Version history for each file.
- Deleted items retention to protect against accidental or malicious deletions (Recycle Bin).
- Litigation hold or retention policies to help prevent unwanted data destruction.

These are good features but the built-in capabilities aren't sufficient for organizations that expect and need an enterprise-grade backup and recovery toolset.

Microsoft 365 native data protection

The challenges

Enterprise IT leaders are cautious about ensuring that their users' data is protected. Many won't make a new service available to users until they have a reliable backup and recovery solution in place. Since the native recovery options in Microsoft 365 have limitations, we suggest a similar approach.

Here are some of the known challenges with relying only on Microsoft 365's native data protection:

Deleted items recovery

Microsoft 365 holds deleted files in the recycle bin and purge folders for a set period of time. But a bad deletion (accidental or malicious) could go unnoticed past the prescribed expiry date. If items expire from the recycle bin and purge folders, there is no backup copy available. That isn't the only concern with recovery in Microsoft 365:

- Users have full access to recycle bins and can accidentally (or maliciously) delete data permanently with no option for recovery.
- Bad actors are writing malware targeting Microsoft 365, gaining access to these recycle bins by taking advantage of the Microsoft 365 APIs.
- Recovering files from the Recycle Bin can work for a small number of items, but bulk recovery scenarios prove to be almost unusable. Furthermore, you cannot recover to an alternate location (e.g., for export or for inactive user accounts).



Litigation hold or retention policies

Within Microsoft 365, items marked for a litigation hold, or with a retention policy applied, generate hidden copies that are retained, but the recovery process isn't easy or user-friendly once the original file is deleted.

The deleted items recovery, litigation hold, and retention policies weren't meant to be used in place of a segregated, full-coverage backup solution. Many organizations want to use these features for their intended purpose, but when they're hijacked for a data protection workaround, it nullifies the usefulness of what they were developed to do.

Having a segregated backup of your Microsoft 365 data radically minimizes data loss and frees up the built-in features to be used more effectively. But how do you go about choosing the right backup solution for your organization?



Three critical features you need in a Microsoft 365 backup and archive solution

Not all backup solutions are created equal, so it's important to identify what you actually need before you start the conversation. At a minimum, you'll want to have the ability to do full coverage backups with flexible recovery options, a high level of performance, and scalability so the solution grows with your organization. Beyond that, there are other advanced features to consider that will enhance your ability to protect, recover, archive, and even manage your organization's Microsoft 365 data.





Full coverage

When a backup solution only protects mailboxes, but your organization heavily relies on Teams for internal communications, that solution isn't going to meet your needs. There are many offerings that only protect mailboxes, and some have expanded to protect OneDrive for Business as well.

A full-coverage backup solution should be able to target specific mailboxes or site collections with unique policies. Alternatively, it should be able to cover all mailboxes, OneDrive for Business site collections, SharePoint, and Teams with a default policy.

When covering all targets with a default policy, the solution should auto-enroll new users when they're added to your organization so new mailboxes, OneDrive for Business, SharePoint, and Teams are automatically included in the scope of protection.



If you're looking for a complete Microsoft 365 backup solution, you want something that can handle all:

Mailboxes

- Active and archive mailboxes
- Public folder mailboxes
- Shared mailboxes
- Any and all message attachments

OneDrive for Business site collections

SharePoint site collections

- All content types
- Site hierarchies
- Permissions

Teams (and Groups) site collections

- Document libraries
- Conversations
- All files sent through conversations
- Wikis

Unified audit log

2 Flexible recovery

When your Microsoft 365 backup solution gives you flexible recovery options, you'll have the ability to easily address unanticipated or unconventional recovery requirements. This can be particularly important when managing data through changing roles, staff turnover, mergers and acquisitions, and other organizational changes.

Ensuring that you have flexible recovery options in your backup solution will give you peace of mind that you'll be able to provide efficient and effective recovery support for your organization.



Examples of flexible recovery options:

- **Restore items, folders, mailboxes, or sites with multi-level recovery** – get your data back no matter what.
- **Reinstate multiple mailboxes in a single operation** – resolve large-scale data loss affecting multiple users.
- **Recover data to a preferred location, including cross-tenant recovery/migration (and on-premises Exchange and SharePoint)** – flexibility for users who need access to the data, have changed, or don't have access to the original location of the data such as M&A tenant-to-tenant migration or as part of an exit plan from the cloud.
- **Perform point-in-time recoveries** – roll back the clock on data.
- **Apply filters to your recovery** – recover an entire mailbox except for contacts or recover an entire dataset of OneDrive sites within a date range.
- **Maybe you don't need to recover** – access Microsoft 365 accounts when employees leave or in the case of audits without having to maintain an active license.

3

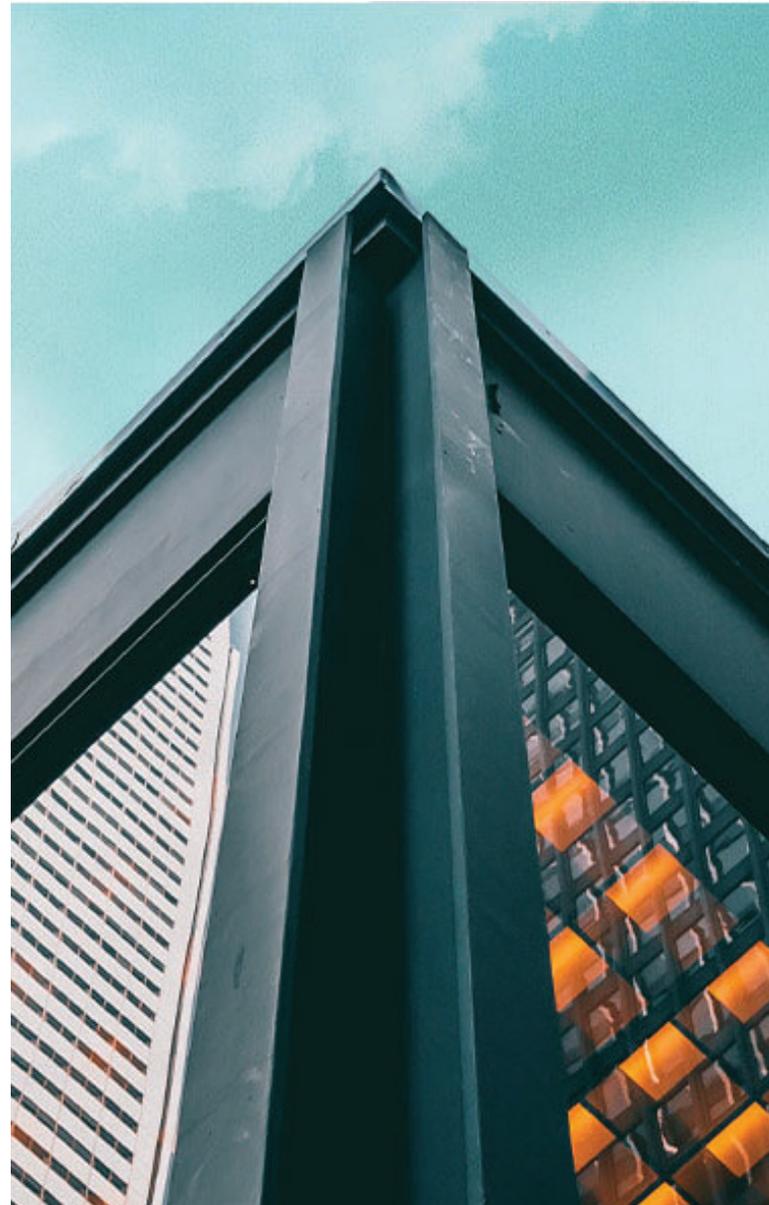
Performance & scalability

You're already managing increasingly-large volumes of data. The cloud makes this easier and more cost-effective as long as it can accommodate the level of performance and scalability your organization needs as it grows. You need a solution that will allow you to manage your volume of data today, tomorrow, and in the years to come.

When it comes to choosing for performance and scalability, your Microsoft 365 backup solution needs to be able to:

- Scale to petabytes of data and billions of objects,
- Capture data at rates of multiple terabytes per hour.
- Augment incremental backups with continuous data protection.

Making the shift from on-premises storage to the cloud is an investment that needs to be sustainable and usable. That's why it's essential for your chosen data protection solution to be able to handle your needs as they grow.



Additional advanced features

Finding a Microsoft 365 backup solution that gives you full coverage, flexible recovery, and a high level of performance and scalability will give your organization a strong security posture. But these additional features enhance your ability to protect and recover the right data at the right time.

Continuous data protection

A Microsoft 365 backup solution that provides continuous data protection (CDP) will actively monitor your data and automatically capture modifications in a near real-time manner. Unlike normal incremental scans or snapshots, which happen at scheduled intervals, CDP is always running to capture any changes as they occur.

Features like CDP are useful for augmenting your Microsoft 365 backup strategy by applying CDP to high-priority site collections and/or users to ensure the continuity and integrity of mission-critical data.

Archive storage for former employees' data

Today's workers are increasingly transient, which leaves IT dealing with a data challenge when it comes to archiving inactive Microsoft 365 user accounts' data. This has become particularly important with the emergence of compliance regulations such as the European Union's (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Finding a backup solution that provides automatic archiving of Microsoft 365 mailboxes, OneDrive and SharePoint data, and Teams means you can avoid unnecessary licensing costs when someone leaves your organization.

Additionally, with a backup solution that gives flexibility around long-term retention, user data can be restored in the future.

Enterprise-grade security

It's no longer enough to protect your data from loss due to mistakes or software crashes. Today you need to protect your data from being stolen, maliciously deleted, and being modified.

To protect your data from being stolen – or even viewed – by anyone, you need a Microsoft 365 backup solution that offers end-to-end data encryption. This means that any data in transit is encrypted, and that your backup data is encrypted when it's stored.

To protect your data against unwanted deletion and modification, you need a Microsoft 365 backup and archive solution that uses immutable storage for your data. This is normally accomplished through the use of some form of WORM (Write Once, Read Many) storage.

Choose the right Microsoft 365 backup solution for your organization

Knowing what's possible and the benefits for your organization can make all the difference when evaluating each solution that allows you to protect and recover your Microsoft 365 data.



Take a closer look at HubStor

HubStor on Azure is a fully-managed solution, which means there's no added hardware and no cloud complexity for you to monitor and maintain. HubStor provides full support of Microsoft 365 Multi-Geo, allowing your HubStor tenant to reside in any Azure region automating compliance with regulations concerning data sovereignty. You can also choose to run HubStor in your own Azure account or use HubStor's.

With HubStor, you and your data are never locked in. You can cancel anytime with no penalties or hassles with migrating your data.

[Book demo](#)



HubStor Inc.
515 Legget Drive, Suite 800
Ottawa, ON K2K 3G4

Toll-free: 855-704-1737

sales@hubstor.net | www.hubstor.net