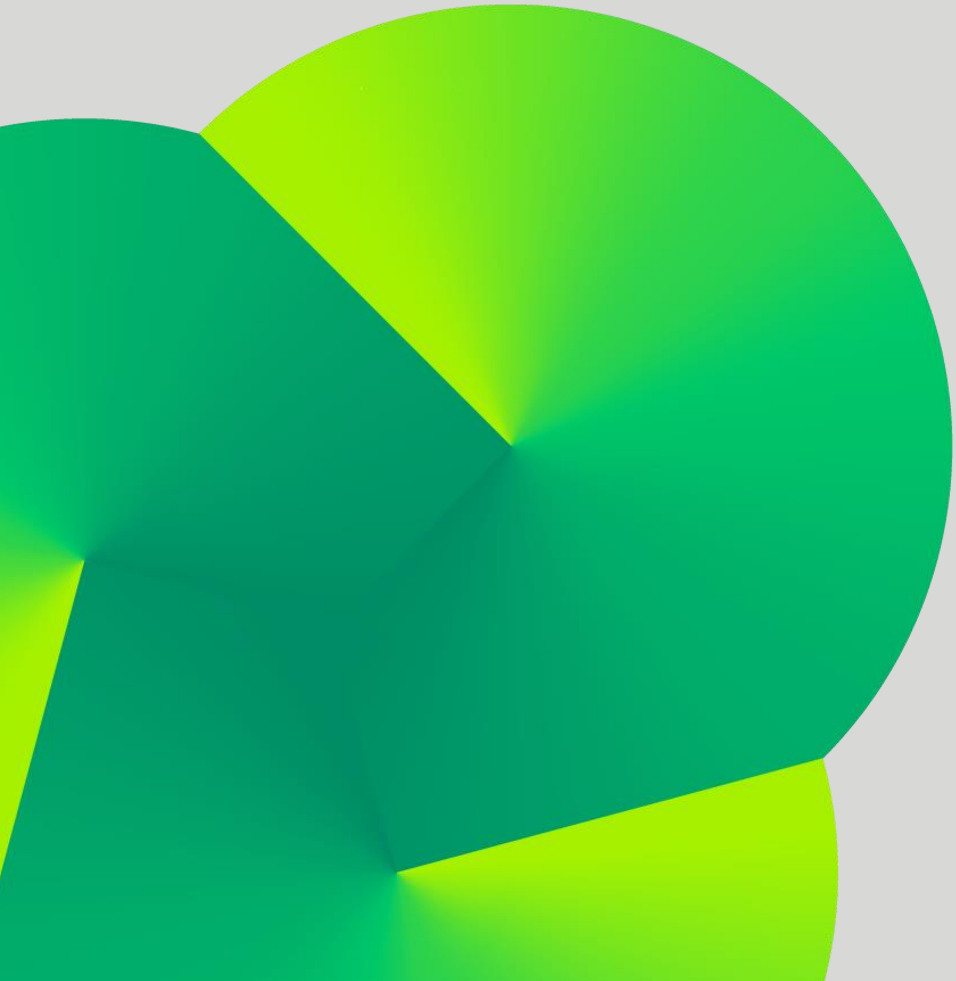
tesserent

MICROSOFT 365 BACKUP

Why you should consider backing up your Microsoft 365 data to a third-party backup service



Introduction

With many organisations using Microsoft 365 as their central collaboration and communication platform to effectively complete their business activities, the Microsoft 365 platform hosts your business-critical data, configurations, and workflows that could cause significant impact on your organisation if lost or corrupted.

Depending on the licensing model you have subscribed to, you may be eligible to access some native services provided by Microsoft that can provide some protection to your data using a retention policy. These services allow you to retain data even if deleted by the user within your Exchange, OneDrive, SharePoint, and Teams services.

Unfortunately, a retention policy only allows you to recover the data, but not the configuration or structure of a mailbox, OneDrive or SharePoint site. In addition, if an account becomes corrupt, infected by malware or breached by a ransomware attack, then this also impacts the data within the retention policy.

Read below to understand more why you should consider using a 3rd party backup service for your Microsoft 365 data.

Guidance from Microsoft

Microsoft will always endeavour to provide a safe and stable environment; however, they recommend using a 3rd party service to back up their services. Within the Service Availability section of the 'Microsoft Services Agreement'[1] which covers Microsoft 365 services, Microsoft states:

We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. ***We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services****.*

In addition, Microsoft recommend using a 3rd party backup service to recover from a ransomware attack on your Microsoft 365 environment in their published guide, *Recover from a ransomware attack in Microsoft 365*[2].

[1] https://www.microsoft.com/en-us/servicesagreement

[2] https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/recover-from-ransomware?view=o365-worldwide

Backup of Exchange Online Mailboxes

When you use a third-party backup service to backup mailboxes within your Exchange Online environment, it backs up the entire mailbox structure and any configurations within. If you need to perform a recovery of a mailbox, you will be recovering it in the same state it was in at the time of backup.

If you use the native Microsoft 365 retention policy rather than a third-party service, you would need to perform a search of a mailbox and then you would essentially perform an export (to a .PST file) of the search result in an unstructured format. This export can then be added to Outlook and imported.

This process typically exposes the organisation to the following risks:

- A .PST file typically has no security applied to it and if someone gets a hold of that file, potentially sensitive information is exposed.
- A .PST file consumes unnecessary storage space on servers and endpoint devices.
- The end-user is impacted even further by need to find emails in an unstructured format and import into the desired folder structure. This could take days to complete depending on the mailbox size.

In summary, it's a very messy and time-consuming process.

Backup of SharePoint Online and OneDrive

Very similar to Exchange Online mailboxes, data that resides within SharePoint and OneDrive can have a retention policy applied where a copy of the file is saved in a hidden location if the file is deleted by the end-user.

Unfortunately, deleted files will still contribute to your SharePoint Online or OneDrive quotas. For OneDrive this is typically not a problem due to a 5TB quota allowance with an E3 or above license, but for SharePoint Online this can be detrimental as quotas are limited to 1TB + 10GB per user. For example, if you have 200 users, this will limit you to 3TB in SharePoint Online storage. As such, using a retention policy can either limit your functional usage of SharePoint or require additional charges for more storage.

Additionally, SharePoint sites are often used for much more than just a file repository. If you lose a SharePoint site or site collection, it can easily be recovered with a 3rd party backup service with all the web parts, workflow, lists and files in place. A retention policy will only be able to recover your file items where you would still need to create the folder structure and save the files into locations where you hopefully can remember where they were.

Backup of Microsoft Teams

Teams has settings, configurations, and membership which all need to be protected and recoverable. A 3rd party backup solution can protect not only the data but also these settings and their associated interconnections between applications.

More than ever before, people are using Teams channels for projects and special initiatives at a rapidly growing rate. But once you complete a project, you probably need to keep a copy of the ended project for long-term needs such as legal and compliance requests. What often happens is that these Teams get mistakenly deleted or retention misapplied, which makes other files or essential documents unavailable.

Backups can also help in short-term scenarios. For example, if an employee says something inappropriate in a Teams conversation, but then deletes the message, having a backup would make those chats recoverable and available to HR for review. Third-party backup vendors not only provide protection from the unknown but can also offer a variety of ways to restore missing or accidentally deleted teams or channels.

Demanding RTO's and RPO's

If your company provides the managed services for the Microsoft 365 environment, then it's important to understand the 'Recovery Time Objective' and 'Recovery Point Objective' timeframes that are required to meet your agreed service levels.

If there is a mailbox or SharePoint site that is needs a full recovery, then it may take a day or two to recover it to the same state it was in before the incident if using a retention policy. If your service level agreements don't allow for a full day or two to recover, then you would need a 3rd party recovery service that that perform this recovery to meet your service levels (potentially in minutes depending on mailbox or site size).

Returning Employee

If your organisation likes rolling out the red carpet to returning employees by restoring their mailbox and OneDrive data upon return, and if they have been gone more than 30 days, this would not be possible with the native services in Microsoft 365.

With a 3rd party backup solution, this recovery can be done beyond 30 days and up to the period allowed within the 3rd party backup service[3].

[3] Depending on the service, this could be customised or pre-defined.

Managing Hybrid Email Deployments

Organisations that adopt Microsoft 365 typically need a window of time to serve as a transition window between on-premises Exchange and Microsoft 365 Exchange Online. Some even leave a small portion of their legacy system in place to have added flexibility and additional control. These hybrid email deployments are common yet pose additional management challenges.

If your organisation has mailbox data in both Microsoft 365 and an on-premises Exchange implementation[4], using a 3rd party backup service to backup both environments with a single backup system is recommended.

Self-Service Recovery

Microsoft by default will allow users to perform a self-service recovery for up to 14 days after the item is deleted where it can be configured on a per user level for 30 days. Some 3rd party backup services will allow users to recover items beyond the 30-day period as long as it has been included within a backup and has not exceed the backup retention period.

If your organisation requires a self-service recovery solution beyond 30 days, then a 3rd party service is needed. It is important however that you identify this as not all services provide this capability.

Compliance Scanning, Reporting and Rectification

Many organisations have legal and compliance obligations for standards such as PCI-DSS and PII data. While Microsoft 365 has Data Loss Prevention (DLP) policies that allow you to stop someone from emailing credit card information or sharing a file with PII data, it is rarely implemented with any restrictions to allow business continuity. Additionally, DLP policies can only protect at the time of sending an email or sharing a file. They won’t protect against data that already resides within your Microsoft 365 environment prior to the DLP policy implementation.

Some 3rd party back-up services provide the capability to scan for and complete a report on your backup data on anything that breaches the compliance regulations applicable to your organisation. With this report, it will allow you to reach out to these users to manually rectify or if desired connect to Microsoft 365 using the API and systematically remove any compliance breaches.

NOTE: This feature is typically requiring an add-on cost.

Where to store your data?

Depending on the 3rd party backup solution you choose to use, you may not have a choice of where the data is stored, however the storage location will always be provided by the 3rd party

[4] Only some 3rd party backup services can backup both environments.

Microsoft 365 backup provider. If the storage location is a concern, always check with the provider or your partner as to where this stored to help make an informed decision.

Some 3rd party Microsoft 365 backup solutions require you to provide the backup location, and in this scenario, the storage location becomes a bigger discussion point as you need to also understand the various implications of not only where you store your data, but what you store your data on. Some considerations for data storage include:

- If you are using a SaaS 3rd party Microsoft 365 Backup provider:
  - SaaS offerings will have a specific quota. Typically, this is a pooled quota where you get might get 50GB per user and therefore if you have 200 users, this becomes 10TB of storage to backup all of your data for the entirety of the retention period. Consider whether this is enough storage for you for the required retention period.
  - You can buy additional storage, but this extra cost may be the difference between this solution and another.
  - Confirm where they store the data and if this meets your compliance and DR requirements.
- If you are providing the storage for a 3rd party Microsoft 365 Backup service:
  - Using NAS storage will work but will likely have performance issues and is typically not recommended.
  - Block storage can meet performance needs, however, is expensive in comparison to Object storage or NAS storage.
  - Block storage may not allow compression of the data or application layer encryption.
  - Providing your own Object storage solution in general is very expensive and there would need to be other requirements to obtain value from it than just a backup of your Microsoft 365 data.
  - You could use Object storage within a public cloud provider such as AWS or Azure where you would save on costs and gain compression and encryption benefits, however there would be egress charges applied for any recoveries that need to be considered in your business case.
  - If storing in Azure, there is the risk that the disaster event requiring the backup may be impacting both Azure and Microsoft 365. If you are concerned about the very unlikely catastrophic event to Microsoft, then storing in Azure may not be the best option.

Summary

In the early days of Microsoft 365, it was widely considered a solution that you no longer needed to backup. Microsoft had enough built-in redundancy and protections to not require this anymore. However, as the Microsoft 365 service has matured and so too has the customers maturity in using the service and its associated capabilities, it has become clear that there are gaps in the native service offerings (no matter what license add-on you have).

Having a 3rd party backup service for Microsoft 365 is vital to any organisation that has business critical information stored in their Microsoft 365 environment for the following top 5 reasons:

1) Microsoft themselves are now recommending that 3rd party backup services are used, which is a significant change in the rhetoric from the early days when the service was first established.
2) If there is a malware or ransomware breach, having an external offsite copy is the easiest and sometimes only way to recover the data.
3) Recovering an Exchange mailbox is a slow, messy and insecure process using the native tools.
4) A SharePoint site or site collection cannot be recovered using the native tools, only the files stored within in an unstructured format can be meaning the folder structure, site design and any web part configurations will be lost.
5) You wish to restore returning employees data or have aggressive RTO’s and RPO’s to meet.

Tesserent recommends you work with a partner to determine your Microsoft 365 recovery requirements to assist you in determining the best fit backup service from both a functional and financial perspective. We can help you navigate these challenging topics and have a Microsoft 365 environment that is prepared for scenarios that range from a disaster or a simple recovery of a mailbox or SharePoint site.