ManageEngine
RecoveryManager Plus

Protecting data in your Microsoft 365 services

www.recoverymanagerplus.com

Table of Contents

Introduction

Data in your Microsoft 365 services is constantly replicated to multiple geographically-dispersed Microsoft data centers for data restoration in case of infrastructure failures on any data center. For large-scale failures, service continuity management procedures are initiated, and users will remain almost oblivious to these underlying issues.

Microsoft's geo-redundancy is well suited to deal with major infrastructure failures, but for smaller and higher probability events like accidental deletion or malware attacks, geo-redundancy does not offer much protection to data. Other native capabilities like Recycle Bin and OneDrive for Business Files Restore work to an extent, but there are still some gaps left by them. This is why Microsoft recommends its users to turn to third-party applications for complete data protection in its services agreement.

> 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.

This guide will analyze the reasons why the native Microsoft 365 features provided for data protection are not sufficient and what kind of tools you can equip yourself with to improve your data security.

Native data protection features

Microsoft 365 provides the following features to ensure data protection:

- Recycle Bin
- Retention policies
- Files Restore

Recycle Bin

Recycle Bin in Exchange Online, SharePoint Online, and OneDrive for Business helps administrators recover from accidental deletion of any kind.

The duration for which deleted objects are stored in the Recycle Bin is the same for SharePoint Online and OneDrive for Business, but different for Exchange Online. Let's see in detail about how Recycle Bin works in Exchange Online, SharePoint Online, and OneDrive for Business.

Exchange Online

Data in your Microsoft 365 services is constantly replicated to multiple geographically-dispersed Microsoft data centers for data restoration in case of infrastructure failures on any data center. For large-scale failures, service continuity management procedures are initiated, and users will remain almost oblivious to these underlying issues.

Microsoft's geo-redundancy is well suited to deal with major infrastructure failures, but for smaller and higher probability events like accidental deletion or malware attacks, geo-redundancy does not offer much protection to data. Other native capabilities like Recycle Bin and OneDrive for Business Files Restore work to an extent, but there are still some gaps left by them. This is why Microsoft recommends its users to turn to third-party applications for complete data protection in its services agreement.

SharePoint Online and OneDrive for Business

Deleted items in your SharePoint Online and OneDrive for Business sites are moved to the Recycle Bin where they are retained for a period of 93 days. If users empty their Recycle Bin before 93 days, the items are moved to the second stage Recycle Bin (site collection Recycle Bin) where they are retained for the remainder of the 93 days. Once the 93 days are up from the date of deletion, the items are purged from Microsoft 365 and cannot be recovered by the user or administrator.

It does not matter if the item is in the user's Recycle Bin or the site collection Recycle Bin at the end of 93 days, as the data will be purged regardless.

As a final protective layer for the data in your SharePoint Online and OneDrive for Business sites, Microsoft 365 retains its own copy of all site contents for an additional 14 days beyond the 93 days. Administrators can contact Microsoft Support to request a restore any time within this 14-day window.

These factors show that Microsoft's Recycle Bin feature is a way to recover from accidental or malicious deletions, but it's not a comprehensive solution that can work at all times.

Retention polices

Microsoft 365's Litigation Hold provides administrators with a way to secure mailbox and site data. When a Litigation Hold is deployed on a mailbox or a site, no content can be permanently deleted by the users. However, retention policies are only secure until your privileged accounts are hacked or your administrators turn rogue. If either of these unfortunate cases were to happen, the retention policies can be turned off using the administrator credentials and content can be deleted.

To combat this, Microsoft provides a feature called Retention Lock or Preservation Lock that ensures no one, including administrators, can turn the retention policy off or make it less restrictive. Once a retention policy is created, it cannot be modified to make the policy lenient. However, Preservation Lock allows administrators to widen the scope of a retention policy by adding locations or extending its duration. Preservation Lock prevents people with malicious intentions from undoing the retention policy.

The downside of Preservation Lock is that this change can never be undone. A restrictive and wide Retention Lock can quickly result in your allotted storage space being filled up, and you might be forced to buy additional storage space from Microsoft.

Depending on the size of your organization and the volume of data that your company stores in SharePoint Online, you might end up spending quite a bit on storing all your data.

Files Restore

Microsoft 365 provides you the ability to roll back all files and folders in OneDrive for Business sites to a previous time. This feature allows you to recover from large-scale disasters like ransomware and malware attacks on your OneDrive for Business sites.

Even though Microsoft provides a way to detect ransomware and recover from it, it also lists a few limitations of this feature.

- Files Restore uses version history and the Recycle Bin to restore OneDrive, so it's subject to the same restrictions as those features. When version history is turned off, Files Restore won't be able to restore files to a previous version.
- Deleted files can't be restored after they've been removed from the site collection Recycle Bin by manual deletion or emptying the Recycle Bin.
- Albums are not restored.
- If you upload a file or folder again after deleting it, Files Restore will skip the restore operation for that file or folder.

Other issues to consider

Employee turnover and data retention

When an employee leaves your organization, removing the Microsoft 365 license associated with the user starts a countdown. 30 days after the mailbox is unlicensed, all data in the mailbox will be deleted permanently.

If you wish to hold on to the data in these unlicensed mailboxes, there are a few options: assigning a license to the mailbox, making the mailbox a shared mailbox, or exporting it to PST format. Each method has its own limitations when using native tools.

- Assigning an Microsoft 365 license to the mailbox of a user has left the organization leads to unnecessary costs.
- Making the user's mailbox a shared mailbox has these limitations:
  - If you use Exchange Online Kiosk licenses, you cannot access shared mailboxes.
  - Shared mailboxes have a size limit of 50 GB, if the size exceeds the limit, you'll have to apply a license to the mailbox to keep using it.

    A shared mailbox doesn't have a username and password. To access a shared mailbox, users' have to be given access to it. Granting access to individual mailbox folders in the shared mailbox is not possible.
- Exporting to PST is a much more convenient option, but then again, there are a fair few limitations to this as well. The export to PST often creates duplicated items.
  To overcome this, Microsoft provides an **Enable deduplication** option, but that option has several limitations, too.
  - The deduplication feature might mistakenly identify a message as a duplicate and not export it (but still cite it as a duplicate in the export reports).
    These are messages that a user edits but doesn't send.
  - Unique messages can also be marked as duplicates when the Copy-on-Write page protection feature is enabled, as in the case of a mailbox being on Litigation Hold or In-Place Hold. The Copy-on-Write feature copies the original message (and saves it in the Versions folder of the user's Recoverable Items folder) before the revision to the original item is saved. In this case, the revised copy and the original message (in the Recoverable Items folder) might be considered duplicate messages and therefore only one of them would be exported.

Compromised privileged accounts

Losing access to privileged accounts is catastrophic. As we've seen so far, Microsoft's native methods can recover Microsoft 365 data from small-scale data deletions as administrators can use the second-stage Recycle Bin to recover deleted items. But, an account with elevated privileges can also wipe out all data in the second-stage Recycle Bin, and at that point, the data cannot be recovered using native tools.

An effective data protection solution for your Microsoft 365 data

All these problems can be overcome by deploying a robust Office 365 backup solution.

A backup solution for your Microsoft 365 environment ensures you always have a copy of your data from which you can restore any data you need at any time. ManageEngine RecoveryManager Plus is an Microsoft 365 backup solution that allows you to back up all items in your Exchange Online mailboxes and SharePoint Online and OneDrive for Business sites. The backup data is stored within your premises and is entirely under your control, which makes it easy to hold the backup data for as long as you need.

With RecoveryManager Plus, you can:

- Restore Exchange Online mailbox or SharePoint Online and OneDrive for Business items in a few simple clicks, no matter how long ago the item was deleted.
- Define a custom retention policy for your Office 365 backups and automatically discard backups when the retention limit is reached.
- Restore entire OneDrive for Business files and folders to any backed-up point without any limitations.
- Easily back up or export mailboxes to PST format of employees who recently left your organization, and store them for as long as you need.

Conclusion

Organizations deploy Microsoft 365 for the stability and convenience of a cloud-based service that enables employees to work from anywhere and anytime. It also satisfies most business' requirements when it comes to security, data protection, archiving, and service availability.

However, Microsoft 365 still does not provide much in terms of data protection, as all it takes is a privileged account getting hacked or an administrator going rogue to wipe all the data from your services. A robust backup solution that can back up and restore all mailboxes in your Exchange Online and sites in your SharePoint Online and OneDrive for Business is crucial if you're looking to migrate to Microsoft 365 completely.