ManageEngine
RecoveryManager Plus

9 reasons

why you need to back up your Microsoft 365 data

Introduction

Data in Microsoft 365 is continuously replicated to multiple, geographically-dispersed data centers; this ensures data is safe even if infrastructure failure occurs in one data center. In the event of large-scale failures, service continuity management procedures are initiated, enabling users to remain productive and almost oblivious to these underlying issues.

So with all these protective measures in place, do you really need to back up Microsoft 365 data?

The short answer is yes. Microsoft itself explicitly recommends users back up all Microsoft 365 data in section 6.b of the Microsoft 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 further explore the reasons why you need to back up your Microsoft 365 data, and how having a robust Microsoft 365 backup solution can help prevent data loss in the event of an outage.

Reasons to back up Microsoft 365

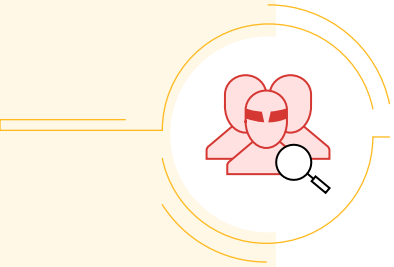
1. Accidental deletion

Microsoft 365's geo-redundancy feature is designed to keep your data safe by storing it in a separate physical location in case one site fails. However, this feature also causes any deletion to be replicated across all other geographic locations, and the deleted data will be removed from all Microsoft 365 data centers.

Microsoft 365 provides a Recycle Bin for its Exchange Online, SharePoint Online, and OneDrive for Business services that's useful for recovering items from accidental deletion, but there's a caveat: The Recycle Bin has a limited window within which you can restore the deleted items.

- Deleted Exchange Online items are stored in the Recycle Bin for a maximum of 30 days (120 days max for calendar entries).
- Deleted SharePoint Online and OneDrive for Business files and folders are stored in the Recycle Bin for a maximum of 93 days.

Once the retention period expires, deleted items can't be recovered. On the other hand, a backup solution provides the flexibility of backing up your Microsoft 365 data and storing it indefinitely until you need it.

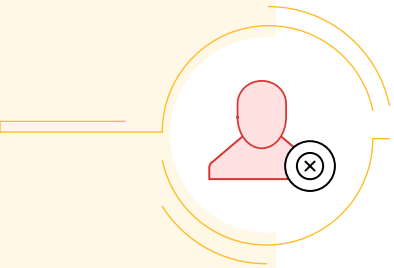


2. Insider threats

According to the Ponemon Institute 2018 Cost of Insider Threats study, the average cost of an insider-related incident is around $513,000. Insider-related incidents can cost a company up to $8.76 million a year, and in North America, the number rises to $11.1 million a year.

Critical data being deleted or modified by a disgruntled employee can financially impact an organization if the data is not recovered instantly. In some cases, the malicious action might have gone undetected for a long time; by the time it's found out, it might be too late to recover any lost data.

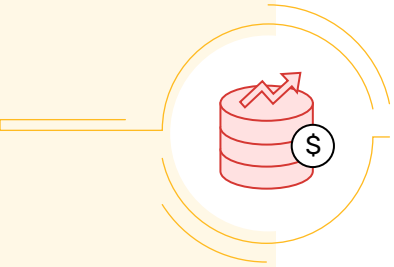
Having a backup solution that frequently backs up your data not only protects you from malicious attacks from the outside, but also insures you against actions performed by your own employees, whether intentional or not.



3. Compromised privileged accounts

Losing control over privileged accounts is potentially catastrophic. With elevated privileges, data can effectively be completely erased from your Microsoft 365 environment. Further, removing data from the second stage Recycle Bin in Exchange Online, SharePoint Online, and OneDrive for Business can make recovering those emails and files impossible.

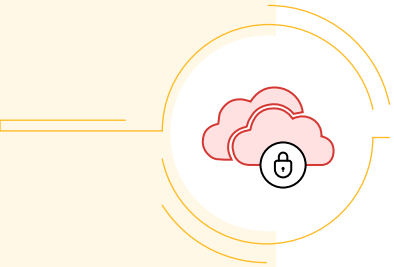
With a powerful backup solution and periodic backups, data can be easily retrieved and you can reduce the recovery point objective (RPO) of your Microsoft 365 environment.



4. Increasing cost of additional storage

Storing all Microsoft 365 data without deletion increases the size of your Exchange Online and OneDrive for Business environments over time. When data in your mailboxes and sites exceeds the storage limit of your plan, you'll have to pay to upgrade to a plan with more storage.

With a backup solution, you'll always have a copy of the data to restore it at a moment's notice, eliminating the need to pay for higher subscription plans.



5. Ransomware and malware entry via OneDrive Sync Client

Microsoft's OneDrive Sync Client is a tool that can sync your OneDrive data from the cloud to your desktop and vice versa. While this tool provides employees the flexibility to work from anywhere and at any time, there is one vulnerability that can pose a ransomware threat.

If a ransomware attack on your system infects the files in your synced copy of OneDrive for Business, the data will be synced back to the cloud, and all the data in your OneDrive for Business environment will also be infected. 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—neither by manual deletion or by emptying the Recycle Bin.

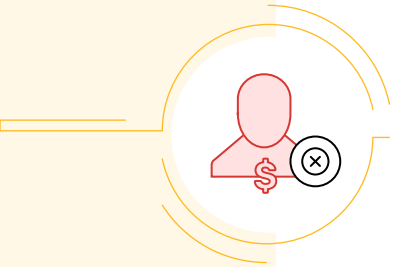
- Albums are not restored.
- If you upload a file or folder again after deleting it, Files Restore will skip the restore operation for that file or folder.

Having a backup and recovery solution eliminates all these limitations and empowers you to easily recover from any ransomware attack.

6. Ransomware attacks on Exchange Online mailboxes

Most of us are familiar with ransomware attacks on documents, but ransomware attacks on emails are new to the industry. According to Datto's Annual Ransomware Report, of the more than 2,400 MSPs surveyed, 28 percent claim to have seen ransomware attacks in SaaS applications. Of those, nearly half of respondents reported seeing attacks in Microsoft 365 specifically, with 22 percent reporting G Suite attacks. These attacks vary from regular ransomware attacks syncing to cloud applications, to the more sinister infections that are made specifically for the cloud.

For this exact reason, having the ability to recover all your Microsoft 365 emails at once is something that every organization has to have.



7. Inactive users can cost you a fortune

When employees leave the organization, it's necessary to store all their emails and documents in case they're needed in the future. Unless an Microsoft 365 license is applied to the user, all data associated with that account will be deleted from Microsoft 365 servers after a fixed period of time determined by Microsoft.

Instead of paying for inactive user licenses, organizations should use backup software to compress and securely store that user data for as long as needed.

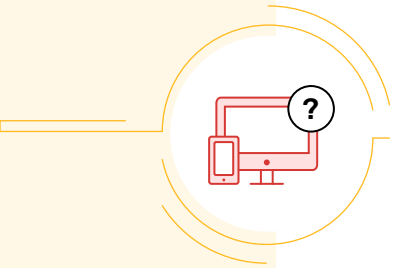
8. Preservation Lock

An important thing to understand about retention policies is that any additional version of a file counts towards the storage used by your Microsoft 365 account. Additionally, retention policies are only effective if you enable Preservation Lock.

Preservation Lock is an Microsoft 365 feature 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 more 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 make you quickly fill up your allotted storage space, and you might be forced to buy additional storage space from Microsoft.

On the other hand, a third-party backup solution provides the flexibility to maintain a copy of all files while still using minimal storage space in Microsoft 365.



9. Lost or stolen devices

The major advantage of Microsoft 365 is the flexibility it provides, enabling remote work as long as you have an internet connection and a device from which to access it. While this is a good thing for organizations in terms of improving the productivity of employees, IT teams have to be increasingly vigilant to secure these additional devices.

Lost or stolen devices containing logged-in applications can lead to data mishaps, and administrators need to be able to remotely wipe these devices to prevent data breaches. Having regular backups will allow you to restore all data back to the user when they get a new device.

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus | M365 Manager Plus

ManageEngine
RecoveryManager Plus

ManageEngine RecoveryManager Plus is a comprehensive backup and recovery solution that empowers administrators to back up and restore their Active Directory, Entra ID, Microsoft 365, Google Workspace, on-premises Exchange and Zoho WorkDrive environments. With its incremental backups, flexible retention policies and multiple modes of restoration—such as domain controller recovery and object-, item- and attribute-level restoration—RecoveryManager Plus delivers a holistic solution for backing up data that is critical for your enterprise to function.
For more information, visit www.manageengine.com/ad-recovery-manager.

$ Get Quote Download