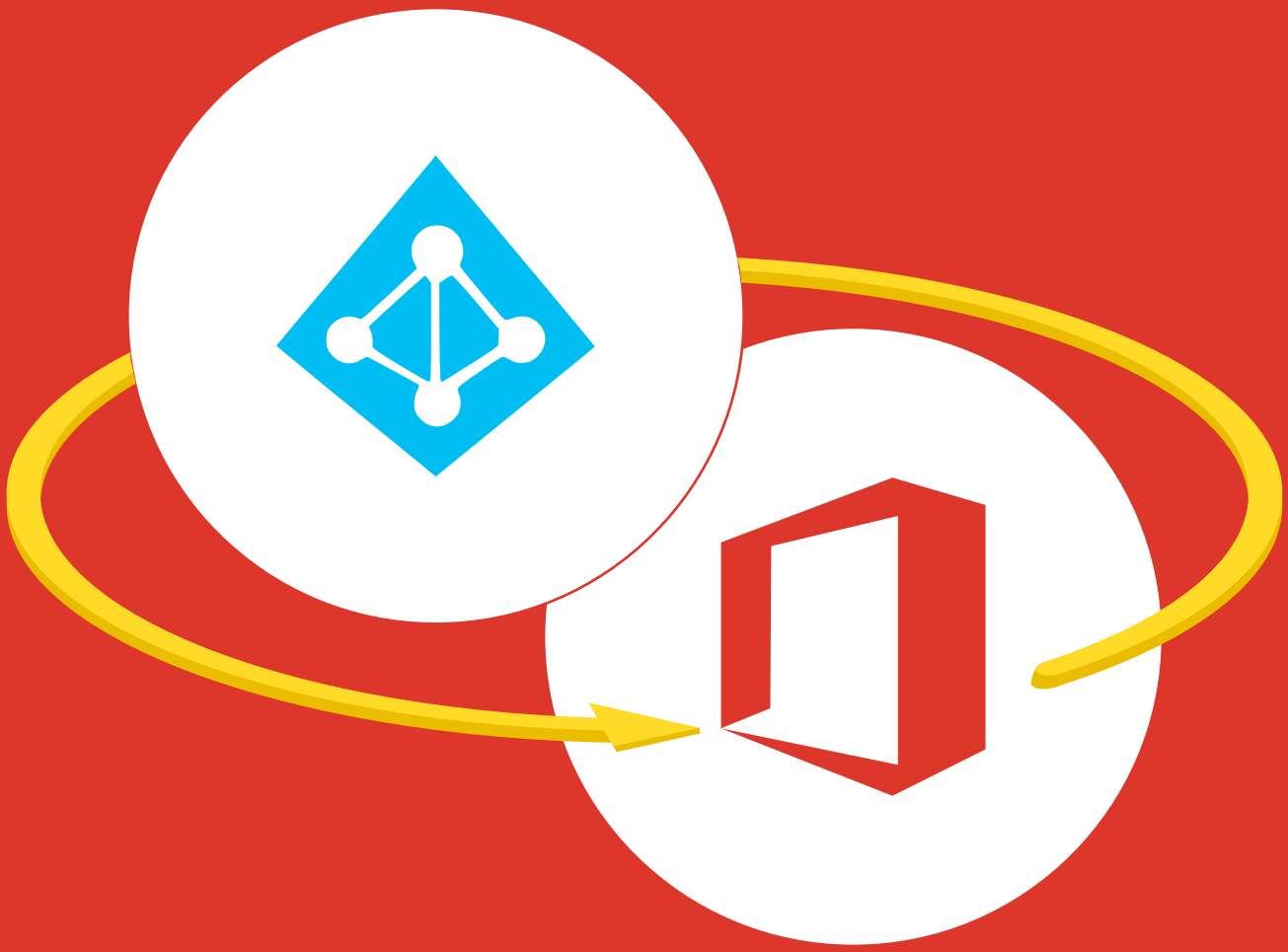
5 reasons

why you need an enterprise data protection solution



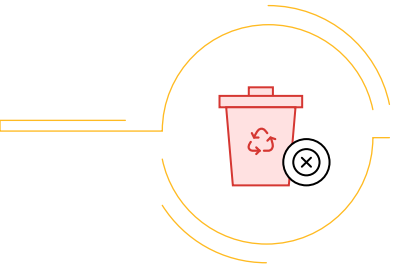
ManageEngine
RecoveryManager Plus

Introduction

Data protection is unarguably the most important cybersecurity setting in the IT admin world. However, most of the time, data protection takes the back seat when planning the cybersecurity posture. Why? This disconnect is because most of us do not understand the actual benefits of having an effective data protection solution in place.

This guide will explore the reasons you need a data protection solution for Azure AD and Microsoft 365 data, and how it can help prevent data loss in the event of an outage.

Reasons to use an enterprise data protection solution



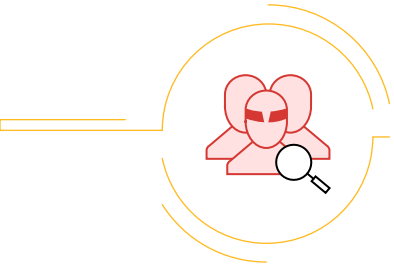
1. Accidental deletion

Microsoft keeps your data safe by storing it in multiple physical locations 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 data centers.

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

- Deleted Azure AD items are stored in the Recycle Bin for a maximum of 30 days.
- Deleted Exchange Online items are stored in the Recycle Bin for a maximum of 30 days (120 days 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.

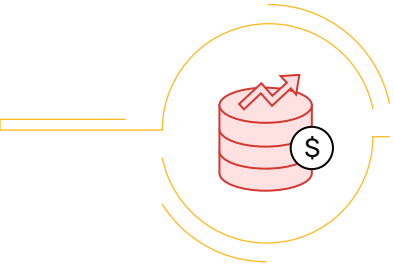
On the other hand, a data protection solution provides the flexibility of backing up your Microsoft 365 data and storing it indefinitely until you need it.



2. Insider threats

Critical data being deleted or modified by a rogue administrator or someone masquerading as an administrator can negatively impact an organization if the data is not recovered instantly. Since the native recycle bin comes with a timer, if you don't happen to notice the items were deleted in time, you won't be able to restore them down the road when you find out they've been deleted.

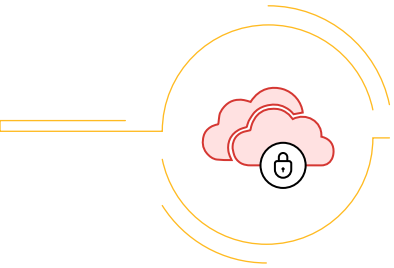
Having a data protection solution that frequently backs up your data not only protects you from malicious outsider attacks, but also secures you against actions performed by your own employees, whether intentional or not. You can reduce the recovery point objective of your Azure AD and Microsoft 365 environment and stop worrying about lost credentials or rogue employees.



3. Increasing cost of additional storage

Storing all Microsoft 365 data increases the size of your Exchange Online mailboxes and OneDrive for Business sites over time. When data in your mailboxes and sites exceeds the storage limit of your plan, you'll have to upgrade to a plan with more storage, which can quickly rack up costs.

With a data protection solution, you'll always have a copy of all your data and can restore it in a moment's notice, eliminating the need to pay for higher subscription plans. You can maintain lean mailboxes and sites and restore data as and when needed.



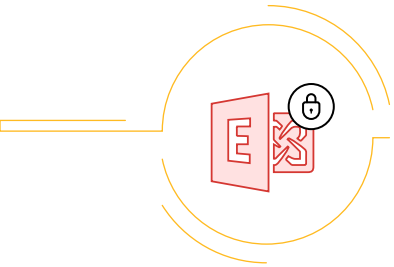
4. Ransomware and malware entry via OneDrive sync client

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 gives employees the flexibility to work from anywhere and at any time, there is one major vulnerability that poses 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 nor 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 data protection solution eliminates all these limitations and empowers you to easily recover from any ransomware attack.



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