COHESITY

TIPSHEET

5 reasons you need a third-party solution to back up Microsoft 365

Overview

Microsoft 365 (M365) is one of the most widely used office productivity SaaS applications, with nearly 350 million commercial monthly users.[1] But just because M365 files and data live in the cloud doesn't mean they're safe or always available. Your organization needs to ensure you can recover files that may have been deleted from a ransomware attack or a careless employee. Or perhaps you need to meet legal and compliance retention requirements.

Here are the top 5 reasons you need a third-party backup solution to keep your data safe and available whenever you need it.

1. Your enterprise data in the cloud is your responsibility.

Moving to the cloud offloads the headaches associated with on-premises IT infrastructure management, security, and upgrades. Yet it's still up to your IT staff to ensure enterprise data can be recovered at all times and brought back quickly when needed. Microsoft 365 hosts your data in the cloud, but backing it up is your responsibility. Cloud service providers (in this case, Microsoft) focus on service uptime and availability, but as a customer of its cloud service, the onus is on you to safeguard your business data. You need a backup and recovery solution that will protect your data wherever it lives—including in the cloud.

2. Native tools provide limited flexibility for data retention and recovery.

M365's Exchange Online, SharePoint Online, OneDrive, Teams, and Groups come with basic native data retention options, but their flexibility is limited and may not align with your business-level SLAs (for example, deleted email mailboxes are only saved for 30 days). Beyond these basic settings, litigation hold and/or retention policies can be kept as long as needed, but getting the data back can be time consuming and complex. You need to ensure that your backup service has flexibility and provides simple processes for storing and retrieving data to meet your compliance and business needs. A third-party backup service offers greater flexibility, so when you need to restore deleted items to any point in time, you can do so quickly and easily.

Microsoft 365 native protection policies at a glance

Here's how long Microsoft 365 keeps your items by default with their built-in settings:

- Exchange Online
  - 14 days, or up to 30 days if configured
  - 30 days for deleted email boxes
- OneDrive
  - 93 days for site collection Recycle Bin
  - 30 days for a user's Recycle Bin
  - Recovery of data back to a point in time up to 30 days, if configured
- SharePoint
  - 93 days for site collection Recycle Bin
  - 30 days for a user's Recycle Bin
  - Retains backups of deleted items for an additional 14 days
  - Admins can recover deleted site collections and contents up to 90 days
- Teams
  - 1-7 days for messages
  - Other data types have limited retention based on the services providing them

1 Microsoft Earnings Release FY22 Q3

3. Your employees expect a rapid response when data is lost or compromised.

Employee productivity matters, and your workers count on always-available access to their data. When it goes missing, gets deleted, or is infected, they expect your IT team to respond rapidly to restore critical business data. What's your plan to quickly get SharePoint, OneDrive, and Exchange data back to a last known-good state? What if you need to recover just an individual folder or drive, or a single message from an entire mailbox? Can you find what you need quickly? How long does this take you today? Unfortunately, native options may let you down. Here's what won't let you down: an enterprise-class backup and recovery solution that ensures your IT team can granularly get data back quickly so Recovery Time Objectives (RTOs) are met or even exceeded. Imagine providing an exceptional user experience so employees can get back to work fast.

4. Office data has become a ransomware target.

If your enterprise relies only on native data protection, you may be out of luck if and when ransomware strikes—and you need to recover at scale. A recent Ponemon Institute report puts the average cost of a single ransomware attack at $5 million due primarily to productivity loss, system downtime, and information theft. And the attackers are likely after your backup snapshots and production data. You need a backup and recovery solution that ensures immutability of backup data and responds at scale to ransomware attacks, so you can quickly recover and restore data across your global data footprint—including from and to public clouds.

5. Chances are, you have more than just M365 data to protect.

The last thing busy IT operators need is yet another backup silo to look after. You likely have other SaaS and homegrown cloud applications using cloud infrastructure and platform services that you need to protect. You may even have more remote office/edge locations that need protection. And chances are you still have some critical applications that run on-prem, such as VMware, Oracle, or others. To protect all these holistically, you need a modern backup solution that consolidates protection for a wide range of data sources no matter what they are and where they're deployed. Ideally, this comes from a single platform—all managed through a single UI—to keep your life simpler. No one wants (or has time) to manage a patchwork of solutions.

SaaS or self-managed: have it your way with Cohesity

You moved to the cloud and adopted SaaS to simplify operations, so it's time to get true flexibility with an as-a-service approach to data protection. Cohesity offers modern backup and recovery for M365 through our DataProtect software, and you can choose how to take advantage of it. You may want to manage your own infrastructure to protect cloud data sources such as M365, or you may prefer to start protecting Microsoft 365 data through a backup-as-a-service (BaaS) model. Shift to on-demand capacity and Opex spending? Check. Eliminate on-prem infrastructure and get automatic software updates? Check. Any way you go with Cohesity—whether as a service, self-managed, or a combination of the two—you can easily manage your backups through a single global UI.

Enable Work Anywhere. Protect Microsoft 365 Data Everywhere.

An old adage reminds us not to put all of our eggs in one basket. Take that advice when it comes to choosing between native and third party data protection options. With Cohesity you can keep all your Microsoft 365 data backed up and safe—on-premises or in the cloud—with an end-to-end, modern backup and recovery solution that gives you easy, granular, instant recovery when you need it most.

Download this M365 Ransomware Protection guide to learn more about backing up and protecting your M365 data.

COHESITY