

5 Reasons Your Business Needs to Consider a Third-party Solution to Back Up Microsoft 365



Overview

Enterprises are increasingly adopting Microsoft 365 for email and calendaring, file storage and sharing, and teamwork and communication, with nearly 300 million¹ commercial monthly active users relying on it today. Using such cloud-based productivity solutions, your organization is creating and interacting with more unstructured business data than ever before. The most popular products in Microsoft 365 include Exchange Online, SharePoint Online, OneDrive, Teams and Groups and you should know the business reasons your company needs to back them up. Whether your industry is highly regulated or not, you must protect and manage that data to:

- ensure you can recover files that users may have mistakenly (or maliciously) deleted
- meet legal and compliance retention requirements
- successfully recover from cyber attacks such as ransomware

Just because it lives in the cloud doesn't mean it is safe or always available when you need it most.



1. Your enterprise data in the cloud is your responsibility

Moving to the cloud offloads on-premises IT infrastructure management, security, and upgrade headaches. Yet it's still up to your IT staff to ensure enterprise data can be recovered at all times and get it back quickly when needed. Microsoft 365 hosts your data in the cloud, but backing it up is your enterprise's responsibility. Cloud service providers (in this case, Microsoft) focus on uptime and availability, however as a customer of its cloud service, the onus is on you to safeguard your business data. The right modern backup and recovery solution will protect your data everywhere—both in the cloud and in your data center—with the option to be consumed as a service or deployed as software—all managed through a single UI.

The Growth of Microsoft 365

- Microsoft 365 has nearly 300 million commercial monthly active users¹
- Microsoft 365 generated 38 billion collaboration minutes in a single day¹
- Microsoft Teams reached 145 million daily active users¹

¹ Microsoft FY21 Third Quarter Earnings Conference Call, April 27, 2021



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

There are many reasons organizations keep their data from internal needs to legal and compliance reasons. Microsoft 365's Exchange Online, SharePoint Online, OneDrive, Teams and Groups come with some 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. Also, the minimum (default) setting for Deleted Item Recovery/Retention is just 14 days and the maximum is 30. Beyond these basic settings, litigation hold and/or retention policies can allow mailboxes and their data to be kept as long as needed, but getting the data back can be time consuming and complex. A modern backup service with flexibility and simple processes for storing and retrieving data to meet your compliance and business needs.



3. Your workforce expects 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 and meet business level SLAs. What's your plan to get SharePoint Online and OneDrive content repositories, and Exchange Online mailbox data back to a last known-good state? What if you need to recover just an individual folder or drive, a single message from an entire mailbox; can you find it quickly for recovery? How long does this take today? What's needed is a tightly integrated enterprise-class backup and recovery solution with Microsoft 365 that ensures your IT team can get data granularly from user accounts back quickly so that Recovery Time Objectives (RTOs) are met or even exceeded, providing an exceptional user experience that gets employees back to work fast.



4. Office data has become a ransomware target

If your enterprise relies only on the native data retention and versioning features you may be out of luck when a ransomware attack happens. M365 emails are a primary target for phishing which is a common way for ransomware to infiltrate and infect your systems. A recent Ponemon Institute report puts the average cost of a single ransomware attack at \$5 million due primarily to productivity loss,

systems downtime, and theft of information. What's needed is a backup and recovery solution that ensures immutability of backup data and responds at scale to ransomware attacks—allowing you to 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

And the last thing busy IT operators need, is another backup silo to look after. You have other SaaS and homegrown cloud applications that are using cloud infrastructure and platform services that you also need to protect. You have more remote and edge locations now more than ever that also needs protection. And you still have some critical applications on-premises whether it be VMware, Oracle, or others. What you need is a modern backup solution that's built on a single platform and managed through a single UI that protects and consolidates all your data sources no matter what they are and where they are deployed.

Consider backing up your SaaS data with Backup as a Service

You moved to the cloud and adopted SaaS to simplify operations, so why not take an as a Service approach to protect it? Cohesity offers modern backup and recovery for M365 through our DataProtect software and we give you a choice of how to take advantage of it. Some may want to manage their own infrastructure to protect cloud data sources such as M365, while many others may find that the quickest way to start protecting Microsoft 365 data is 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 - self-managed, as a Service, or a hybrid combination of the two, you'll be able to 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 and keep all of 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.

[Download this guide](#) to learn more about backing up and protecting your data in Microsoft 365.

COHESITY

© 2021 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.