COHESITY

TIPSHEET

4 Reasons Your Business Needs to Back Up Microsoft 365

Overview

Enterprises are increasingly adopting Microsoft 365 for email, collaboration and managing their unstructured data in the public cloud, with more than half of all businesses relying on it today. Using the cloud-based productivity solutions, your organization is creating and interacting with information anywhere, anytime, leading to more business data than ever. Your enterprise must oversee and protect all of that data everywhere it goes—whether your industry is regulated or not. There are different products in Microsoft 365, but because Exchange Online, SharePoint Online, OneDrive, Teams and Groups are the most popular, you should know the business reasons your company needs to back them up.

The Growth of Microsoft 365

- More than half of all businesses use Microsoft 365
- Microsoft 365 has 258 million commercial monthly active users[1]
- Microsoft leads the world in enterprise cloud revenue
- Microsoft Teams reached 115 million daily active users[2]

1. Cloud data 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 protect your data at all times—wherever it lives—and get it back quickly when needed. Microsoft 365 hosts your data in the cloud, but backing up your data is your enterprise's responsibility. Cloud service providers (in this case, Microsoft) focus on high availability, so as a customer of its cloud service, the onus is on you to safeguard your business data. The right web-scale backup and recovery solution will protect your data everywhere—both in the cloud and in your data center—without using bolt-on cloud gateways and multiple user interfaces leaving you scrambling to recover to any point in time.

2. Limited flexibility for data retention and recovery

There are many reasons organizations keep their data, ranging from internal needs to legal and compliance requirements. Microsoft 365's Exchange Online, SharePoint Online, OneDrive, Teams and Groups come with some native data retention options, yet their flexibility is limited and some of their advanced options can be hard to use. For example, look at the email defaults: Deleted mailboxes aren't saved beyond 30 days. 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 solution will couple flexibility with simple processes for storing and retrieving data to meet your compliance and business needs.

[1] Microsoft FY20 Third Quarter Earnings Conference Call, April 29, 2020.

[2] Microsoft Blog, author by: Jared Spataro, Corporate Vice President for Microsoft 365. October 28, 2020.

3. Your workforce expects a proactive response when data is lost or compromised

Employee experience matters and your workers count on always-available access to their data. When information goes missing, gets deleted, or is infected, they expect your IT team to respond fast. What's your plan to get SharePoint Online and OneDrive content repositories, and Exchange Online mailbox data back to a known-good state, and if needed, to recover an individual folder or drive, a single message or an entire mailbox? Microsoft's built-in data protection doesn't guarantee data is retained because it requires that employees change their behaviors, and we all know how hard that is. What's needed is a Microsoft 365-compatible enterprise-class backup and recovery solution that ensures your IT team can get data from user drives and mailboxes back quickly so that Recovery Time Objectives (RTOs) are met and even exceeded, while also providing an exceptional user experience that gets employees back to work fast.

4. Email has become a ransomware target

If your enterprise relies on legacy backup that require synthetic fulls and falls victim to a ransomware attack, your IT team can spend days (even weeks!) in recovery mode. 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 responds fast to ransomware attacks and lets you quickly locate and delete infected files across your global data footprint – including the public clouds. Also needed is instant mass restore capabilities, which enable recovery of hundreds of virtual machines instantly, at scale, and to any point in time.

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 enterprise's Exchange Online, SharePoint Online, OneDrive, Teams and Groups data backed up and safe—on-premises or in the cloud—with an end-to-end, web-scale backup and recovery solution that gives you easy, granular, instant recovery when you need it.

Download this eBook to learn more about backing up and protecting your data in Microsoft 365.

COHESITY