MYTH VS. REALITY

WHAT YOU NEED TO KNOW ABOUT MICROSOFT 365 BACKUP

INTRODUCTION

PERCEPTION IS NOT REALITY. MANY ORGANIZATIONS THAT USE SAAS APPS LIKE MICROSOFT 365 OPERATE UNDER A COMMON MISCONCEPTION THAT IT'S THE SAAS VENDORS' RESPONSIBILITY TO PROTECT THE DATA AND THAT SAAS BACKUP ISN'T NECESSARY. THIS IS THE RESULT OF CRITICAL KNOWLEDGE GAPS SURROUNDING MICROSOFT'S ROLE IN DATA PROTECTION.

SaaS providers, such as Microsoft, have best-in-class security and disaster recovery capabilities to protect against infrastructure threats, including hardware and software failure, power outages and natural disasters. However, they do not protect you from some of the leading causes of SaaS data loss such as:

HUMAN ERROR

Employees can overwrite important files or delete business-critical information, whether knowingly or unknowingly.

RANSOMWARE

The same tools that make SaaS apps great collaboration platforms also enable easy propagation of ransomware.

SYNC ERRORS

A third-party app sync error can ruin valuable SaaS data with no option to undo it.

INSIDER THREATS

SaaS vendors have no way to identify intent. If an authorized user makes a deletion request, it is viewed as legitimate, making employees and compromised credentials effective cyberattack vectors.

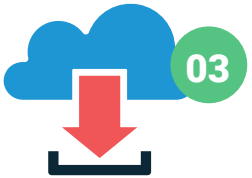
DEMYSTIFYING MICROSOFT 365 MYTHS

MICROSOFT 365 IS A HIGHLY SECURE PLATFORM

Microsoft data centers are protected by state-of-the-art security infrastructure, which make them virtually impossible to breach directly. However, architectural and functional aspects of Microsoft 365 make you vulnerable to compromise and data loss due to human mistakes, programmatic errors, malicious insider activity, phishing, malware and ransomware attacks.

DATA PROTECTION IS MICROSOFT'S RESPONSIBILITY

Microsoft follows the "Shared Responsibility Model" where they are responsible for application uptime and availability, while you, on the other hand, are responsible for the protection of your data.



BACKUP FOR MICROSOFT 365 ISN'T NECESSARY

While Microsoft 365 has built-in features like Recycle Bin and shadow copies to store deleted data, these are temporary archival solutions and are not comparable to a backup solution.

HOW DATA LOSS OCCURS IN CLOUD APPLICATIONS

REALITY

Data loss can occur in cloud-based applications, including Microsoft 365.

Microsoft 365 and the cloud do not prevent data loss caused by users. Estimates suggest that at least 80% of businesses using SaaS have lost their data at some point.[1]

REALITY

Deleted items in Microsoft 365 will be permanently removed after 14 days.[2]

Deleted or corrupted items in Microsoft 365 may be unrecoverable before anyone realizes the needed files are missing. The average time it takes from compromise to detection is 228 days.[3] Expanded Microsoft 365 licenses and features offer some archiving tools but do not protect against deletion. Plus, with Microsoft 365 alone, there's no fast, easy way to restore content exactly as it was and where it was to help you get back on track quickly.

Exchange Online, SharePoint Online and OneDrive for Business are some of the common SaaS applications businesses rely on every day. But without a smart backup plan, finding and restoring lost Microsoft 365 data can take hours, days or even longer.

REALITY

Without a robust backup solution, the time and cost of restoring lost data can be extreme.

Estimated time to restore data from Microsoft 365:

Read on and learn how to broaden your backup and recovery plan to include purpose-built protection for Microsoft 365.

EMAIL

SEARCHING FOR A LOST EMAIL CAN TAKE HOURS.

REALITY

Finding and restoring a lost email via Microsoft 365 can take hours.

Key business decisions, project planning, file sharing and other employee-generated data that run your business are often communicated over email. With many workers connected via email for extended hours each day, backup for Exchange Online is now more important than ever.

Unfortunately, lost email is inevitable. Users may accidentally delete important messages as they manage their overflowing mailboxes. Organizations may suffer data loss due to ransomware, file corruption or malicious deletion. By default, Exchange Online purges deleted messages after 14 days. That key email may already be permanently erased by the time a user realizes it's missing.

Even if you choose extended Microsoft 365 licenses with a longer window before purges, the time it takes to find and restore a lost email can be cost-prohibitive. If you've ever had to search through archives using the Exchange Online Litigation Hold feature, you certainly wouldn't want to go through that again. Litigation Hold is a great safety net for archiving but not an effective method for backup and recovery.

FILES

USERS CAN DELETE KEY FILES ON SHAREPOINT AND ONEDRIVE.

REALITY

SharePoint's collaboration capabilities leave valuable data exposed to the risk of data loss events such as ransomware attacks, deletion, configuration mistakes and sync errors. The complexity of SharePoint makes recovery of data difficult once lost.

SharePoint Online and OneDrive for Business are key tools for many Microsoft 365 users as well as for the IT staff that supports them. Both applications provide users and teams with the tools to share and organize files, plus the ability to work from nearly anywhere. Another benefit for organizations is that these applications make it easy to manage user access and permission levels as compared to setting up custom network drives.

Many users are under the assumption that their SharePoint Online and OneDrive for Business data can't be lost because it's in the cloud. However, data can be deleted due to user error or malicious actions and files can become corrupted. Without a backup solution, Microsoft 365 provides no method for recovery after data is purged. And even if the data is still in the Microsoft 365 Recycle Bin, searching for what's needed can be similar to looking for a needle in a haystack, making restoration tricky.

SharePoint Site Admins can permanently delete their SharePoint data, making it immediately unrecoverable.

Corrupted files can take hours to rebuild.

Items in the recycle bin are unrecoverable after 186 days.

End users can permanently delete data in their OneDrive for Business account, making it immediately unrecoverable.

TOTAL MAILBOXES

DELETED EXCHANGE ONLINE MAILBOXES, FOLDERS AND CALENDAR ITEMS CAN'T BE RESTORED WITH JUST MICROSOFT 365.

REALITY

Microsoft 365 has no protection against deleted mailboxes, folders and calendars.

Although it may require hours of searching, it is possible to restore a single lost email using Office 365 alone. However, there's no way to restore account information such as folders, calendars, tasks or entire mailboxes. Your company's executives and sales team may have information for important business connections stored in Outlook. Lost data can mean lost deals or stalled strategic partnerships. Plus, entire Exchange Online mailboxes may be lost to malicious or accidental deletion and restoring these emails one-by-one would take forever.

UNLIMITED RETENTION

CLOUD BACKUP SHOULD MAKE LIFE EASIER, BUT IT WON'T IF YOU'RE FORCED TO CONSTANTLY MANAGE YOUR STORAGE.

REALITY

Constantly managing cloud retention and storage limits in the cloud can eat up all the time you wanted to save.

Cloud backup offers many benefits to overworked IT admins, including storage that easily grows with an organization's data footprint. However, depending on the backup solution you choose, increasing data in the cloud can come at a high cost that may not fit your budget. Constantly monitoring and adjusting cloud storage eats up all the time you were supposed to save with cloud backup. This is especially true when backing up applications with constantly changing amounts of data, such as Microsoft 365, which grows as rapidly as your company grows.

REALITY

The amount of data created over the next three years will be more than the data created over the past 30 years.

The world will create three times the data over the next five years than it did in the previous five.
An estimated 59 zettabytes (ZB) of data will be created in the world this year.[4]

THE SOLUTION

LOOK FOR A BACKUP SOLUTION THAT HAS THESE FEATURES:

1] COMPREHENSIVE PROTECTION

A reliable backup, with unlimited storage space and an unrestricted retention policy, ensures that your crucial Microsoft 365 data is always backed up and protected.

2] COMPLETE AUTOMATION

Aim for a 'set and forget' backup that provides daily, automated Microsoft 365 backup and auto-discovers new or altered content to backup. The backup process must run quietly in the background.

3] EASY & RAPID RESTORE

The backup must work for you by making it simple to locate and restore lost data.

4] TRANSPARENT REPORTING

A good solution should include an immutable audit log that provides a transparent, actionable report of each Microsoft 365 backup, as well as daily backup health status reports.

ARE YOU UNSURE WHERE TO BEGIN? GIVE US A CALL OR DROP AN EMAIL AND WE'LL LEND YOU OUR EXPERTISE TO HELP ENSURE THE PROTECTION AND RECOVERABILITY OF YOUR COMPANY'S VITAL MICROSOFT 365 DATA.

CONTACT US FOR A NO-OBLIGATION CONSULTATION.

Sources

1. https://www.mydbsync.com/blogs/reasons-to-protect-your-saas-data/
2 This retention can be extended to a maximum of 30 days.
3 IBM Cost of Data Breach Report
4 https://www.idc.com/getdoc.jsp?containerId=prUS46286020