SPANNING
A Kaseya COMPANY

THE DEFINITIVE GUIDE TO BACKUP FOR MICROSOFT 365

HOW TO ENSURE COMPLETE DATA PROTECTION FOR EXCHANGE ONLINE, SHAREPOINT ONLINE, ONEDRIVE AND MICROSOFT TEAMS

TABLE OF CONTENTS

NOW THAT YOU'VE FOUND THE PERFECT PRODUCTIVITY SOLUTION IN THE CLOUD...

it's time to know what your options are to keep your Microsoft 365 data safe from loss.

But wait! Doesn't Microsoft protect your Microsoft 365 data?

As you'd expect, Microsoft 365 comes with Microsoft's trusted security measures and data replication and recovery mechanisms. These ensure your data is as safe and available in the cloud as it was on-premises. This powerful system of protection is designed to guard against data loss caused by software malfunctions, hardware failure, power outages and natural disasters.

For example, if a server in one of Microsoft's data centers fails, it is highly unlikely that Microsoft will lose your data. Built-in redundancies and high-availability architectures ensure that your data will be available whenever you need it. Microsoft guarantees that their services, and your data, will be up 99.9% of the time. This means that you can be confident that you won't lose data even if Microsoft has an infrastructure failure.

However, Microsoft can't protect you from mishaps and failures on your side, such as accidental deletion, malicious user activity, ransomware, hacking, configuration errors, or programmatic errors such as synchronization and integration issues.

While there are threats to your Microsoft 365 data that Microsoft simply cannot prevent, third-party backup and restore solutions can protect against them. With the right solution in place—one that can handle backup and restores equally well—you don't have to worry about lost productivity, data loss or non-compliance.

What's at Risk?

PRODUCTIVITY

DATA LOSS

NON-COMPLIANCE

THE TRUTH ABOUT SAAS DATA LOSS

In an extensive survey of IT decision-makers, 77% reported SaaS data loss. This is significantly more than the 58% that reported SaaS data loss in an earlier IDG survey.

These statistics make it clear that data loss in the cloud is a growing problem, yet many IT decision-makers still feel quite confident in their organizations' ability to secure cloud data — 80% among U.S. respondents to the Spanning survey. Their confidence is, in all likelihood, misplaced. When asked to describe their strategy for backup and recovery, 50% stated that they would rely on their cloud vendor. This can only mean their organizations are put at risk.

77%

of companies that use SaaS applications suffered a data loss incident over a 12-month period.

Microsoft can't protect you from some of the most common causes of data loss.

SaaS vendors simply can't protect against every type of data since much of it is beyond their control.

For example, Microsoft builds redundancy into their infrastructure to support their uptime SLAs. But as with any SaaS platform, Microsoft takes action on that data as instructed by you, the customer. If you ask them to delete data, they're contractually bound to do so. If it turns out an employee made a request by mistake, or that a hacker made the request or the request was the result of a programmatic or sync error, Microsoft has no way of knowing that.

Once data is lost, the SLA does not provide for restoring lost data to Microsoft 365 applications. The SLA covers uptime, or the ability to reach and use Microsoft services, but it doesn't cover the protection of your data. In "Backing up Software-as-a-Service Applications," Deni Connor of Storage Strategies NOW explains, "the dirty little secret of the SaaS industry is that companies lose company SaaS data on a regular basis and most SaaS providers do not offer on-demand data restore capabilities that can be initiated by their customer companies."

WHAT CAN YOU LOSE?

Here are a few examples of how data loss can happen in Microsoft 365.

- A disgruntled employee decides to delete his or her email, easily emptying and purging the Recycle Bin, making data recovery and restoration difficult.
- Deleted files, emails or entire mailboxes are retained for a period of time (which varies by each Microsoft 365 service and is based on retention policies), but are not recoverable after this period has expired.
- Deleted accounts are recoverable for 30 days, after which time they and all their associated data are permanently gone.
- An employee deletes documents and then empties the Recycle Bin. Once cleared, you have only 14 days to alert Microsoft that a restore is needed.

The data you store in SaaS applications is at risk for the same threats that cause on-premises data loss, and you should protect your data in the cloud just as you do for on-premises data.

That's the risk, here's the reality.

Risks can be avoided, but here are some real life examples of data losses from posts on techcommunity.microsoft.com.

DATA LOST TO ACCOUNT DELETION

ADMIN'S POST
"We deleted a user account in Microsoft 365 and it has been more than 30 days. Now we received a request to access the person's OneDrive documents. Is there a way to recover these documents?"

MICROSOFT SUPPORT'S RESPONSE
"It's not feasible to restore a user account that has been deleted more than 30 days. According to the article below, when we delete a user account, it becomes inactive. During this inactive period, you have up to 30 days to fully restore the account. However, after 30 days, all data for that user is permanently deleted —except documents saved on the teamsite."

DATA LOST TO DELETED EMAILS

ADMIN'S POST
"I have an employee who…deleted all of her emails in Microsoft Outlook as well as logged onto her email account via Microsoft Exchange Online and deleted them there as well… Is there a way to recover the emails she deleted?"

MICROSOFT SUPPORT'S RESPONSE
"The emails in the Recover deleted items folder will be kept for 14 days, the emails in the Recover deleted items folder will be purged and will not be found after 14 days."

DATA LOST TO ADMIN ERROR

ADMIN'S POST
"I inadvertently set a retention policy of 90 days for all user mailboxes. This caused all email other than this time to be deleted. Is there any way to restore these emails to the folder they were in before the retention policy ran?"

MICROSOFT SUPPORT'S RESPONSE
"No, the (MRM) policy does not apply to the Recoverable Items folder. It is only for the visible Deleted Items folder."

DATA LOST IN SHAREPOINT ONLINE

ADMIN'S POST
"...in some of these larger file moves, users have reported large losses of data. The files were moved, and confirmed, but when the user comes in the next day their files have disappeared."

MICROSOFT SUPPORT'S RESPONSE
"It's difficult to suggest a best practice as it comes down to the ways in which your users like to work. In my own business unit I have some who like to only work in the browser, and someone who only like to work with synced folders. You can explain to your users how they can do it, and then they find their own way."

DATA LOST TO ACCOUNT AND MAILBOX DELETION

ADMIN'S POST
"Is it possible to recover a user and their mailbox past 30 days since deletion? I have a user deleted permanently about 45 - 60 days ago and now we need their mailbox back."

MICROSOFT SUPPORT'S RESPONSE
"No - after 30 days (approximately) the mailbox is removed and cannot be recovered, unless you use a service like Spanning.com to take online backups."

THE TOP 4 REASONS YOU NEED BACKUP FOR MICROSOFT 365

Accidental Deletion

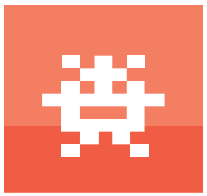
In a Spanning survey of more than 1,000 IT decision-makers in the US and the UK, 43% identified accidental deletion of data by users as a source of SaaS data loss for their organizations—more than any other factor.

When someone accidentally deletes an item, there's still hope while it's in the recycle bin, where it stays temporarily—in SharePoint and OneDrive it will remain for 93 days and in Exchange Online the item will remain for 14 days by default, or up to 30 days. At that point, the item moves to a secondary Recycle Bin. Whenever the item hits the secondary Recycle Bin, it remains there for 93 days in total before it's deleted forever, or less if the site is near quota.

Hackers

Fully one-quarter of IT decision-makers surveyed pointed to hacking as a source of data loss in their organizations. Unfortunately, this problem is getting worse. In fact, ransomware is now considered the number one cyberthreat to organizations, with more than 4,000 attacks occurring on a daily basis.

One current example of the hacking risk for Microsoft 365 is the use of sync clients to access files in Microsoft 365, a practice which can introduce files infected with ransomware into Microsoft 365 tenants.



60%

of all data attacks were carried out by insiders, according to IBM's 2016 Cyber Security Intelligence Index.

Malicious Insiders

Shockingly, a 2016 Cyber Security Intelligence Index found that 60% of all data attacks were carried out by insiders. In any busy organization where employees and contractors with access to data and files are constantly coming and going, that fear is well-founded.

In Microsoft 365 environments, where multiple employees have shared access to files, contacts and more, the risk of insider attacks grow, regardless of whether they are in the form of a terminated employee deleting data on the way out, a disgruntled user purging important documents or anything in between.

Programmatic Errors

Sync malfunctions, configuration glitches and other types of programmatic errors are common when using third-party apps along with Microsoft 365. For example, an employee installing a productivity app on a mobile device can easily wipe out an entire list of contacts or calendars during the sync process.

IS MICROSOFT'S ARCHIVING SOLUTION THE ANSWER?

Microsoft offers an archiving package (included with the license for E3 and higher) with a Litigation Hold feature for long-term data preservation. Once a user is placed on Litigation Hold, every email, calendar item and file in OneDrive and SharePoint is preserved along with any changes made to the item while the user is on hold.

When making a decision whether or not to use Litigation Hold as a backup plan, keep the following in mind. **Litigation Hold is a business process.** With input from the legal team, the business defines the policy for legal holds. IT is responsible for implementation but shouldn't make the decision to put users on Litigation Hold without the input of the organization's legal team.

Archives are for storing data, not for getting it back fast.

Although you can use these features to preserve data, will you be able to rapidly and efficiently restore your data? No. Archives and Litigation Hold are used to store data to meet regulatory, compliance and legal retention needs. They can't rapidly restore lost data back into production and they don't have the functionality needed to automate accurate restores.

Backups, on the other hand, are copies of production data that you can use to quickly restore any lost data back into production. So before you decide to rely on a feature like Litigation Hold to protect your data, be aware that it isn't exactly the right tool for what you're trying to achieve.

Don't be discouraged. There's a better way.

If you want to get lost data back, a better way is available with third-party cloud-to-cloud backup. Read on to learn more.

WHY THIRD-PARTY CLOUD-TO-CLOUD BACKUP IS THE WAY TO GO

Cloud-to-cloud backup and restore solutions for Microsoft 365 protect against threats to data that Microsoft can't. They ensure that you can immediately recover lost data without missing a step, turning potential data disasters into non-issues.

Only cloud-to-cloud backup delivers these key benefits.

With cloud-to-cloud backup, a separate and secure copy of all your data is kept and updated for you regularly. As a result:

- When data loss happens, you can rapidly restore your data yourself back to the point before the data loss occurred.
- When data loss happens, you can look to your backup provider to rapidly get data back the way it was before the loss occurred.
- You'll avoid steep costs associated with recreating or manually recovering lost data.
- You'll improve overall employee productivity.
- You'll satisfy key auditing and compliance requirements.

You need a backup solution that provides accurate, reliable restore functionality. What good is backup if you can't restore lost data back into your environment quickly and accurately?

Remember, backup is only as good as the recovery that comes with it.

When choosing your backup provider, it's important that their features, benefits and security standards meet your regulatory and compliance needs. For a SaaS or cloud-based solution, such as Microsoft 365, the best backup and restore solution is also architected as a cloud-to-cloud solution. Those vendors understand the intricacies and cloud technology necessary to keep your data safe and easily available for restore. In addition, a backup solution must provide accurate, reliable restore functionality. What good is backup if you can't get the lost data back into your environment quickly and intuitively?

Now we'll look at other factors to consider when selecting a cloud-to-cloud backup solution.

7 THINGS TO LOOK FOR IN A CLOUD-TO-CLOUD BACKUP SOLUTION

01 AUTOMATED AND ON-DEMAND BACKUP

02 GRANULAR POINT-IN-TIME RESTORE

03 EASE OF USE

04 COMPREHENSIVE ADMINISTRATOR CONTROL

05 SECURITY CREDENTIALS

06 MICROSOFT APPSOURCE APPROVED

07 UNLIMITED STORAGE

SPANNING
A Kaseya COMPANY

01 AUTOMATED AND ON-DEMAND BACKUP

Automated backup means that, if you choose, you can “set and forget” your backups, knowing you’ll always be protected without additional effort on your part. Choose a backup provider that lets backup run quietly in the background, but also gives you the option to run a manual backup whenever you choose.

02 GRANULAR POINT-IN-TIME RESTORE

When data loss happens, you must be able to get your data back exactly as it was, as quickly as possible. The most sophisticated backup and restore solutions will provide granular restore that allows you to retrieve data from any point in time in just a few clicks. This means you can recover historical snapshots or versions of an application’s data and restore them into your Microsoft 365 tenant.

SPANNING
A Kaseya COMPANY

03 EASE OF USE

Backup software should make the lives of IT professionals easier. Look for a vendor that provides an intuitive user experience that works seamlessly with Microsoft 365.

Your backup solution should also be transparent and informative. Check for daily or real-time updates that will help you understand the status of your backups and if there are any errors that need attention.

Another important, yet often overlooked factor, is end-user enablement. Your company migrated to the cloud to allow employees to work anytime, anywhere, encouraging innovation to happen faster than ever before. When accidents happen in Microsoft 365, shouldn't employees also be able to resolve their own data loss issues? When end users are able to restore data themselves, they can not only continue working with minimal disruption to their workflow but also spare the IT team from addressing countless support desk calls.

Ensure the solution you choose is intuitive and easy enough that end users of your Microsoft 365 tenant can restore their own data.

SPANNING
A Kaseya COMPANY

04 COMPREHENSIVE ADMINISTRATOR CONTROL

As we've discussed before, housing your data in the cloud does not change the fact that you are in control of it. In light of this, you'll want a backup solution that offers customizable administrator settings so you can wield this control as you see fit. A good backup and restore solution will let you balance the control you want with the freedom of the cloud by offering these administrator options:

- Assigning new users
- Selecting specific site collections to include and automatically include all new site collections
- Monitoring and resolving backup errors with a detailed status history
- Accessing an immutable audit log of all administrator and user actions

05 SECURITY CREDENTIALS

Make sure the provider you choose uses industry best practices for security standards. Use this checklist of key qualifications to confirm your provider is secure enough to protect your data.

- ✓ SSAE SOC2 Type II compliant
- ✓ HIPAA and GDPR compliant
- ✓ Strong block ciphers – 128-bit SSL encryption in transit and 256-bit AES encryption at rest
- ✓ At least 99.9% uptime
- ✓ Application-level authentication
- ✓ Earned the BBB EU Privacy Shield, operated by the Council of Better Business Bureaus Privacy Certification
- ✓ Is certified under the US-EU and Swiss-US Privacy Shield
- ✓ Log analysis to guard against intrusions
- ✓ File integrity and policy monitoring
- ✓ Rootkit detection
- ✓ Real-time alerting and active response

SPANNING
A Kaseya COMPANY

06 MICROSOFT APPSOURCE APPROVED

AppSource is Microsoft's online app store for business applications such as Microsoft 365. Microsoft created AppSource so their customers could easily find, compare, try, and install Microsoft and partner solutions as simply as installing an app on a smartphone. Microsoft also ensures the integrity, performance and compatibility of all AppSource listed products through rigorous requirements on quality of code and cloud service and a requirement that you can "try before you buy." By choosing a backup provider available through AppSource, you get a guarantee of quality and performance and a superior customer experience from trial through implementation to ongoing service and support.

07 UNLIMITED STORAGE

Your organization's volume of data will always expand. Don't compromise by choosing a "pay-as-you-go" storage model. Unlimited storage models charge one price, regardless of how much data you consume, and save you from having to periodically make room for more data or seek approvals to purchase more storage. Find a vendor who offers unlimited storage and will scale up or down.

Spanning Cloud Apps, a Kaseya company, is the leader in SaaS Cloud-to-Cloud Backup, proven and trusted by more than 10,000 organizations across the globe to provide enterprise-class data protection. Spanning's cloud-native, purpose-built solutions for Microsoft 365, G Suite, and Salesforce provide easy-to-use yet powerful capabilities for end-users and administrators and meet the rigorous requirements for listing on Microsoft AppSource, Salesforce AppExchange and G Suite Marketplace.

START A FREE 14-DAY TRIAL AT
SPANNING.COM/START-FREE-TRIAL

@SPANNINGBACKUP

FOLLOW US ON LINKEDIN

READ OUR BLOG

WWW.SPANNING.COM

+1 (512) 236-1277