SPANNING

THE DEFINITIVE GUIDE TO BACKUP FOR OFFICE 365

ENSURING COMPLETE AND EFFECTIVE DATA PROTECTION FOR OFFICE 365

TABLE OF CONTENTS

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

It's time to get to know your options for keeping your data in Office 365 safe from loss. You may be surprised to discover that there are various options available to protect your Office 365 data.

After all, doesn't Microsoft protect your Office 365 data for you?

As you'd expect, Office 365 comes with Microsoft's trusted security measures and data replication and recovery mechanisms that 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 Office 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

These days, the question isn't so much who has experienced a loss of SaaS data as who hasn't. Of the more than 1,000 IT decision-makers that Spanning surveyed in late 2015 and early 2016, only 23% reported no SaaS data loss in the 12 months covered by the survey. That means 77% suffered a loss of data in the cloud—significantly more than the 58% cited by IDG in a 2014 report.

Those 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 US respondents to the Spanning survey. What's the reason for their confidence? Asked to describe their strategy for backup and recovery going forward, 50% stated they would rely on their cloud vendor for backup and recovery—more than would rely on their own manual or automated data backups.

77%

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

Microsoft can't protect you from your users.

SaaS vendors simply can't protect against every type of data loss, because 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, Microsoft has no way of knowing that.

Once data is lost, the SLA does not provide for restoring lost data to Office 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 Office 365.

- A disgruntled employee decides to delete his or her email, easily emptying and purging the trash bin, making data recovery and restoration difficult.
- Deleted files, emails, or entire mailboxes are retained for a period of time (which varies by each Office 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.

The data you store in SaaS applications is at risk for the same threats that cause on-premise data loss, and you should protect against them in the cloud just as you do for on-premise 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 Office 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 Office 365 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."

THE TOP 4 REASONS YOU NEED BACKUP FOR OFFICE 365

Accidental Deletion

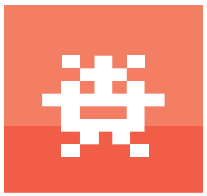
In a Spanning survey of more than 1,000 IT decision-makers in the US and the UK, 43% identified accidental deletion of data by users as a source of SaaS data loss for their organizations – more than any other factor.

When someone accidentally deletes an item in Office 365, including SharePoint, there's still hope while it's in the recycle bin, where it stays temporarily (how long exactly depends on which service is involved) before moving to a secondary recycle bin. After a *finite amount of time* there, it's purged completely, never to be recovered unless it was backed up.

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 growing worse; in fact, ransomware is now considered to be the number one cyber threat to organizations, with more than 4,000 attacks occurring on a daily basis.

One current example of the hacking risk for Office 365 is the use of sync clients to access files in OneDrive, a practice which can introduce files infected with ransomware into Office 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 Office 365 environments, where multiple employees have shared access to files, contacts, and more - especially when using Sharepoint and/or OneDrive - the risk of insider attack grows—whether from a terminated employee deleting data on the way out, or from 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 Office 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.

Another sync risk comes with the use of sync clients to interact with data in OneDrive and SharePoint. The original sync client for Office 365 was particularly prone to sync-related data loss issues; it's been replaced, and the new client is available for all Windows supported client OSs. However, it doesn't support everything - i.e., syncing shared folders or SharePoint files.

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, as well as any changes made to the item while the user is on hold.

Sounds like a good way to keep from losing your data, doesn't it? Well, not exactly. And that's because there's a very important difference between an archive and a backup.

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

Archives are designed to store data for long periods of time to meet regulatory, compliance, and legal retention requirements. They're not built to rapidly restore data back into production, nor do they have advanced search capabilities, which is the functionality you really need if you suffer a data loss.

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

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

If you're looking for help to get your lost data back, don't stop—because help is available, in the form of 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 Office 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 a 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.
- Customers will be reassured of the resilience of your brand and your business.

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 intuitively?

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 Office 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 DAILY AND ON-DEMAND BACKUP

02 GRANULAR POINT-IN-TIME RESTORE

03 INTUITIVE USER INTERFACE

04 COMPREHENSIVE ADMINISTRATOR CONTROL

05 SECURITY CREDENTIALS

06 SUPPORT

07 UNLIMITED STORAGE

SPANNING

01 DAILY AND ON-DEMAND BACKUP

Daily, 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 Office 365 tenant.

SPANNING

03 INTUITIVE USER INTERFACE

Backup software should make the lives of IT professionals easier. Look for a vendor that provides an intuitive user experience that works seamlessly with Office 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 Office 365, shouldn't employees also be able to resolve their own data loss issues? When end users are able to restore data themselves, they not only can continue working with minimal disruption to their workflow, but also can 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 Office 365 tenant can restore their own data.

SPANNING

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 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
- Monitoring and resolving backup errors with a detailed status history
- Accessing detailed records 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 compliance
- ✓ HIPAA compliance
- ✓ Strong block ciphers – 128-bit SSL encryption in transit and 256-bit AES encryption at rest
- ✓ At least 99.9% uptime
- ✓ TRUSTe privacy and security seals
- ✓ Log analysis to guard against intrusions
- ✓ File integrity and policy monitoring
- ✓ Rootkit detection
- ✓ Real-time alerting and active response

SPANNING

06 SUPPORT

Even though you'll be purchasing a software solution to protect your Office 365 and SharePoint data, how the provider treats you during the discovery, sales, implementation, and support processes is of paramount importance. Be certain you can trust a SaaS vendor before you entrust them with your critical data, and ask how they will handle your support issues. A great backup provider will give you access to various resources, including forums, articles, how-to videos, and email support, so if you ever have any questions, you'll be able to get the answers you need with ease.

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 is the leading provider of backup and recovery for SaaS applications, protecting more than 8,000 organizations from data loss due to user error, malicious activity and more. We are the only global provider of powerful, enterprise-class data protection for Microsoft Office 365, G Suite, and Salesforce. With data centers located in North America, the EU, and Australia, Spanning is the most trusted cloud-to-cloud backup provider with millions of users around the world.

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

@SPANNINGBACKUP
FOLLOW US ON LINKEDIN
FOLLOW US ON GOOGLE+
READ OUR BLOG

WWW.SPANNING.COM

+1 (512) 236-1277