



EBOOK

# 6 Reasons to Back Up Microsoft 365

## Executive Summary

Productivity suites such as Microsoft 365 (formerly Office 365) and G Suite are growing rapidly in all types of businesses, from SMEs to large organizations driven by the different market players (such as Managed Service Providers, Value Added Resellers, etc.).

This trend is very pronounced in the United States. Europe is just behing the US with very strong adoption growth rates in recent years. Today, **65% of organizations have adopted Microsoft 365** compared to 19% for G Suite (Bitglass Study Data).

There are many new challenges for IT managers, since user data is no longer stored on workstations or on-premise servers;

they are directly stored in the Cloud on the servers of these service providers.

However, on outsourced infrastructures data is not protected from the usual security risks: inadvertent deletion, ransomware, malicious access.

Businesses should not assume that because the IT environment has shifted to the cloud that the data does not need protecting in the same way as local environments.

## To Backup or not to backup Microsoft 365?

**M**icrosoft Microsoft 365. Frankly, what's not to like? It lets you unplug your ageing mail and file servers and externalize your critical applications to a secure location managed by one of the largest and best known names in the tech universe, Microsoft.

To their credit, Microsoft have done a great job converting many of their flagship solutions to a SaaS offering. Already **150 million users** and counting. Your emails, OneDrive files and SharePoint data are globally safe and sound in the cloud.

**Remember that Microsoft 365 is the transferal of core Microsoft applications (including email) to the cloud.** The teams on the ground **still need to continue managing and protecting** data generated within this cloud infrastructure.

Because Microsoft 365 lets you create and share so much critical information, the security and longevity of this data becomes paramount. What the platform always provide is an adequate level of protection. **This eBook examines why we should give serious consideration to deploying additional protection.**



# Why you should own your data security

**W**hen it comes to data security, we're reminded of the phrase about not being able to see the forest because of all the trees! Microsoft themselves point out that infrastructures are increasingly hybrid and complex. The average organization continues to manage dozens of separate security products on myriad systems<sup>1</sup>.

We will have to wait some time for that all-encompassing master dashboard, completely invisible infrastructure and 100% infallible security.

Even with all our security tools, we are still unable to detect all threats in real time. According to the Ponemon Institute calculated the **average time to detect a data breach was almost 200 days** in 2018<sup>2</sup>.

More than **six months to see that data is potentially compromised** is worrying! Fortunately, we can act by investing in third-party data protection solutions to insure our digital assets during and beyond this period.

Many organizations deploying SaaS solutions do not have a coherent and automated backup plan. They rely on having no backups or simply basic SaaS provider content retentions.

This is cause for concern because typically a SaaS such as Microsoft 365 will set limits on how much data they are prepared to handle on our behalf.

The SaaS provides infrastructure, redundancy, high availability and failover but **rarely provides long-term data versioning and generous or unlimited storage capacity.**

// The Ponemon Institute  
calculated the average time  
to detect a data breach was  
almost 200 days in 2018<sup>2</sup>

*Larry Ponemon, Chairman and Founder, Ponemon Institute*

When the option is available, associated retention costs are often so high that they are basically non-viable.

1 Source: [6 steps to holistic security](#) (Microsoft)

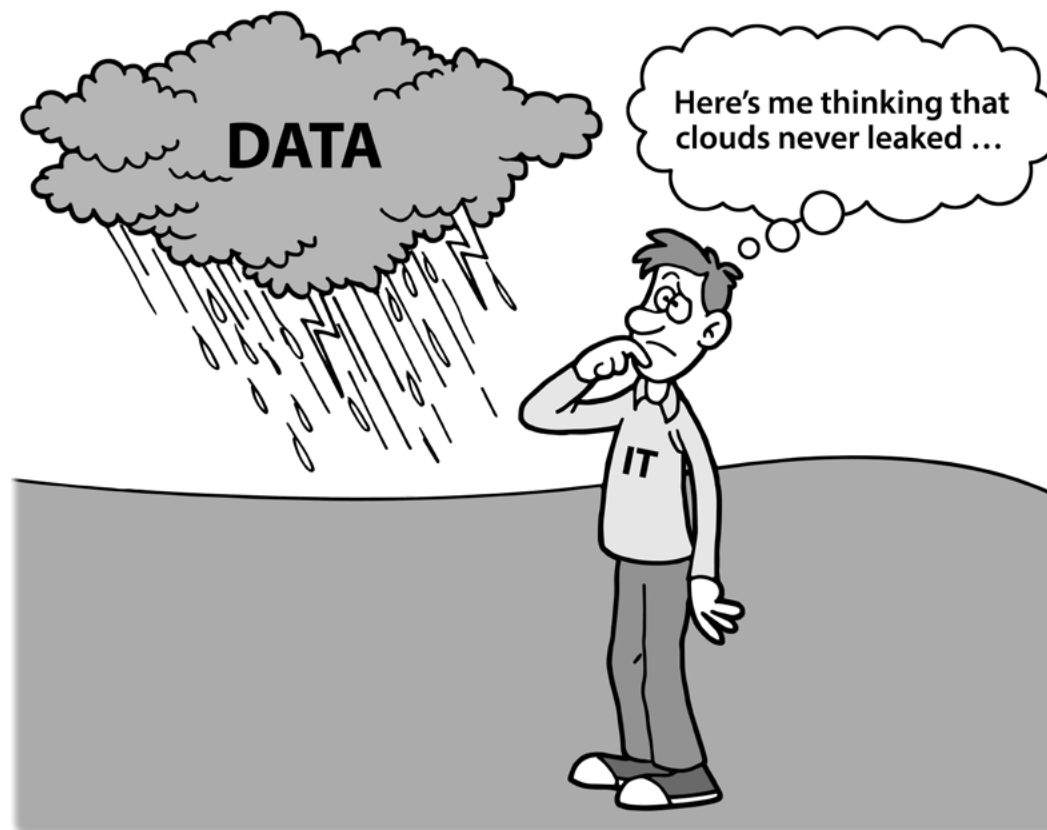
2 Source: [Ponemon cost of a data breach 2018](#)

In other words, **SaaS solutions don't really cut it as genuine data storage and backup alternative for your business.**

Lastly, any SaaS (yes, even Microsoft 365) can crash, lose data, go out of business, modify the level of service or itself be subject to cybercrime. Hybrid solutions and comprehensive backup and restore solutions

mean your options remain open in all circumstances. If pushed to find a takeaway cliché, it's would be: do not keep all your eggs in the same basket.

**The following 6 reasons** will hopefully convince you to supplement your Microsoft 365 installation with a genuine backup and recovery solution.



# REASON #1

## External Risks

If IT managers and teams are responsible for managing internal risks, there are certain threats and situations that are beyond the control of your teams. Issues on the SaaS service side, ranging from **partial loss-of-service to complete cessation of service** with short or no notice.

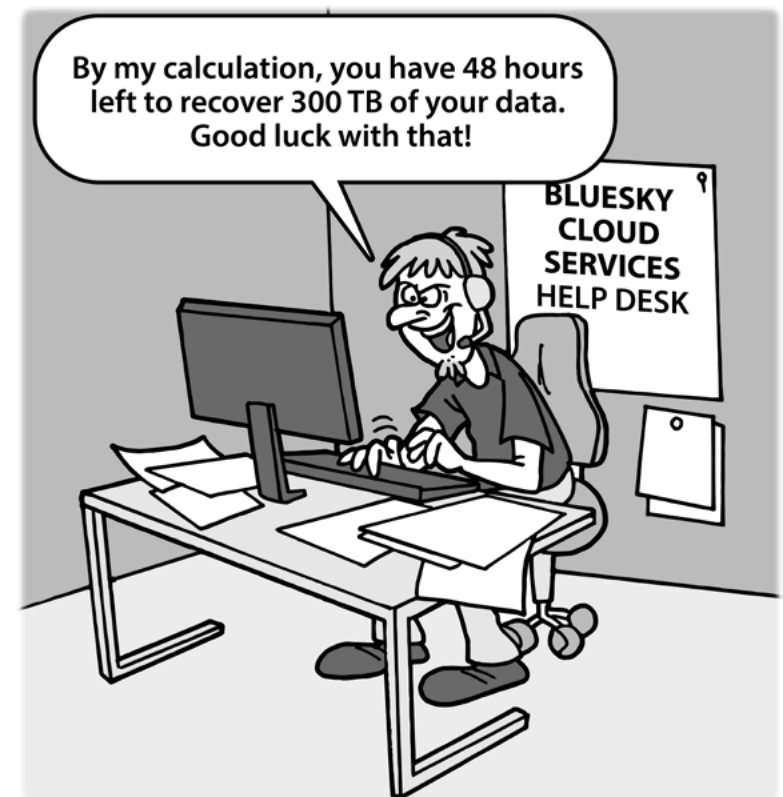
The partial loss-of-service is a frequent short-term incident, where you have access to only a part of your data for a short period of time. Sometimes this is due to an internal network issue, or the service provider loses a couple of servers or storage nodes and the recovery process kicks-in: new servers are automatically allocated, launched, loaded with the proper OS and software.

Your data is automatically cloned by the internal service recovery processes (some smart cloud equivalent to a RAID process). Sounds good. Most of the time you do not even notice. But sometimes you do, when realizing that specific folder data is now a-month-old. **Data losses may be small but they can still have a critical impact.**

On the other end of the spectrum, you'll no doubt heard of this sad old story of a SaaS platform that decided without warning to close all its services with only two weeks' notice. Customers are told "please retrieve your content before this date". Unfortunately retrieving large volumes in a short periods of time -not to mention having all customers doing it at the same time- rarely works out well.

Many companies have lost data here. Admittedly, this was in the early days of SaaS service. Where such a situation to happen today, the service would certainly provide a longer grace period to customers. It's far from sure this would be enough to prevent data loss because, **compared to 10 years ago, we are now storing much greater volumes of critical data in the cloud.**

The bottom line: if you feel the data you store in the cloud has significant value to your business, this raises one key question: "Can we afford to live without part of the data we are storing in Microsoft 365 and Exchange online"?



## REASON #2

### Internal Risks

The Aberdeen group recently reported that **32% of organizations had lost data from the Cloud<sup>3</sup>**. Most cloud data loss is through human error such as relying on the recycling bin or deleted email folders to recover lost data and finding that this data no longer existed or that the wrong document version was available.



3 Source: [Solutions review](#)

Other causes of data loss occur when the SaaS provider changes; **data stored on the outgoing platform is often definitively deleted after 30 days**. A project transition team could easily be responsible for letting the clock tick down because they are too busy setting up the new provider to take care of data in the old subscription. In addition, data migration from SaaS subscriptions is frequently manual and complex and therefore sometimes neglected or only partially completed.

Regrettably, malicious acts of disgruntled employees, past or present, continue to be the cause of email and file deletion. Anyone with access to the Microsoft 365 admin account can rapidly do a lot of damage. And even if Microsoft 365 does offer an option to prevent the change of a retention period to a lower value/duration, it's no sure how many companies have implemented this yet. If your company is one of them, **you still need your longest retention periods to be configured for more than 200 days in order to be safe<sup>2</sup>**. Remember that this is the average time **to detect a data breach** as we saw in the previous section.

A key recommendation is to generate backup copies which are managed by a different admin to reduce risk of wholesale and irretrievable data loss.

There are solutions available that archive emails. **Archiving is a useful feature** but should not be a substitute to actual backup. Archiving removes primary data and transfers it to another, typically unique, location. **Backup best practice means having several copies or versions of one data** set on at least two physical sites and on separate backup media.

## REASON #3

### Retention Strategies

**M**icrosoft 365 has a limited data retention strategies for deleted objects. For example, default maximums on emptied folders are 30 days. There is no notion of versioned backups, missing objects and longer-term retentions. And if a data breach or loss occurs, it may be **5 whole months since Microsoft 365 definitively deleted your data.**

The key recommendation here is to have several versioned copies of some or all mailboxes which are stored on prem or in another cloud or on tape.

Rapid and granular restores can be time consuming from within Microsoft 365 because the tool exists to manage emails not backups. **You cannot for example navigate back to a point in time** and see what emails or folders looked like at a given instant or select objects to restore based on keyword searches or creation dates.

Ensure you have the tools to maintain email recovery flexibility. Ideally, **you should have short-term backup retentions and long-term backups and archiving in place.**

Plus a choice of granular email or folder recovery or complete mailbox or database restoration options.

Because **email continues to store critical unique data** with essential file attachments, the backup solution needs to be rapid.

If you can get the email back from Microsoft 365 directly, that's great. If the service is down, or if you need older data, then you will need to call on of a genuine and fully functioning backup tool.





## REASON #4

### Regulations

**T**rust is an all-important issue when it comes to any SaaS contract. A SaaS customer entrusts confidential client data to the SaaS provider. Because the provider has sole responsibility for the cloud infrastructure, there can be conflict between the service they provide and the regulations in the country or region in which the data is created and managed.

As both a business and SaaS customer, you still have control over the services you use and the data you collect. It's important to be up to date on all the privacy legislation necessary, to make sure all the data collected from your customers remains protected.

GDPR in Europe is an example of potentially conflicting situations regarding private data and cloud storage. In the coming years, this legislation is unlikely to be softened. On the contrary, certain SaaS providers will be increasingly at odds with the data laws globally.

From a business perspective and also a regulatory perspective, wherever your business is located, **it's now mandatory to protect enterprise data** which has become the core resource of your organization. **Data is key to restarting your activity.** Depending on your localization, you are also subject to eDiscovery obligations,

or similar rules for searching and preserving emails and data on a subject related to a lawsuit or legal dispute.

Such **regulations require that you keep your data under tight control because your CEO is legally responsible** for implementing the tools that preserve and store this data for the required period of time. Again, the key words here are "your data". SaaS is no more than a commodity with limited interest in long term or regulatory preservation.



## REASON #5

### 3-2-1 Backup Strategies

American photographer [Peter Krogh](#) wrote that there are two types of people: those who had suffered disk failure and data loss and those who would one day. From this he developed a **3-2-1 approach for data storage** which entails backing up primary data to at least two other supports in, ideally, two different locations.

For Microsoft 365 primary data is with Microsoft in the Cloud. Other copies could be on hard disk and another copy on tape stored off site or in a different cloud location.

**Risk of total data loss is reduced exponentially by diversifying storage targets and storage locations.**

Because **we're well and truly in the age of cybercrime**, let's take the example of ransomware where encrypted files are propagated through primary data to secondary data or backup copies. **Infected files can travel over the network and impact other storages**; an opened email attachment can shut down one or more endpoint machines and even infiltrate backed up data.

One solution is to have an "air gap" backup storage destination. **Air gap storage** is anything that is not accessible over the network, typically offline tape or high density optical disk. Used and useful for archiving and backups with long-term retentions, **air-gapped**



**data can get many admins out of a tight spot when faced with a massive cyberattack** on critical systems and data.

The more the data is offline, the longer it can take to restore. The **advantage of having a 3-2-1** approach is that you can restore rapidly if the incident is routine or minor and you can restore -period- in the event of catastrophic loss on primary and secondary storages.

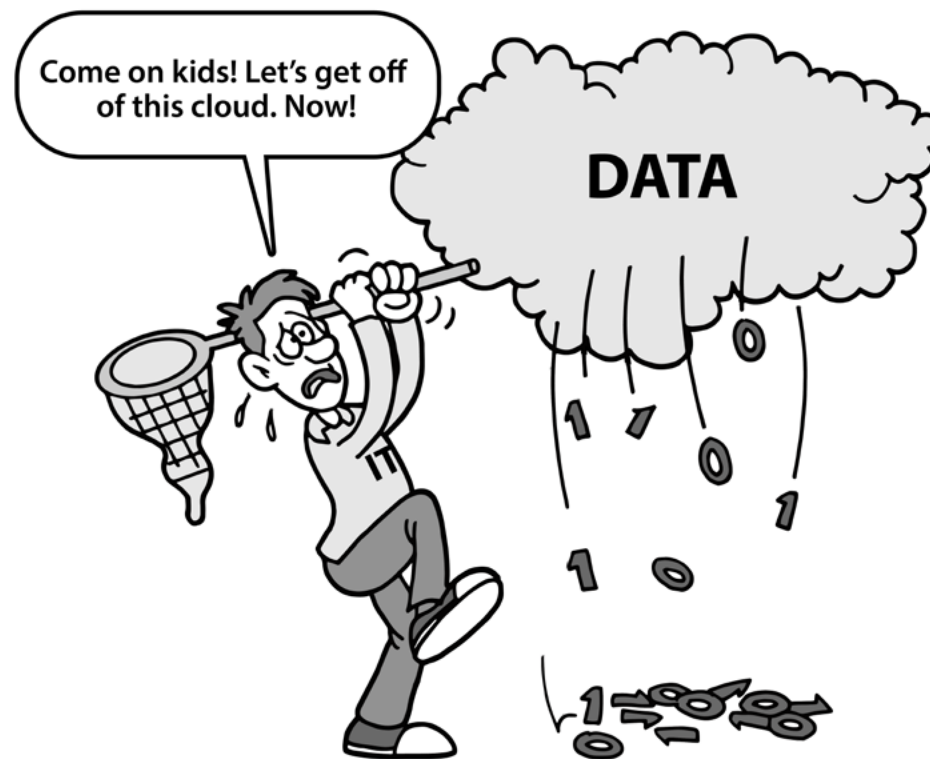
## REASON #6

### Get out-of-SaaS Card!

If you have been around for a few years, you'll know that IT infrastructure management is all about cycles. If the current cycle is about out-sourcing, out-storing, offloading "weight" to specialized services, the goal is not only to reduce infrastructure costs.

There is **a big move towards extending the enterprise IT system to the cloud**, to make it easier to add and remove servers, services or users on demand.

The current drivers are all about cost-efficiency. This creates a lot of opportunities for optimizing the infrastructure, for leveraging specialized services and extending the company's reach rapidly as needed by business.



**This race for productivity must not make us throw caution to the wind:** all critical applications and services must be reversible. An alternative to SaaS hosting should be studied to ensure reversibility at all times. Regarding Microsoft 365 and emails, we recommend operating a mixed SaaS/on-premise infrastructure.

**Having an email backup solution that covers both on-prem and cloud mail servers** is a natural leverage for helping to make the switch when needed.

While you are at it... do not stop there: your backup must consolidate multiple apps and databases to simplify the task for your IT management team.

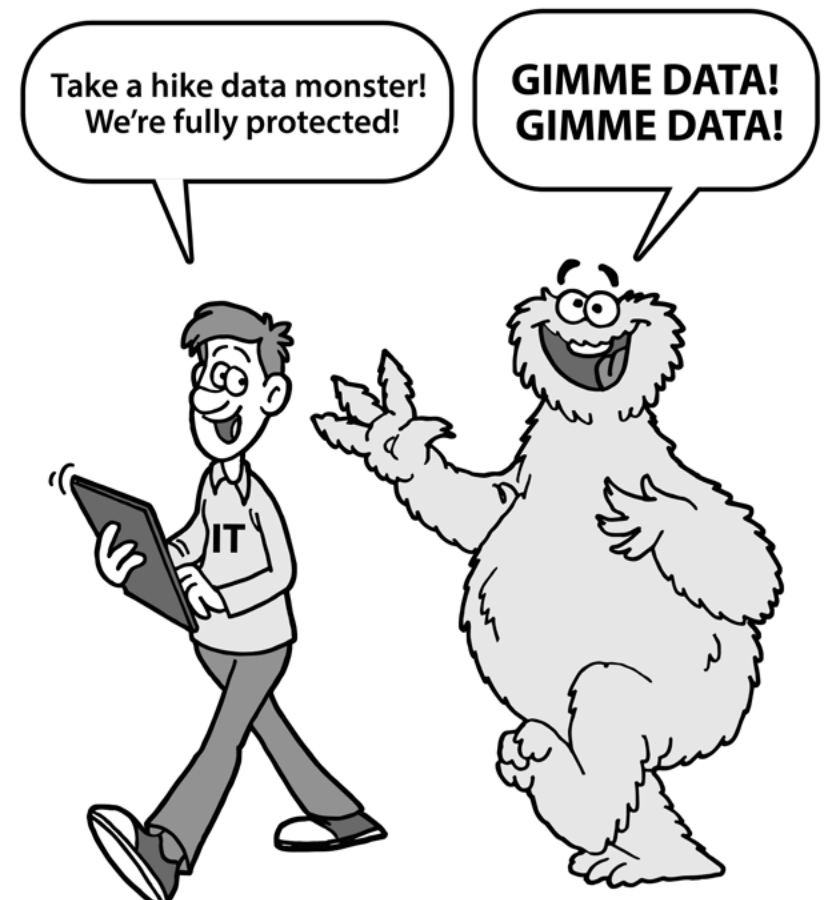
## CONCLUSION

It is clear in many domains, including SaaS, that hybrid infrastructures are the way forward... Whatever your requirements, the cloud provides flexibility and off-site redundancy and activity spike management. The on-prem side means you have control of your data locally, the ability to restart critical business applications –including email- if data is lost from the cloud through downtime or human error.

We are not pushing for a return to on-prem servers and the cost and maintenance time associated with this architecture. We are saying that SaaS can sometimes mean we lose sight of our actual data and when the smoke settles on a major incident, we are comforted in the knowledge that this data is still available and under our jurisdiction.

At Atempo, we always **seek out concrete benefits of actual technological revolutions** that it knows the customers can benefit from. Microsoft 365 is spearheading how we manage critical business data. Atempo has the solutions to ensure this data continues to thrive in your ecosystem.

*Read more below on our flagship solution  
Tina with full Microsoft 365 integration.*



# Tina Advantages

IT security is fast becoming the key factor underpinning IT purchases. Speed, performance, functionality are vital of course but without fundamental respect for data security and integrity, all other advantages fall by the wayside. We'd all like to drive a Ferrari but not many of us would without a seat belt! Tina solution provides complete Microsoft 365 email protection.



## Data and Infrastructure Security

Security is centered around three poles:

- **Data encryption** both at rest and in-flight plus advanced access rights to prevent data leakage or subversion.
- **Data partitioning.** Tina backs up to multiple secure destinations including air gapped targets to stop cyberattacks propagating.
- **Reporting.** To respect regulatory constraints, Tina provides reporting to inform you where your data is, how long it is preserved and who has access.

## Data Sovereignty

Growing numbers of Atempo customers are looking to store their data closer to home and reduce dispersion in far off cloud storages. Sovereignty can be about refusing to submit one's data to the risk of exploitation by a foreign power, even if this may be legal. It can also be about simply taking back control of our data in these high-regulation and high-risk times.

Tina provides protection for SaaS solutions for on-premise and off-premise storage and protection. You can take the decision to restrict what data is stored in the cloud to avoid security and sovereignty issues and align with your regional

## Global Protection, Granular Recovery

It's not uncommon for businesses to manage several backup solutions for their systems, applications and files. Tina is renowned for its global approach and overarching solutions for all virtual and physical machines, multi-OS plus hot application and database backup with granular recovery.

This means that you manage fewer data protection solutions and have just one simple dashboard to supervise.

For Microsoft 365, Tina lets you search for missing emails and mailboxes and navigate back in time to find what you need to recover. Recovery is rapid, simple and granular.

## Cost Efficiency

Tina has a very powerful source and global deduplication engine that provides significant savings on backup storage and reduces the impact of backup on your network. An email attachment sent to 30 users will only be backed up once.

Tina's licensing model is designed to make your life as simple as possible. Adding another mailbox to Microsoft 365 will not impact your license or prevent the level of protection provided to your teams.

For more information, use this QRCode to learn about our solution:






## About Atempo

Atempo is a leading independent European-based software vendor with an established global presence providing solutions to protect, store, move and recover all mission-critical data sets for thousands of companies worldwide. With over 25 years' experience in data protection, Atempo offers a complete range of proven solutions for physical and virtual server backup, workstation's protection and file migration between different storages of very large capacity. **Atempo's** three flagship solutions, **Lina**, **Miria** and **Tina** have been labeled by '**France Cybersecurity**' and '**Used by French Armed Forces**'.

Selected to join the French Tech 120, a government program designed to nurture 25 unicorns by 2025, Atempo is headquartered in Paris and is present in Europe, the US and Asia with a partner network in excess of 100 partners, integrators and managed service providers.

Follow Atempo on social media:

-  <https://www.linkedin.com/company/atempo/>
-  <https://www.facebook.com/Atempo-Data-Protection-467109966988082/>
-  <https://twitter.com/Atempo>



For more information: [www.atempo.com](http://www.atempo.com).