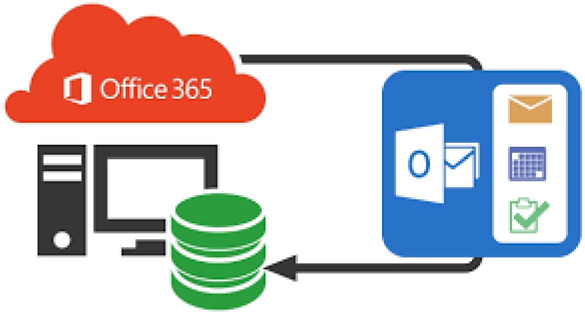
evotec
InfoBrief



7 Reasons why backing up Office 365 is Critical

Contact Evotec

Seven vulnerabilities in data protection

As a robust and highly capable Software as a Service (SaaS) platform, Microsoft Office 365 fits the needs of many organizations perfectly. Office 365 provides application Availability and uptime to ensure your users never skip a beat, but an Office 365 backup can protect you against many other security threats.

The average length of time from data compromise to discovery is over 140 days. A shockingly large gap. The likelihood is high that you

won’t notice something is missing or gone until it’s too late.

Accidental deletion
Retention policy gaps and confusion
Internal security threats
External security threats
Legal and compliance requirements
Managing hybrid email deployments and migrations to Office 365
Teams data structure

Accidental Deletion

If you delete a user, whether you meant to or not, that deletion is replicated across the network, along with the deletion of their OneDrive for Business account and mailbox.

There are two types of deletions in the Office 365 platform, soft delete and hard delete. An example of soft delete is emptying the Deleted Items folder. It is also referred to as “Permanently Deleted.” In this case, permanent is not completely permanent, as the item can still be found in the Recoverable Items folder.

A hard delete is when an item is tagged to be purged from the mailbox database completely. Once this happens, it is unrecoverable, period.

Retention policy gaps and confusion

The fast pace of business in the digital age lends itself to continuously evolving policies, including retention policies that are difficult to keep up with.

Office 365 has limited backup and retention policies that can only fend off situational data loss, and is not intended to be an all-encompassing backup solution.

In the case of a catastrophic issue, a backup solution can provide the ability to roll back to a previous point-in-time prior to this issue and saving the day.

With an Office 365 backup solution, there are no retention policy gaps or restore inflexibility. Short term backups or long-term archives, granular or point-in-time restores, everything is at your fingertips making data recovery fast, easy and reliable

Internal Security threats

Organisations can fall victim to threats posed by their very own employees, both intentionally and unintentionally.

Access to files and contacts changes so quickly, it can be hard to keep an eye on those in which you've installed the most trust. Microsoft has no way of knowing the difference between a regular user and a terminated employee attempting to delete critical company data before they depart. In addition, some users unknowingly create serious threats by downloading infected files or accidentally leaking usernames and passwords to sites they thought they could trust.

External security threats

Malware and viruses, like ransomware, have done serious damage to organisations across the globe. Not only is company reputation at risk, but the privacy and security of internal and customer data as well.

External threats can sneak in through emails and attachments Exchange Online's limited backup/recovery functions are inadequate to handle serious attacks**. Regular backups will help ensure a separate copy of your data is uninfected and that you can recover quickly.**

Legal and compliance requirements

Sometimes you need to unexpectedly retrieve emails, files or other types of data amid legal action.

Microsoft has built-in a couple of safety nets (litigation hold and retention). But, these are not a robust backup solution that will keep your company out of legal trouble.

Legal requirements, compliance requirements and access regulations vary between industries and countries, but fines, penalties and legal disputes are three things you don't have room for on your to-do list.

Managing hybrid email and Migrations

The right Office 365 backup solution should be able to handle hybrid email deployments, and treat exchange data the same, making the source location irrelevant.

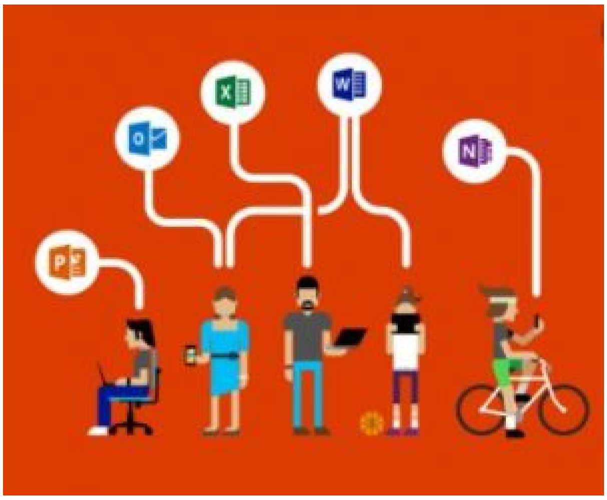
Furthermore, you should be able to store the data anywhere you choose, whether on premises, in cloud object storage such as AWS S3 or Azure Blob, or with a managed service provider

Teams data structure

Microsoft Teams is gaining rapid adoption and growth with the increase in remote working. It's now the centre of our productivity universe.

You need to protect data in all locations, but that's not all you need to protect. Teams has settings, configurations, and membership which all need to be protected and recoverable. A purpose-built backup solution can protect not only the data but also these settings and their associated interconnections between applications.

Backups can also help in short-term scenarios. For example, if an employee says something inappropriate in a Teams conversation, but then deletes the message, having a backup would make those chats recoverable and available to HR for review. Third-party backup vendors not only provide protection from the unknown but can also offer a variety of ways to restore missing or accidentally deleted teams or channels.



The scary reality is that even though sensitive cloud data is stored in Office documents, an estimated 76% is not being backed up2. In fact, IDC states that 6 out of every 10 organizations don’t have a data protection plan for their Office 365 estates3. Do you work in one of these unprotected organizations? If so, hopefully you now have the insights available through this report to encourage your organization to protect its Office 365 data.

Contact Evotec Today