CloudCover 365

The essential backup guide to Microsoft 365 and Teams.

THIS REPORT COVERS

The Microsoft 365 backup myth

7 reasons to back up Microsoft 365 and Teams

Ensuring 365 and Teams availability

Veeam Microsoft 365 virtualDCS

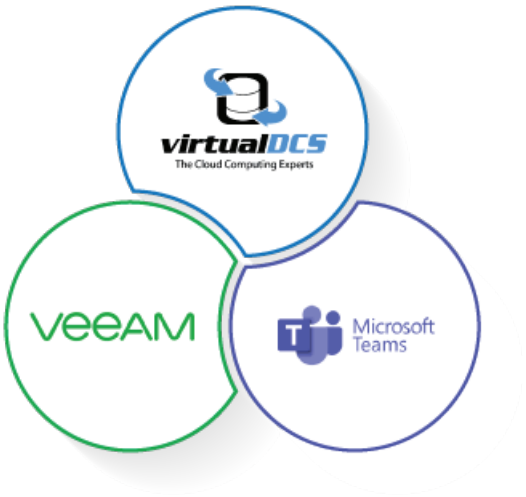
Is your Microsoft 365 data at risk?

One undeniable side effect of the global Coronavirus pandemic has been the increased reliance on remote working and cloud-based technologies.

Face to face meetings and office socialisation has been replaced with video, voice and instant messaging alternatives. Microsoft Teams was already growing rapidly as a staple tool within modern businesses before the pandemic but has quickly become indispensable, with over 115 million daily active Teams users. Now, like any other business-critical application, Microsoft Teams data needs to be protected to guarantee its recovery should an incident occur.

The complexity of Microsoft Teams backup

Microsoft Teams doesn't store information in a dedicated Teams folder, as many would expect it to. As the software interlaces with other Microsoft services, it stores data across multiple service folders. Where it is stored exactly, depends on what feature is being used.



All Chat messages sent through Teams (both team channels and direct) are collected within Exchange folders. On the other hand, every single team and channel an organisation creates is stored within SharePoint folders as an independent site.

When you send a file to a colleague directly, the file is stored in a "Microsoft Teams Chat Files" section in the user's personal OneDrive. However, if you send a file within a channel to multiple colleagues, it can be found within the SharePoint document library so that everyone within the channel can see.

With this in mind, there's no wonder that data can be left behind and the most effective way of protecting Teams data is to have a complete Microsoft 365 backup solution in place.

The shared responsibility model: 365 data isn't automatically protected

There is a common misconception that data in the cloud is inherently safe. Many organisations don't realise that although Microsoft is responsible for managing the infrastructure, it isn't responsible for data backups.

This leaves many unknowingly at risk of significant data loss and this applies to all services across the Microsoft 365 platform, not just Microsoft Teams.

Although Microsoft has some 'safety nets' in place, they come with gaping holes, which are not enough for modern organisations today - especially if they rely on Microsoft 365 data to function, and Teams to collaborate and connect.

Microsoft's responsibility:
Uptime of the Microsoft 365 cloud service. ✓

The user's responsibility:
Access and control of data residing in Microsoft 365. ✗

The 365-backup myth

What organisations assume they are getting, and the backup and recoverability services that Microsoft provides are often different, leaving many businesses to re-assess their Microsoft 365 and Teams data protection strategy, along with the level of control they have within the software overall.

"We strongly advise you to make regular back-up copies of Your Content. Microsoft can't be held responsible for Your Content or the material others upload, store or share using our Services."
– Microsoft Terms and Conditions

What protection does Microsoft actually offer?

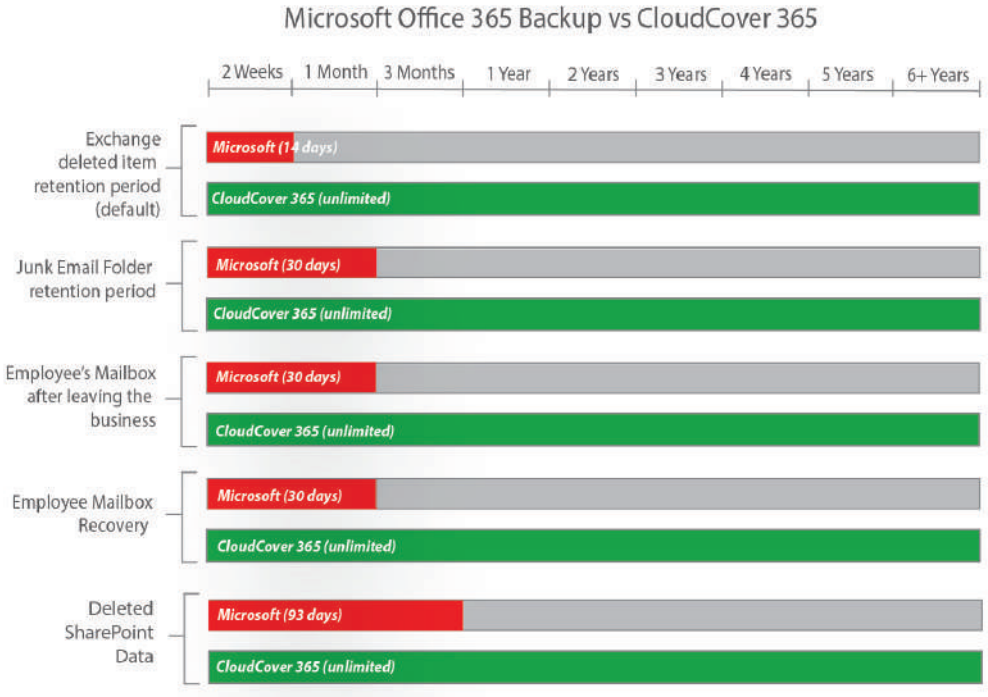
Microsoft 365 offers geo-redundancy protection which can often be mistaken for backup.

Microsoft is responsible for ensuring all elements of its 365 service are available for use. Geo-redundancy provides this as it protects against hardware or site failures, meaning that if there is an infrastructure issue or outage the software will automatically run on a secondary infrastructure in another location, so users have consistent access. Microsoft is not responsible for ensuring data availability for its users.

With backup, a copy of the data is made and stored in another location. This means that if data is lost, deleted or attacked there will be an easily accessible copy elsewhere and this isn't provided as standard with Microsoft 365.

Default Microsoft 365 policies

If an organisation doesn't provision their own backup solution, their data uses Microsoft 365's default policies which are limited. These settings typically only protect data for 30-90 days and some data is even automatically deleted after 14 days.



Seven reasons to backup Microsoft 365

History has proven that it is vital to back up your resources within the Microsoft 365 cloud - especially if you are using Microsoft Teams - and if you want to back up Teams, then you need to have a complete Office 365 backup solution in place.

Working with Veeam, we've identified seven common pitfalls in data protection for the modern organisation when using Microsoft Teams and the 365 suite.

1

Accidental deletion

More collaboration provides a greater chance of human error. Microsoft 365 and Teams data can be edited or deleted from many different sources. If an administrator deletes a channel, or user, the change automatically replicates across the network and deletes all associated data, including personal OneDrive information.

As explained previously, native recycle bins and version histories within Microsoft 365 are very limited and once items are purged from their deleted items folder they become unrecoverable. It's also worth noting the recovery mechanisms that Microsoft provides as standard may not assist if a file was accidentally overwritten, rather than being deleted.

2

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, let alone manage! It is difficult to verify that these policies have been enabled for every application and data source throughout an entire organisation, and that policies have been set to the required durations, especially across the multiple locations where Teams data is stored.

With a complete Microsoft 365 backup solution in place there are no retention policy gaps or restoration inflexibility. Using the 'complete backup' function within CloudCover 365 ensures your Microsoft Teams data is completely protected. 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.

3

Internal security threats

Security threats don't just include hackers and viruses – organisations experience threats from the inside more often than you think. Internal security threats come in a variety of forms, but the majority are tied to a user with malicious intent, and it can be difficult to predict when employees pose a threat. Some may even use insider-knowledge after departing to hack and damage internal systems. A 365 backup solution won't stop employees being malicious, but it will provide reliable recovery.

- Microsoft has no way of knowing the difference between a regular user and a terminated employee attempting to delete critical company data.
- Some users unknowingly create serious threats by downloading infected files or accidentally leaking user-names and passwords to sites they thought they could trust through Phishing.
- An employee could strategically delete incriminating emails or files, keeping these objects out of the reach of the legal, compliance or HR departments.

4 External security threats

Malware and viruses, like Ransomware, have done serious damage to organisations across the globe, risking company reputation, privacy and security of both internal and customer data.

External threats can sneak in through emails and attachments, and it isn't always enough to educate users. Microsoft 365's limited backup/recovery functions are inadequate to handle serious attacks. Regular backups ensure a separate copy of data is uninfected and quickly recoverable - acting as your final line of defence against external threats.

5 Legal and compliance requirements

Many organisations are subject to regulatory requirements, such as health, education and legal sectors, where they need to retain information for compliance. It is difficult to enforce retention policies without a back up solution in place and it becomes even more complicated when reflecting on Teams data storage locations.

Microsoft's default policies are not a robust backup solution capable of handling modern data retention requirements. One of the best ways to ensure Team's retention compliance is to back up the data with an associated retention period. That way, the organisation can guarantee backup data will be preserved for the required time frame.

6 Managing hybrid email deployments and migrations to Office 365

Organisations adopting Microsoft 365 typically need a transition window when migrating from on-premise Exchange to Microsoft 365 Exchange Online. Some businesses even leave a small portion of their legacy system in place to have added flexibility and additional control.

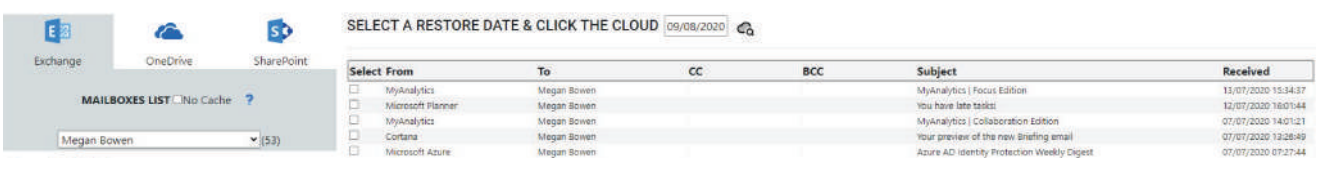
These hybrid email deployments are common, but they pose additional management challenges. The right Microsoft 365 backup solution should protect hybrid email deployments, and treat exchange data the same, making the source location irrelevant.

7 Teams data structure

Microsoft Teams is structured as a user interface that brings together 365 services including SharePoint Online and OneDrive for Business to provide agile, real-time communication and team collaboration.

Businesses need to not only protect data across these locations, but Teams also has settings, configurations, and memberships which all need to be protected and recoverable.

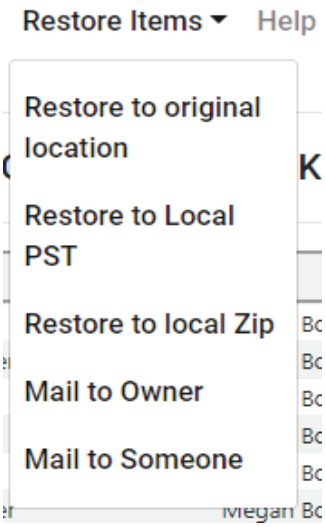
Organisations need a backup solution that offers both complete long-term access and control of Office 365 data, including Microsoft Teams, to avoid the unnecessary hazards of data loss. CloudCover 365 can help.



Complete backup for Microsoft 365

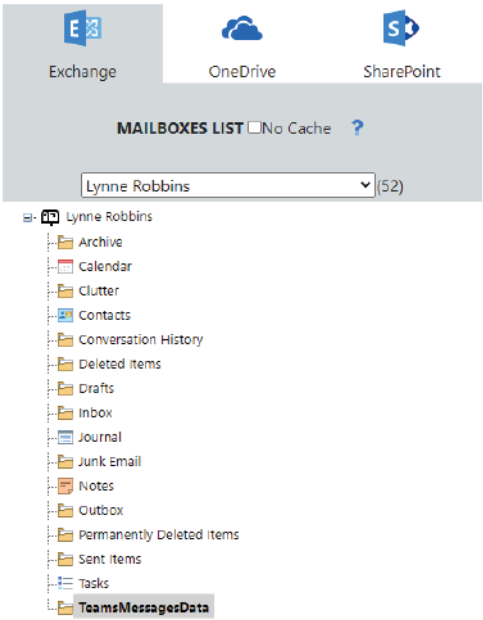
CloudCover 365 was created to alleviate Microsoft 365 backup gaps and put organisations in control of their 365 data for the first time.

Using the newly released API for Teams, combined with our latest update, your organisation can now take advantage of purpose-built backup and recovery for Microsoft Teams, making it easier than ever for users to quickly find and restore Teams data, from entire Teams, to specific channels and settings.



With CloudCover 365, you could:

- Protect Microsoft 365 data, including SharePoint, OneDrive, Teams and Exchange from accidental deletion, security threats and retention policy gaps.
- Restore an individual Microsoft Teams file, or an entire folder instantly.
- Restore data to its original location, local PST, ZIP file, or even email it directly to the end-user through the browser-based portal.
- Utilise unlimited repositories and keep sensitive data archived with no Microsoft purge time limits.
- Select and protect the Microsoft 365 data that matters to you. From specific items to individuals, to folders or an entire organisation.
- View full backup history, including what happened and when.
- Manage users from one easy interface and reduce file recovery requests, with the option to enable end-user self-service for restores.
- Avoid costly investments and access an easy to use, comprehensive solution on a pay-monthly basis.
- Secure backups with your own encryption key and stop data changes with immutability for compliance.
- Create custom backup jobs and retention periods to suit your requirements, with specific backup time slots around your working hours and IT schedules.



The winning team: Veeam and virtualDCS.

Award-winning technologies from Veeam and virtualDCS have combined to create one trusted Microsoft 365 backup solution.

CloudCover 365 is the only Veeam powered Microsoft 365 backup portal to offer end-user restore capabilities. Before CloudCover 365, organisations and IT suppliers would have had to invest heavily to achieve a similar solution, but now, working together, users can take advantage of a comprehensive 365 backup solution like no other, with next-level protection for Microsoft Teams.

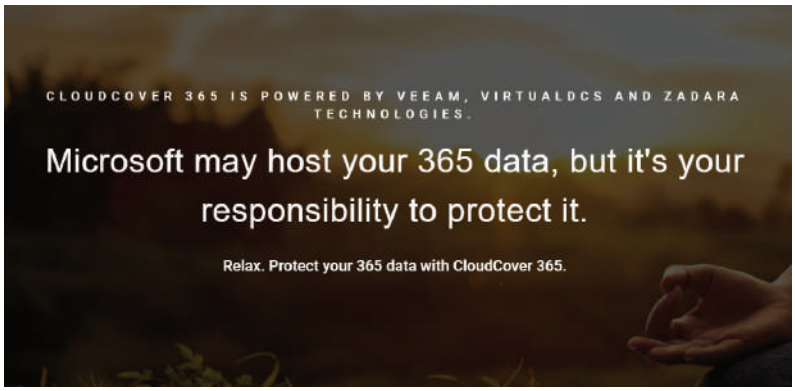
VEEAM

When founded in 2006, Veeam quickly became a leader in backup with the fastest and most reliable data recovery in virtual environments. Regardless of where data resides – physical systems, SaaS services, public cloud, private cloud, hybrid cloud, or multi-cloud – Veeam helps hundreds of thousands of companies keep their businesses running. Veeam has continued to charge forward the industry and deliver simple, flexible and reliable solutions to 400,000+ customers.

virtualDCS

Founded in 2008, virtualDCS remains one of the UK's most established, innovative cloud computing companies and the authors of CloudCover 365 - the world's only Veeam self-service Microsoft 365 portal.

Working in partnership with Veeam for over 10 years, virtualDCS is proud to be a Veeam Gold Partner and the glue that binds the CloudCover 365 solution together, through its innovative console. CloudCover 365 entirely hosted and managed by virtualDCS in the UK.



For a free 14-day trial of CloudCover 365 or to find out more about our unique backup solution visit our website or call +44 (0) 3453 888 327