CloudCover 365

6 Reasons to backup your Microsoft 365 data

THIS REPORT COVERS

The Microsoft 365 backup myth

Common 365 backup vunerabilities

Ensuring Microsoft 365 availability

veeAM

virtualDCS

zadara

Is your Microsoft 365 data at risk?

Microsoft 365 is now a staple in today's business world and a lifeline for organisations that are remote working through the recent pandemic. Although it is heavily relied on, do you feel like you have control of your organisation's Microsoft 365 data?

Their typical answer is "Of course I do," or "Microsoft takes care of it all", but this often isn't the case.

"~~Microsoft already protects my 365 data as part of the service, so I don't need to do anything.~~"

There is a common misconception that SaaS data in the cloud is inherently safe. What most don't realise is that although Microsoft is responsible for the software, it isn't responsible for data backups.

This leaves organisations at risk of significant data loss, including emails, OneDrive files, contacts and more. 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.

If an employee deletes a critical project file or an entire folder of customer orders; with no backup, there's no guarantee that this information would be recoverable.

This report explores the hazards of using Microsoft 365 without a backup solution in place and why your organisation should consider 365 backup to fill the gap to ensure data availability and long-term data retention.

Email	Calendars	Contacts
Public folders	SharePoint online	OneDrive for business

The 365-backup myth

The backup and recoverability services that Microsoft provides and what organisations assume they are getting are often different, leaving many to re-assess their data protection strategies and the level of control they have within the software.

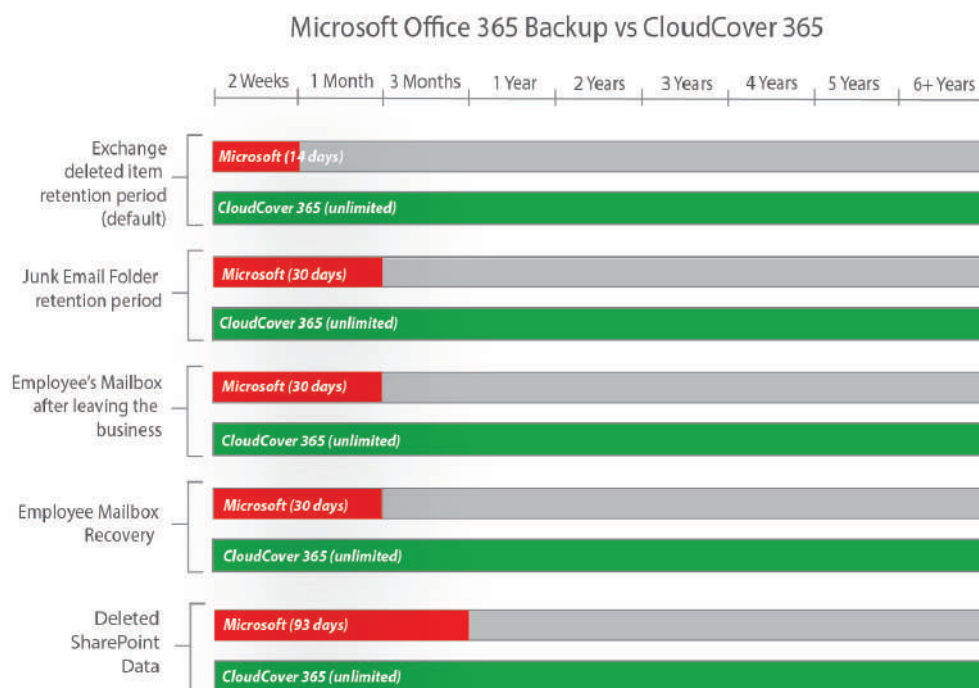## What protection does Microsoft 365 actually offer?

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

Geo-redundancy protects against hardware or site failures, which means 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.

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.

Microsoft Office 365 Backup vs CloudCover 365

	2 Weeks	1 Month	3 Months	1 Year	2 Years	3 Years	4 Years	5 Years	6+ Years

Exchange deleted item retention period (default)
- Microsoft (14 days)
- CloudCover 365 (unlimited)

Junk Email Folder retention period
- Microsoft (30 days)
- CloudCover 365 (unlimited)

Employee's Mailbox after leaving the business
- Microsoft (30 days)
- CloudCover 365 (unlimited)

Employee Mailbox Recovery
- Microsoft (30 days)
- CloudCover 365 (unlimited)

Deleted SharePoint Data
- Microsoft (93 days)
- CloudCover 365 (unlimited)

Why Backup Microsoft 365?

Many consider backup an insurance policy, taking an 'it will never happen to me approach'.

Working with Veeam, we've identified six common pitfalls in data protection for the modern organisation. The key reasons businesses should backup Microsoft 365 include: accidental deletion, retention policy gaps and confusion, internal security threats, external security threats, legal and compliance requirements and managing hybrid email deployments and migrations to Office 365.

1

Accidental deletion

If an administrator deletes a 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 it is unrecoverable. In this example, the default retention periods 'hard delete' user data after 30 days.

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! Microsoft's default policies don't allow for a point-in-time restoration of data, not to mention any additional changes to the software's policies.

Microsoft 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. With the correct solution in place there are no retention policy gaps or restoration 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.

3

Internal security threats

Security threats don't just include hackers and viruses – organisations can also experience threats from the inside, and they are happening more often than you think. Businesses fall victim to threats posed by their very own employees, both intentionally and unintentionally. For example:

- 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.
- 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. Not only is company reputation at risk, but also the 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 on what to look out for. Exchange Online's limited backup/recovery functions are inadequate to handle serious attacks. Regular backups will help ensure a separate copy of data is uninfected and quickly recoverable.

5 Legal and compliance requirements

Sometimes you need to unexpectedly retrieve emails, files or other types of data amid legal action. This is especially true for health, education and legal sectors that need to retain information for sector compliance.

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. Microsoft's default policies are not a robust backup solution capable of keeping any company out of legal trouble.

6 Managing hybrid email deployments and migrations to Office 365

Organisations adopting Microsoft 365 generally need a transition window when migrating from on-premise Exchange to Microsoft 365 Exchange Online. Some 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 be able to handle hybrid email deployments, and treat exchange data the same, making the source location irrelevant.

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

Access the power to securely backup 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.

With CloudCover 365, you could:

- Protect Microsoft 365 data, including SharePoint, OneDrive and Exchange from accidental deletion, security threats and retention policy gaps.

- Select and protect the Microsoft 365 data that matters to you. From specific items to individuals, to folders or an entire organisation.

- Restore data to its original location, local PST, ZIP file, or even email it directly to the end-user through the browser-based portal.

- 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 and pick specific backup time slots to suit your working hours and IT schedules.

- 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.

Restore Items ▾   Help

Restore to original location

Restore to Local PST

Restore to local Zip

Mail to Owner

Mail to Someone
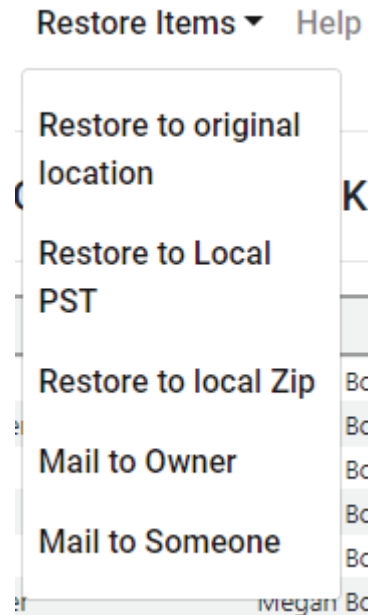
EDIT BACKUP JOB   Help

Selected items to backup
○ Backup Entire Organisation
◉ Backup the following Items

Object	Type	✉	📇	☁	▣	✉	👥
Allan Deyoung	User	☑	☑	☑	☑	☐	☐
Brian Johnson	User	☑	☐	☐	☐	☐	☐
Cameron White	User	☐	☐	☐	☑	☐	☐
Christie Cline	User	☐	☑	☐	☐	☐	☐
Conf Room Adams	User	☑	☐	☐	☐	☐	☐
Conf Room Baker	User	☐	☐	☑	☐	☐	☐

[Add User(s)] [Add Groups(s)] [Add Site(s)] ☐No Cache

[Previous] [Next] [Cancel]

The winning team:
Veeam, virtualDCS and Zadara technologies.

Technology from three award-winning data management leaders has combined to create one trusted Microsoft 365 backup solution.

Before CloudCover 365, organisations and IT suppliers would have had to invest heavily to achieve a similar solution, but now, working together, organisations can take advantage of a comprehensive 365 backup solution like no other.

veeAM

When founded in 2006, Veeam quickly became a leader in backup with the fastest and most reliable data recovery in virtual environments. They have continued to charge forward the industry and deliver simple, flexible and reliable solutions to 375,000+ customers.
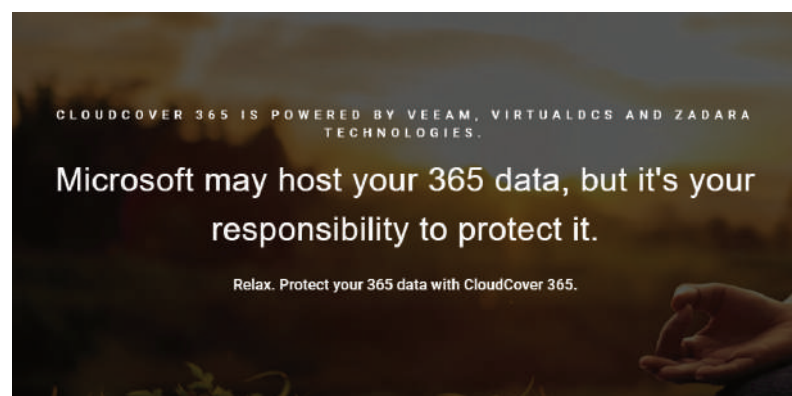
virtualDCS

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.

zadara

In 2011 a team of storage industry veterans recognised a problem. Companies were taking too much risk with their enterprise data storage systems: technical risk, operational risk, and (of course) financial risk. We set out to change that, and Zadara was born. With the introduction of the world's first enterprise storage -as-a-service offering, we're on a mission to provide 'zero-risk' enterprise data storage and management. As part of the trio, Zadara provides object storage services for CloudCover 365.

CLOUDCOVER 365 IS POWERED BY VEEAM, VIRTUALDCS AND ZADARA TECHNOLOGIES.

Microsoft may host your 365 data, but it's your responsibility to protect it.

Relax. Protect your 365 data with CloudCover 365.

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