Veeam Backup *for Microsoft Office 365*

The Control and Protection Required for Your Office 365 Data

Insight®

VEEAM

6 reasons
why you should backup Microsoft 365

1	**Accidental Deletion** – When a file is hard deleted it means it is tagged to be purged from the mailbox database completely. Once this happens, the item is unrecoverable.
2	**Retention Policy Gaps** – point-in-time restoration of mailbox items is not in scope with Microsoft, M365 has limited backup and retention policies which only fend of situational data loss, and is not intended to be an all-encompassing backup solution.
3	**Internal Security Threats** – which could be brought out by a terminated employee or a user unknowingly downloading infected/corrupt files.
4	**External Security Threats** – Including Malware and Viruses, regular backups using a comprehensive backup solution will ensure a separate copy of your data is uninfected and that you can recover quickly.
5	**Legal and Compliance Requirements** – If you need to unexpectedly retrieve emails, files or other types of data amid legal action, you need a robust backup solution to keep your company within compliance. If you accidentally delete a user, their on-hold mailbox, personal SharePoint site and OneDrive account is also deleted.
6	**Managing hybrid email deployments and migrations to Office 365** – hybrid email deployments are common, yet pose additional management challenges. The right Microsoft 365 backup solution will be able to handle hybrid email deployments and treat exchange data the same, making the source location irrelevant.

The Office 365
Shared Responsibility Model

	Primary Responsibility	Supporting Technology	Security	Regulatory
Microsoft's Responsibility	**Microsoft Global Infrastructure** Uptime of the Microsoft Office 365 Cloud Service	**Office 365 Data Replication** DC to DC geo-redundancy **Recycle Bin** Limited, short term data loss recovery (no point-in time recovery)	**Infrastructure Level** • Physical Security • Logical Security • App-Level Security • User/Admin Controls	**Role as a Data Processor** • Data Privacy • Regulatory Controls • Industry Certifications *HIPPA, Sarbanes-Oxley*
Your Responsibility	**Your Office 365 Data** Access and control of your data residing in Office 365	**Office 365 Backup** Copy of your data stored in a different place **Full Data Retention** ST & LT retention filing any/all policy gaps granular & point-in time recovery options	**Data Level** *Internal:* • Accidental Deletion • Malicious Insiders • Employee Retaliation • Evidence Tampering *External:* • Ransomware • Malware • Hackers • Rogue Apps	**Role as a Data Owner** • Answer to corporate and industry regulations • Demands from internal legal and compliance officers

Without a Backup of your O365 Data, you risk;

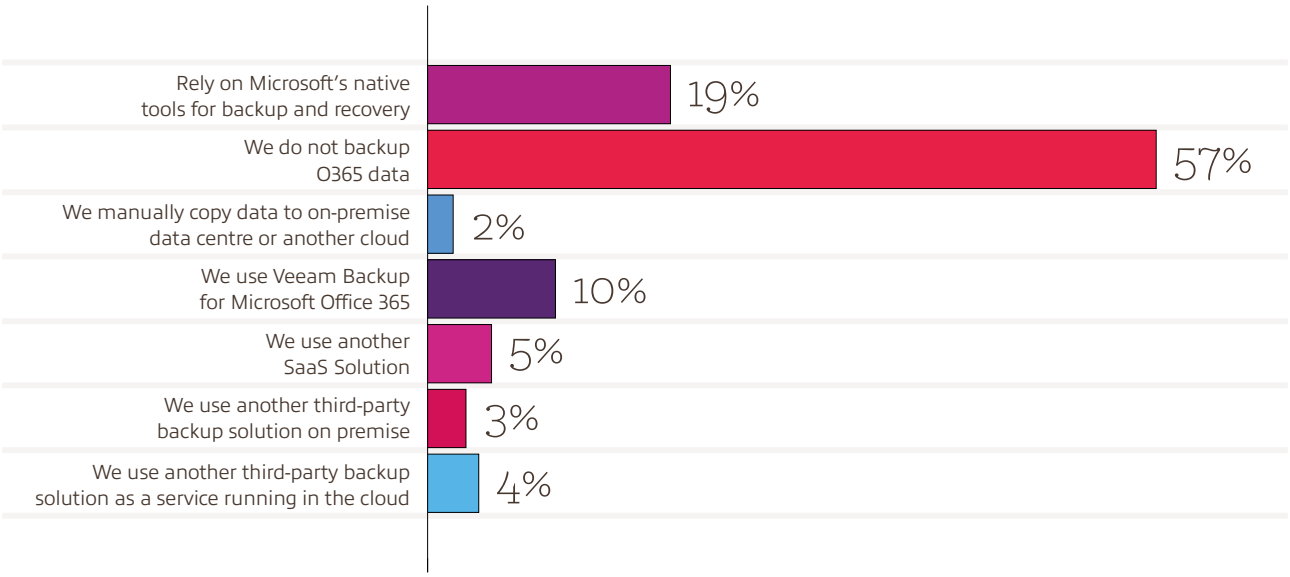
- Limited access and control of your own data
- Retention policy gaps and data loss dangers
- Security vulnerabilities
- Regulatory Exposure

In section 6.b. of the Microsoft Services Agreement it states that:

"We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages. In the event of an outage or disruption to the Service, you may temporarily not be able to retrieve Your Content. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services."

According to IDC (May 2019) – nearly 60% of organisations do not have a data protection plan for their O365 environments or rely on the native Microsoft capabilities.

According to a Veeam 2019 Survey, the below were customers M365 protection strategies:



A closer look at the
Retention Policies

Microsoft Retention Policy	1 week	1 month	3 months	1 year	2 years	5 years →
Inbox or folder data	In Office 365				Moved to archive	
Deleted items (recycle bin)	In Office 365	Permanently deleted				
Auto-archived data (set at 1 month)	In Office 365	Moved to archive				
Deleted Sharepoint Online sites and items	1st stage recycle bin	2nd stage	Permanently deleted			
Deleted OneDrive for Business files	1st stage recycle bin	2nd stage	Permanently deleted			
Employee leaves the company	In Office 365	Permanently deleted				

The average length of time from **data compromise to discovery** is over **140 days,** yet default settings only protect for 30-90 days*

What does Microsoft back up?

Veeam Retention Policy	1 week	1 month	3 months	1 year	2 years	5 years →
Inbox or folder data	Protected with Veeam					
Deleted items (recycle bin)	Protected with Veeam					
Auto-archived data (set at 1 month)	Protected with Veeam					
Deleted Sharepoint Online sites and items	Protected with Veeam					
Deleted OneDrive for Business files	Protected with Veeam					
Employee leaves the company	Protected with Veeam					

Veeam Backup *for Microsoft 365* is more than simply filling gaps.

It's about providing access and control to **all** Exchange Online, Sharepoint Online and OneDrive for Business data and **storing it in one location, making recovery fast, easy and reliable.**

Microsoft Office 365 eliminates the need to host your own emails, files and content management infrastructure, **but** it does not eliminate the need to back up your business critical data.

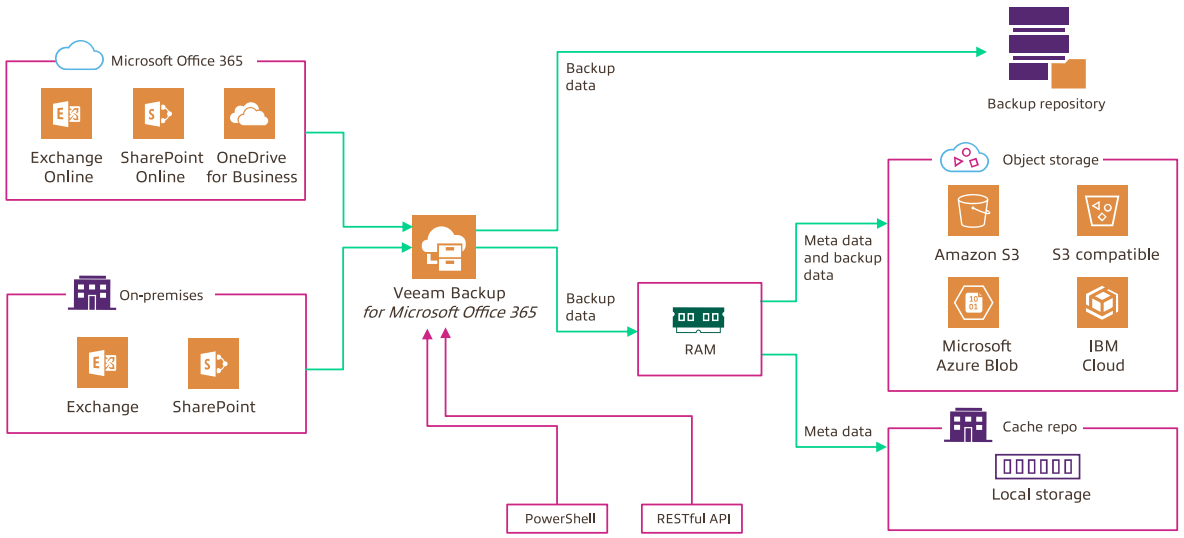
Microsoft is in charge of the infrastructure, but you are responsible for the protection and availability of your data.

**Microsoft Office 365, 6 steps to holistic security, chapter 1.*

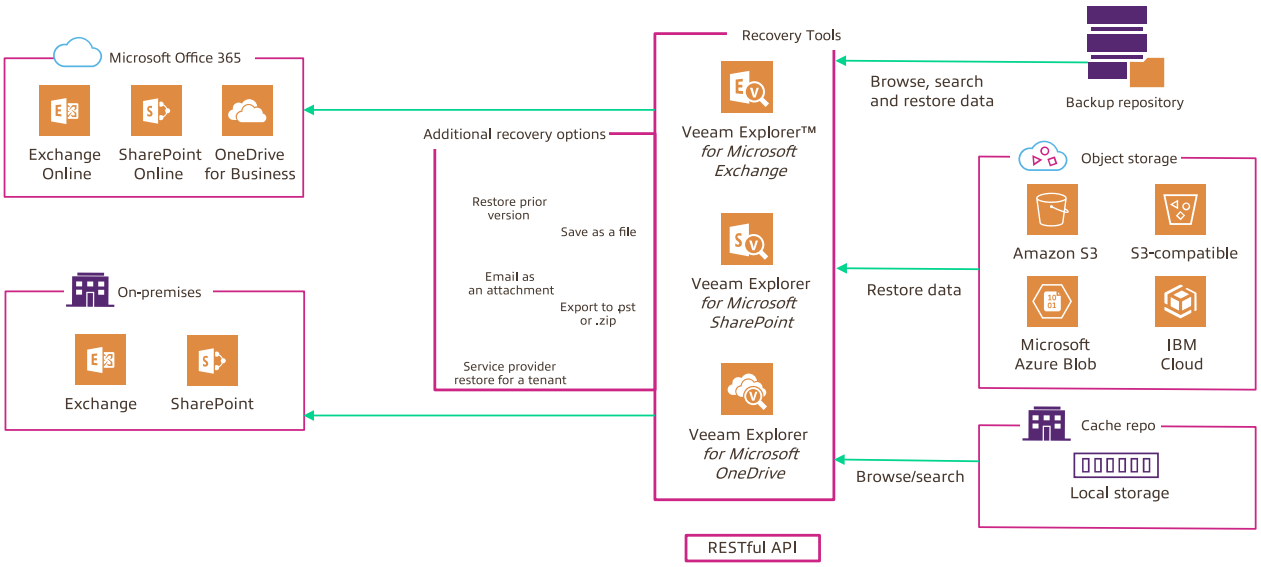
Solution Architecture
at a glance

Veeam Backup *for Microsoft Office 365*

Backup from on-premises and Microsoft Office 365 services to local or object storage



Delivering flexible restore options



Item-level retention
Select items to back-up based on the modification date for a specific retention period.

Snapshot-based retention
Based on point-in-time backup for the complete data set for a specific retention period.

Veeam® Explorer™ for Microsoft Exchange offers revolutionary technology that gives you instant visibility into Exchange backups, granular recovery of individual items and easy-to-use eDiscovery options — all without restoring the full Exchange database or entire server.

What's new
in Version 4

new

Object storage support delivers a cloud-optimised deployment option specifically for cloud-first companies, where users can leverage cost-efficient object storage to store Office 365 data — including AWS S3, Azure Blob, IBM Cloud and S3-compatible providers.

new

Added security with at-rest encryption for Office 365 data in object storage for peace-of-mind that your data is secure and protected.

new

Faster backup performance for SharePoint Online and OneDrive for Business data, shortening backup windows and ensuring you make your recovery time objectives and recovery point objectives.

Contact our dedicated Veeam specialist today to arrange a free demo

or visit: uk.insight.com/shop/veeam

Insight®

VEEAM

MKT4374