druva

Top five reasons for Microsoft 365 backup

Why you need a third-party backup solution

Introduction

The ways you deploy application software have changed dramatically as the internet expands. Instead of locally installing programs, you leverage the cloud with Microsoft 365 (previously known as Office 365) and other SaaS applications. Yet with the overwhelming success of Microsoft 365, there is confusion about its inherent data protection capabilities, as a SaaS solution, hosting data in the cloud. Protecting data is one of your top IT priorities. However, backup and restore functionality for Microsoft 365 applications such as Sharepoint, OneDrive, and Exchange Online, is often a misunderstood aspect of Microsoft 365.

Microsoft itself says it best in their service agreement:

"We recommend that you regularly backup your content and data that you store on the services or store using third-party apps and services."

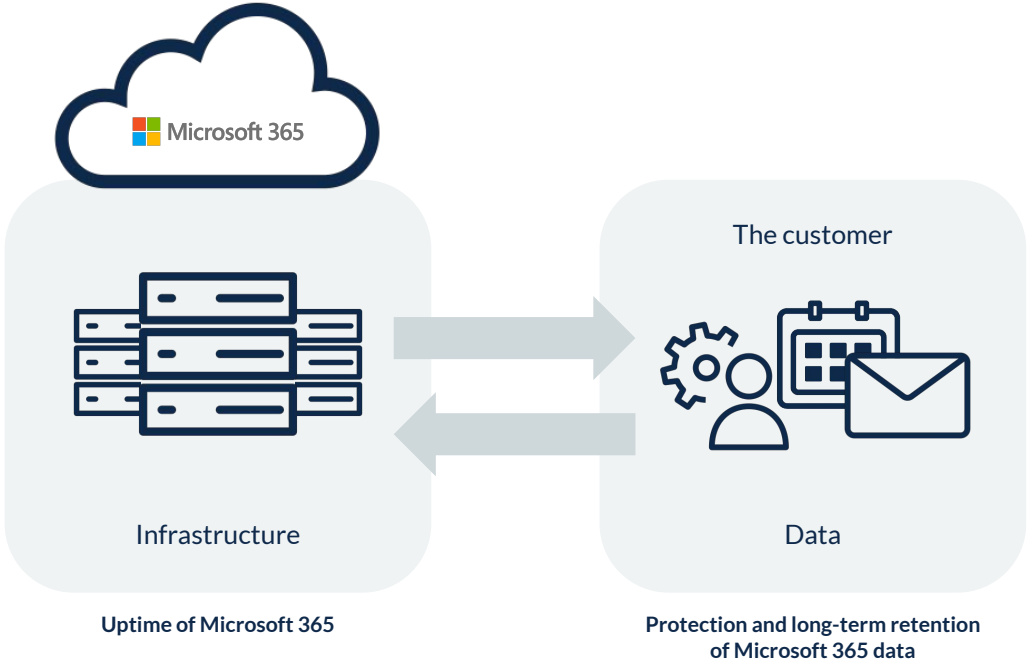
[1] 8/30/2019, https://www.microsoft.com/en-us/servicesagreement/

This eBook explains five important risk areas for your Microsoft 365 data and how you can mitigate these risks:

1. **Microsoft 365 data is prone to user error**
2. **Ransomware prevention is not enough**
3. **Data retention gaps risk non-compliance**
4. **eDiscovery and legal hold functionality falls short**
5. **Internal threats increase data risk**

druva

> **Microsoft 365 is a good offering that will satisfy a number of business requirements for security, archiving, data protection, encryption and other essential business processes, but it has some feature and function gaps that must be well understood before deployment. Many third-party solutions will do a better job at filling these gaps and should be evaluated and considered by decision makers.**
>
> — Osterman Research



Shared responsibility model of data stored in Microsoft 365

#1 | Microsoft 365 data is **prone to user error**

Ensure your data is protected when accidents occur

There's no question, end users and even admins occasionally delete files accidentally, overwrite files as they create and collaborate, or synchronize files incorrectly, potentially leading to data corruption. Even an entire team site may be inadvertently deleted. Overall, without a true Microsoft 365 backup solution, your valuable data is vulnerable.

In common cases, office workers may not realize their business-critical data was accidentally deleted until months later. For example, a well-intentioned intern tidies up the file system and moves a considerable amount of older project data to the Recycle Bin. They then permanently delete it — mistakenly believing they're saving the company storage space and money. Months later, after the intern's Microsoft 365 account has been deactivated, another group urgently wants the deleted data. Unfortunately the data would most likely be lost forever in this situation.

On the other hand, with an efficient third-party Microsoft 365 backup solution, your organization can achieve:

- **Regular point-in-time backups and unlimited retention** vs. the Microsoft 365 limited data retention capabilities
- **Bulk and granular point-in-time restores** vs. the limited recovery options provided by Microsoft 365
- **SLA requirements are met with quick recovery and self-serve options** vs. Microsoft 365's slower recovery times

So, the next time your business-critical data is accidentally deleted, you won't have to worry — a dedicated, third-party backup and restore solution is on your side.

> **"Cloud-native data protection and management provides a solution to the long list of problems our IT team encounters regularly.**
>
> — IT Director, San Jose Sharks

#2 | Ransomware prevention is **not enough**

Be prepared with cyber resiliency and keep business moving

If you manage an enterprise's IT team, you know that ransomware is a constant threat. For instance, a distracted executive will click on an innocent-looking link or a visitor will insert an infected flash drive.

Beyond perimeter security and protective hardware and software, you must be prepared with cyber resiliency and establish adequate recovery measures — ensuring your data can be bulk-recovered by IT reliably and quickly. As a result, users and businesses can continue to operate in the aftermath of a ransomware attack. Asking end-users to manually recover individual files, which may also be contaminated, isn't the answer. Your enterprise loses money every second that people can't work.

Effective SaaS backup solutions do what Microsoft 365 can't, enabling data protection that is:

- **Reliable** — quickly detect when an attack first occurred and identify which files were infected.
- **Comprehensive** — restoring an entire folder array is as easy and fast as restoring a single file or email.
- **Safe** — maintaining a copy of data in an independent, external location is a fundamental security rule.
- **Fast** — ransomware can cause wide-spread damages. Ensuring business continuity requires rapid bulk-recovery to pristine point-in-time data by IT.

If and when a ransomware attack strikes, you'll be armed and ready with a third-party backup solution.

> **"Very early on when we signed up with Microsoft 365, we knew that we wanted to be able to have a third-party store for the data.**
>
> — Director of IT Operations, Workforce Software

druva

#3 | Data retention gaps **risk non-compliance**

Meet compliance requirements with flexible and unlimited retention

Your organization must comply with state and federal regulations as well as corporate data governance policies. That's why data retention plays such a significant role. Certain industries like healthcare, for example, are obligated to keep data for more than seven years.

Unfortunately, Microsoft 365 doesn't quite meet the needs of your organization when it comes to retention duration and retention policies. It only provides 30-93 days of maximum retention and retains audit logs for six months. Since Microsoft 365 provides limited retention, it's difficult for organizations to comply with regulations.

But when you have a third-party backup solution in place, you will:

- **Receive unlimited data retention** options
- **Simplify** retention settings and eliminate complexity
- **Take advantage of a flexible audit history** with unlimited retention

Closing Microsoft 365 data retention and compliance gaps lets your organization fully satisfy compliance requirements.

> **"Apps like Microsoft 365, generally don't give you adequate backup, compliance, or other critical features.**
>
> — Director of IT and Cloud Operations, Frontier Silicon Ltd.

#4 | eDiscovery and legal hold **functionality falls short**

Ensure end-to-end legal hold support

To comply with eDiscovery and legal hold requirements and avoid costly penalties, legal teams must ensure that all case-related data, across your enterprise, is protected from accidental deletions and is quickly accessible.

In Microsoft 365 environments, recovering this data can be tedious and time-consuming, requiring IT overhead and end-user disruption. Higher-priced Microsoft Microsoft 365 enterprise plans offer some legal hold capabilities, but they are limited to Microsoft 365 data only — and this is one area where Microsoft 365 falls short — since data subject to legal holds could reside in other applications or on unsupported user endpoint devices.

Microsoft 365 also has limitations on formats, speed, and bulk recovery. Limited Microsoft 365 data retention policies and default settings may also impede your ability to provide key content, including departing employee data and intentionally deleted data. Lastly, Microsoft 365 does not provide fast integration with eDiscovery tools.

So, what can your organization do to meet eDiscovery and legal hold requirements? Consider a third-party backup solution that:

- **Provides comprehensive legal hold support** with no data retention limitations.
- **Automatically and fully collects data across enterprise workloads**, not just Microsoft 365 data, without disrupting employees.
- **Supports faster export speeds**, multiple file formats, and bulk custodian holds.
- **Integrates easily** with third-party eDiscovery tools.

With a third-party backup solution, your legal team is always prepared for litigation.

> **“[Cloud data protection] gives us full data visibility and 24×7 access …**
>
> — Head of IT, Policy Services

#5 | Internal threats **increase data risk**

Prevent data loss when employees depart your organization

When employees leave your organization, does business-critical data leave with them? Do you know if precious and sensitive data has been deleted or tampered with? It is not uncommon that departing employees may delete, hide, or tamper with important data. In many cases, these corrupt activities could have started months ago — and without a proper backup solution, there is no way to provide protection or conduct thorough data investigations.

Unfortunately, solely archiving the user's mailbox or OneDrive when employees leave is not an effective solution since the intellectual property has already been lost by then. Your organization also has no view into the history of the incident or the scope of data loss.

Yet, with a true third-party backup solution, you'll be able to:

- **Constantly capture data** (including deleted files or versions) with continuous backups and unlimited retention.
- **Isolate a copy of historic data** outside of the Microsoft 365 environment.
- **Restore data sets** back to the manager or even outside the Microsoft 365 environment.
- **Conduct data investigations and forensic analysis** with built-in search and analytics capabilities.

When you're prepped with all of the above capabilities, you'll have everything you need to stop data loss when internal threats impact your organization.

> **"[With Microsoft 365 backup], users never have to worry about deleting files since restore is only a click away.**
>
> — System Administrator, Wave Computing

druva

Microsoft 365 requires a third-party backup solution

A comprehensive, scalable, and cost-effective SaaS platform protects Microsoft 365 data, and other workloads, from major threats like accidental deletion, file corruption, insider attacks, ransomware, and non-compliance with data retention, legal hold and eDiscovery:

1. **If users overwrite or lose data, it's restored quickly.**
2. **If ransomware corrupts data, pristine, uninfected versions are readily available.**
3. **If industry regulations dictate data retention, you've got it, thanks to unlimited retention.**
4. **If litigation requires immediate access to user data, you have it.**
5. **If employees with malicious intentions hide or delete data, you've already safely backed it up.**

The right third-party backup solution does all of the above while providing true data isolation in an air-gapped environment (outside the Microsoft 365 environment) — which is critical from a risk and compliance standpoint.

Close the gaps in Microsoft 365 data protection: druva.com/microsoft365

Q122-20251

druva

Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva® delivers Data Protection and Management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted by thousands of companies worldwide, including over 50 of the Fortune 500. Druva is a privately held company headquartered in Sunnyvale, California, and is funded by Sequoia Capital, Viking Global Investors, CDPQ, Neuberger Berman, Tenaya Capital, Riverwood Capital, and Nexus Partners. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.