Microsoft 365

Microsoft 365 Backup: Best practices for data recovery and business continuity

Customers often ask, "do we need to back up our Microsoft 365 data? If so, what's the best way to do so?" The answer depends on specific scenarios and customer needs. This document offers the Microsoft 365 perspective on these questions to help you guide your organization's decision-making regarding backup and recovery solutions.

Our backup solution philosophy

When you buy a backup solution, you're really buying the ability to recover from a disastrous event, where it's vital to restore business operations and critical data as quickly as possible. This document focuses on Microsoft 365 data backup and restore, which have different responsibility and compliance models compared to other data sources. We aim to help you understand the shared responsibility model for Microsoft 365 and thus focus on areas that require additional consideration.

At this document's publication, more than 2.5 billion files are created in Microsoft 365 every day. Daily collaboration and generative AI drive massive storage growth in individual customer tenants. It's that growth, as well as complexity for IT admins in managing large-scale data, that requires a new breed of backup and restore solutions. Solutions that provide real recovery assurance and maintain Microsoft 365 security and compliance promises. It's critical to adopt a solution that works best for the most common recovery-reliant scenarios that can quickly return your data to a healthy state, so you can focus on your core business. It's essential to adopt a solution that meets the Microsoft 365 security, compliance, and privacy bar you have come to expect.

A deeper look

Maintaining business continuity and resiliency of critical business data and operations is top of mind for many customers. Achieving continuity and resiliency goals while keeping data secure, compliant, and private in the AI era and in the face of massive data growth requires solutions that rise to the challenge of modern software-as-a-service (SaaS) applications.

Customers generally look to acquire a backup solution to recover from various business-impacting catastrophic events. They often ask Microsoft what protections are natively provided and what additional solutions are needed to give them the best operational posture. The answer to that question depends on the nature of the event affecting their data:

1. Service failure: Microsoft 365 natively offers high availability and disaster recovery. This is covered in the Microsoft 365 data resiliency documentation. While no service has guaranteed 100% uptime, the key consideration is data durability and speed of recovery; both of which Microsoft 365 SaaS offerings handle robustly.

2. Customer-side data breaches: Because the customer is the controller of the data, the ability to recover from customer-side data issues – such as a ransomware attack or a case of mistaken deletion—requires a restore solution that provides a fast scaled recovery path to keep your business running. We recommend procuring either the native Microsoft 365 Backup offering or a recognized ISV application built on the Microsoft 365 Backup Storage platform. These solutions are best equipped to recover your tenant's data quickly at scale for optimal business resiliency and peace of mind.

3. Long-term retention, auditability, and discoverability: The Purview suite within Microsoft 365 provides excellent long-term retention features, including a feature that adheres to strict indelibility requirements. This ensures critical data will not be deleted, including versions of files kept in OneDrive and SharePoint. Microsoft 365 Archive provides cold-tier, low-cost SharePoint storage to help manage the costs and lifecycle of inactive content you must retain for an extended period.

4. Regulations in some industries or regions that require copies of data outside the service. While regulations vary by location and industry, our general stance is that this requirement is outdated regarding the shared responsibility model for SaaS offerings, which can lead to unexpected and undesirable outcomes. If needed, you should be aware of the copy's recoverability capabilities and ensure you have a sufficient solution for all your recovery needs.

Scenario-focused approach deep dive

We'll now briefly expand on the four scenarios we just summarized to provide better insight into what is and is not natively covered in Microsoft 365.

Service failure

Microsoft 365 has high availability and disaster recovery (HADR) resiliency built into all its services to address data durability and access reliability. You can read these Microsoft Learn articles to learn more: *SharePoint and OneDrive data resiliency in Microsoft 365*, *Shared responsibility model*, *Exchange Online data resiliency*, and *Data resiliency in Microsoft 365*.

Without restating everything in those linked articles, the various Microsoft 365 services have implemented proprietary technology to deliver a secure, resilient, and durable SaaS solution for your data.

Customer-side data breaches

Ransomware attacks and employee content modifications/deletions are becoming increasingly common. Microsoft 365 Backup defends against these events by keeping data in its natively encrypted format within the Microsoft 365 trust boundary, which allows us to retain the security, compliance, and privacy promises inherent in the service.

With Microsoft 365 Backup or an ISV solution built on the Microsoft 365 Backup Storage platform, you can back up and *more importantly* restore your OneDrive, SharePoint, and Exchange Online data at orders of magnitude faster speeds than otherwise possible, ensuring that you'll be able to get your data back to a healthy state soon after discovering an attack.

Long-term retention and other security and privacy scenarios

It's important to us that your data remains secure, compliant, and private. "Microsoft runs on trust" is one of our company's core tenets.

Microsoft 365 Backup Storage solves the need for fast backup and recovery without the additional risk of multiple security domains or application permissions to view or edit all of your tenant's data.

Multiple security domains are not only a challenge to manage, but also create more attack opportunities. Likewise, the complexities and challenges inherent in managing your data's compliance and privacy rules become more difficult when data is maintained over multiple systems.

The Microsoft 365 Backup Storage platform provides strictly scoped APIs to ensure no application in your tenant has overly permissive or broad access to your content. This aligns with our philosophy to limit and eliminate any application that has tenant-wide data access tokens to ensure that only those authorized can view data based on just-in-time access policies.

By keeping data within the Microsoft 365 trust boundary and utilizing Purview and SharePoint Advanced Management features, you can ensure your data is secure, compliant, and private.

External copy requirement

Some customers may have reasons for keeping a copy of some of their data outside of Microsoft 365. We generally do not recommend taking large quantities of data outside of Microsoft 365 and urge customers to think very carefully about the security, compliance, privacy, and recoverability (in terms of speed and context) of that content once moved outside the service boundary.

If some data does need to be taken out of the Microsoft 365 boundary, in Microsoft 365's opinion, it's best to keep it in Azure as opposed to other clouds or local data centers, as the network and operational efficiencies of doing so improve the likelihood of recoverability. Azure storage is not as powerful in terms of speed as a Microsoft 365 Backup Storage-based solution, but it is the recommended option if Microsoft 365 Backup Storage does not completely cover your needs.

Summary

When deciding whether you need a backup solution for your Microsoft 365 services, selecting a backup and restore tool that will meet the speed and scale needs of that data is paramount. Microsoft 365 has high availability and disaster recovery built natively into the service. A Microsoft 365 Backup Storage-based solution can help you recover from customer-side data breaches like ransomware attacks with exceptional speed. This means you can recover your operations in a matter of hours as opposed to weeks or months, so you can maintain optimal business continuity and resiliency within the Microsoft 365 trust boundary. We strongly recommend you think through your operational recovery plan and understand whether your current or planned backup tool truly meets your operational business goals.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.