Free Guide

# Stop Data Loss: Secure Microsoft Teams Data

## 6 vital actions to protect your Teams data

April 2021
Copenhagen

keepit®

# Table of Contents

# Introduction

Microsoft is striving to make Teams a digital platform as important to your business as the internet browser, and as vital as an operating system. Microsoft's CEO, Satya Nadella, has made it clear that Microsoft is on a mission to make Teams as integral as the internet browser by pulling together all the tools a worker needs to effectively conduct business into one platform.

To achieve this mission, Microsoft will ensure rapid adoption by as many users as possible, as quickly as possible, and they will add a variety of new features to Teams. The new functionalities and features will be continuously added, and while great for user workflow and performance, for businesses, it means less control of their platform. This can lead to significant data protection issues and compliance implications, especially true when a proper data protection strategy and backup solution is not in place.

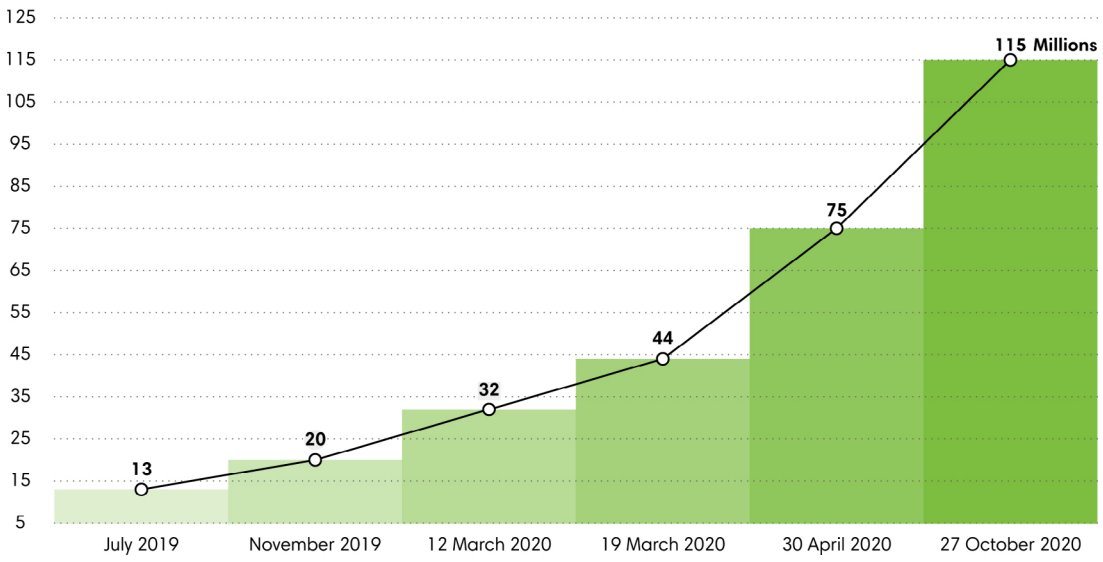
As companies rush to adopt Microsoft Teams to keep up with the demands of working remotely, data protection has never been more important and relevant in the face of the increased movement of data to the cloud and the democratization of data.

This whitepaper explores the pitfalls businesses expose themselves to when adopting Microsoft Teams and solely relying on Microsoft 365 to back up, archive, and manage their data. It will also explore why it is vital to explore third-party data protection and management solutions to avoid costly data loss and to ensure business continuity.

# Cloud Migration: New Gains, New Pains in Data Protection

Enterprise businesses are rapidly adopting cloud-based solutions like Microsoft 365 to meet many organizational needs. During 2020 alone, Microsoft cloud services saw more than a 50 percent jump in usage of their chat and collaboration platform Microsoft Teams. With the changing workplace requirements, companies are accelerating digitalization processes to access new levels of agility and flexibility.

Number of daily active users (DAU) of Microsoft Teams Worldwide (in millions):



Cloud migration has clear benefits, but it also comes with challenges, and many companies fail to implement a dedicated data protection strategy. Relying on a SaaS provider to keep data safe from data loss is not a data protection strategy - it can be risky and potentially detrimental to business continuity as SaaS providers are not responsible for backing up your data.

## Costly, Unrecoverable Data Loss Cases in Microsoft Teams

Whether unrecoverable data loss happens due to malware, ransomware, or human error, companies need to protect their SaaS data. Losing data without a backup solution that allows for searching, finding, and recovering data can be not only costly, but potentially fatal for companies:

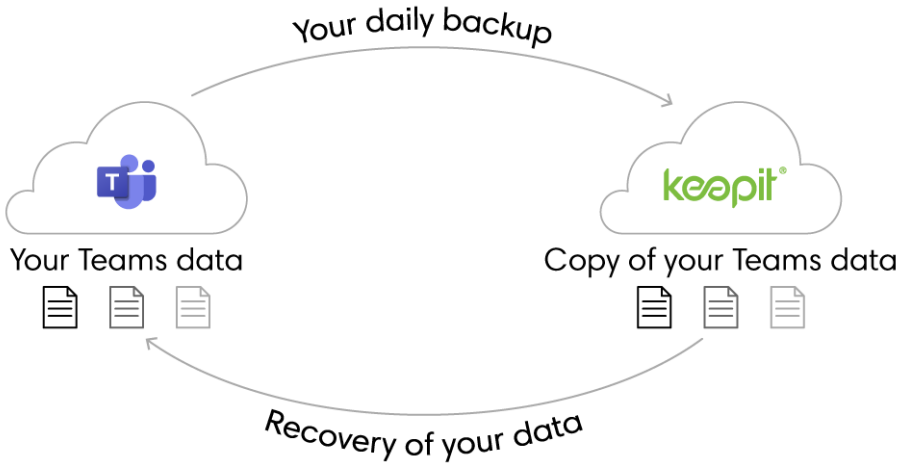
### Malicious Attack

A Carlsbad Company suffered severe business disruptions due to unrecoverable data loss within their Microsoft tenant. An IT contractor maliciously deleted 1,200 of the company's 1,500 Microsoft user accounts. As a result, the company's employees could not access Exchange, SharePoint, and Teams services. The company was completely shut down for two days, unable to communicate with external vendors and consumers. Contact lists could not be rebuilt, employees did not receive meeting invitations, and lost access to key folders. The IT department worked hard to resolve the problems, which persisted for 3 months, costing the company $567,000.

### Human Error

Malicious behavior is only one example of unrecoverable data loss possible in Microsoft Teams. Human error, such as accidental deletion or overwrites, is another elevated risk in collaborative platforms. KPMG, one of the largest global accountancy firms, suffered massive data loss inside Teams when an employee accidentally deleted 145,000 personal chat histories while attempting to remove only a single user's account from an active retention policy. The result: permanent deletion without the ability to recover any of it, with far-reaching impacts within the company's network.

**The takeaway:** The two data loss scenarios above could easily have been remedied had these companies implemented a dedicated cloud data protection solution like Keepit, which provides backup, smart search, and quick recovery of cloud data, regardless of the reason for data loss.



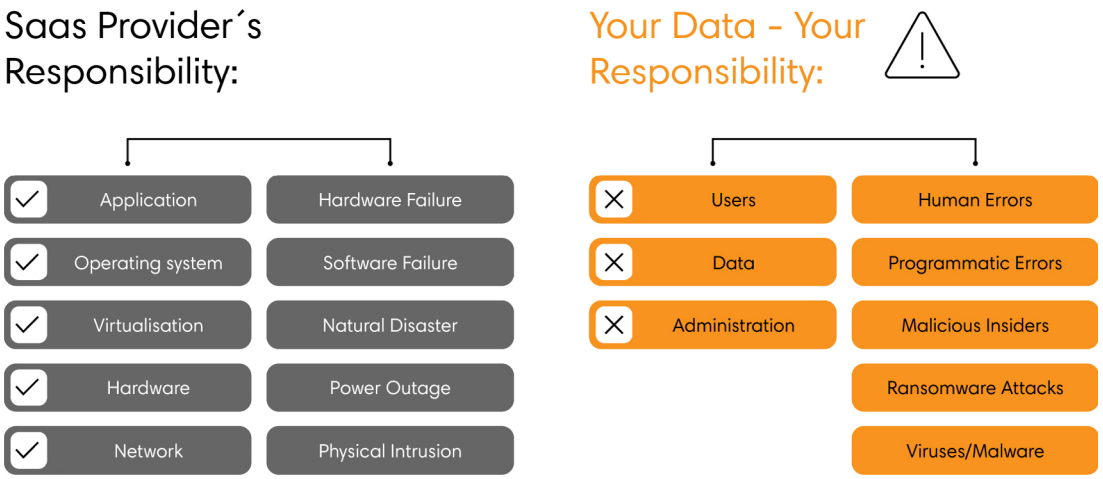
If you recently implemented Microsoft Teams, we have compiled five reasons why a data protection strategy for your Microsoft Teams data is crucial, along with the recommended actions you should take to start protecting your Teams data.

# 5 Reasons Why Data Protection for Microsoft Teams Is Crucial

## I. Microsoft Expects You to Back Up Your Data

The top reason for protecting your Teams data is quite obvious: Microsoft expects you to. Microsoft's responsibility is providing service infrastructure uptime, not backing up your data. Businesses overlook the fact that Microsoft is not responsible for backing up Teams data, nor do they guarantee recovery or protection against data loss (see Shared Responsibility Model below).

Outages and disruptions to the Microsoft infrastructure can pose a major threat to business continuity – especially if data in your Microsoft 365 account is lost or otherwise compromised. Backups in Azure will also be affected when Microsoft servers are down.



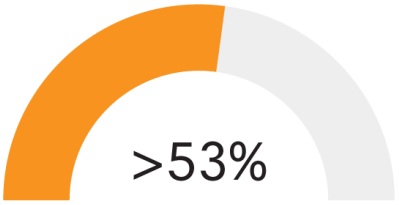
## II. The Sheer Complexity of Protecting and Managing Data

Microsoft Teams is built upon multiple Microsoft 365 and Azure services including SharePoint. One thing that makes backing up Teams data challenging is how the resulting data is stored, since it is scattered throughout Microsoft 365 (as seen below). To protect Teams data, you will need a data protection solution with complete Microsoft 365 coverage. Adding to the complexity of backing up Teams is all of the new features and changes to the Microsoft architecture. Data protection and management are demanding tasks, and with Microsoft's plans of significantly expanding Teams, it is not likely to become simpler:

| Teams data | Location | Backup Situation |
|---|---|---|
| Personal and group chat messages | Azure CosmosDB | Backed up with Keepit |
| Channel conversations | Azure CosmosDB | Backed up with Keepit |
| GIFs used in Teams messages | Teams CDN | Backed up with Keepit |
| Documents shared in personal and group chats | OneDrive for Business | Backed up with Keepit |
| Documents shared in Teams channels (Files) | Document libraries and folders in SharePoint Online sites | Backed up with Keepit via SharePoint Online. |
| Private channels | Separate set of SharePoint Online sites | Backed up with Keepit |
| Email sent to Teams channels via connector | Azure CosmosDB and SharePoint Online | Backed up with SharePoint Online (messages posted to channels are not backed up) |
| Messages posted to channels via Office connectors | Azure CosmosDB | No backup API available |
| Teams calendar | User and group mailboxes (Exchange Online) | Backed up with Exchange Online data |
| Teams meeting recordings | Stream | No Stream backup API available |
| Teams Wiki | SharePoint Online | Backed up with Keepit |
| Teams compliance records | Exchange Online mailboxes | Backed up with Exchange Online data |
| Planner | Azure | Planner backup API is available |
| Teams audit data | Office 365 audit log | Can be extracted with Search-UnifiedAuditLog (PowerShell) |
| Third-party apps | Teams app store and third-party repositories | Responsibility of third-party apps |
| Teams membership and group object | Azure Active Directory | Backed up with Keepit |
| Teams policies and settings | Azure | Some data can be backed up by reading policies and settings with PowerShell |
| Teams usage data | Microsoft Graph | Can be read from the Graph |

## III. Users Are the Weak Link

For the longest time, ransomware has been perceived as the single greatest threat to data loss, but insider threats and human error are significant risks that businesses need to consider in this era of digitization and democratization of data. In a recent report, Microsoft concluded that more than 53 percent of businesses have reported an insider attack in their organization during the past 12 months and that insider threats are becoming a real concern for most organizations.




Have reported an insider attack in their organization during the past 12 months

While insider threats are on the rise, innocent mistakes and human errors are also risks. As employees are getting increasingly tech-savvy through adapting new tools, they are not always fully aware of the security implications of their actions.

Data loss from human error and insider attacks can easily occur in Microsoft Teams due to the easy access users have to support effective collaboration and increased productivity. Users have access to business-critical data such as channel chats, files, plans, calendars, and conversations. However, this can be a double-edged sword, as the easy access can also lead to data loss through accidental overwrites and deletion. The recovery through Microsoft alone may be impossible, or, in the best-case, time-consuming and expensive.

## IV. Back Up Your Data Outside Microsoft's Domain

When designing a data protection and recovery strategy, businesses should consider the 3-2-1 strategy. A 3-2-1 backup strategy means having at least three copies of data: Two of these copies should be stored in different locations and one of the copies should exist independently off-site.

Using Microsoft including Teams means that you already have two copies stored in different locations, as Microsoft stores multiple copies of your production data across separate locations. However, if your production data inside Microsoft somehow gets corrupted, inaccessible or lost, it is your responsibility to have a third copy outside Microsoft's domain, so you can quickly restore that data back into place. A third copy should be stored with an independent cloud backup provider like Keepit, who offers a private and vendor neutral cloud along with multiple and mirrored data centers to ensure you always have access to all your data across time.

Supporting this view, analyst firm IDC also recommends that data backup must be a service outside of the data provider's domain to best protect your data.

## V. Losing Teams Data Is Expensive

The cost of data loss has been well documented over the years. From catastrophic weather events to disabling malware attacks, the IT organization is constantly juggling budget constraints with real-life business continuity risk. Thankfully, most companies will not experience a company wide data loss event. However, almost all companies will experience a data 'unavailability' scenario in the next few months. Whether driven by human error, infrastructure down time or malevolent attack, enterprises must be protected against data loss:

Energy, Oil & Gas

What if your most expensive drilling platform lays idle in the North Sea due to a Microsoft Cloud failure? Key seismic data stored in Microsoft is unavailable and platform engineers are unable to commence their drilling operations. What is the cost of the rig, the team and the thousands of barrels of oil, when it is not pumping oil? Data stored in public cloud is your responsibility to protect.

Financial Services

What if your FX traders learned that their models for the market open were not available? The models were built last evening for today's trading and were shared within the FX traders Teams account. When Teams is unavailable, how long does it take to recover the data if you have backed up to your legacy data center? Does your IT team provide you with a data availability SLA that allows your traders to execute, or will today's market be missed? What is the cost of a loss day in the FX market and what are the ramifications on the IT team?

Pharma

Today's largest Pharma companies have never had so much public brand recognition, every day the world is updated on the progress of vaccine development, trials and production data. What if it was determined that a ransomware attack on their Microsoft tenant including Teams had suddenly stopped the production plant of a key syringe manufacturer. How quickly would that manufacturer's name be in the worldwide news and what would the short- and long-term financial impact be to that supplier?

Data availability is a must have, not a nice to have. Enterprises globally are implementing cloud-based data protection services to ensure around-the-clock data availability. Data availability that is proven, secure, affordable and guaranteed.

keepit®

# 6 Actions to Protect Your Teams Data

Migrating to the cloud with Microsoft Teams brings exciting new possibilities for conducting business. But, with new possibilities often comes challenges. It is time to think about those challenges and how to start protecting your Teams data. To always stay in control of your Teams data, it is recommended that you look for a true third-party data protection and management solution to get the best protection for your Microsoft Teams data.

Data management and protection tools are not created equally, so we have collected six areas that you should consider when choosing a data protection solution:

### Centralize your data protection

Many businesses run a variety of SaaS applications that need data protection. Choosing one centralized solution to protect all your SaaS data is more convenient and efficient than having to manage and pay for separate point-solutions for each SaaS application.

### Look for simplicity

Microsoft Teams is complex to back up yourself. Therefore, you need to look for a data protection provider that turns the complexity of backing up Teams data into a simple task. To save yourself time and money on skilled IT staff, look for a simple solution that is easy, intelligent, and intuitive to integrate and runs every day.

### Plan for the future

Microsoft Teams is constantly adding new features. Understanding the breadth of the Teams coverage and how the data protection provider plans to develop and broaden their Teams coverage over time is important to make sure that the solution scales with your needs today and in the future.

### Security & data availability is key

Look for a data protection solution that brings your data outside of Microsoft's domain, allowing you to always access an off-site copy of your Teams data – even if Microsoft's cloud is down. This will protect you from losing your Teams data, as Microsoft does not back up your data for you.

### Stay compliant

Most businesses need to have a data management and protection solution that allows them to easily search, find, archive, and share specific data (as well as specific versions of data) with their legal team to document to auditors that data is stored and protected according to regulations.

### Predictability matters

Look for a data protection solution that has a wide range of cloud service protection for SaaS applications that also meets your data retention policies and offers predictable pricing to avoid unpleasant and costly surprises in case your data storage needs increase over time.