GIBRALTAR®
DRIVING DIGITAL TRANSFORMATION

2023

PREVENT MICROSOFT TEAMS DATA LOSS

CHALLENGES & BEST PRACTICES

gibraltarsolutions.com

Table of Contents

Introduction

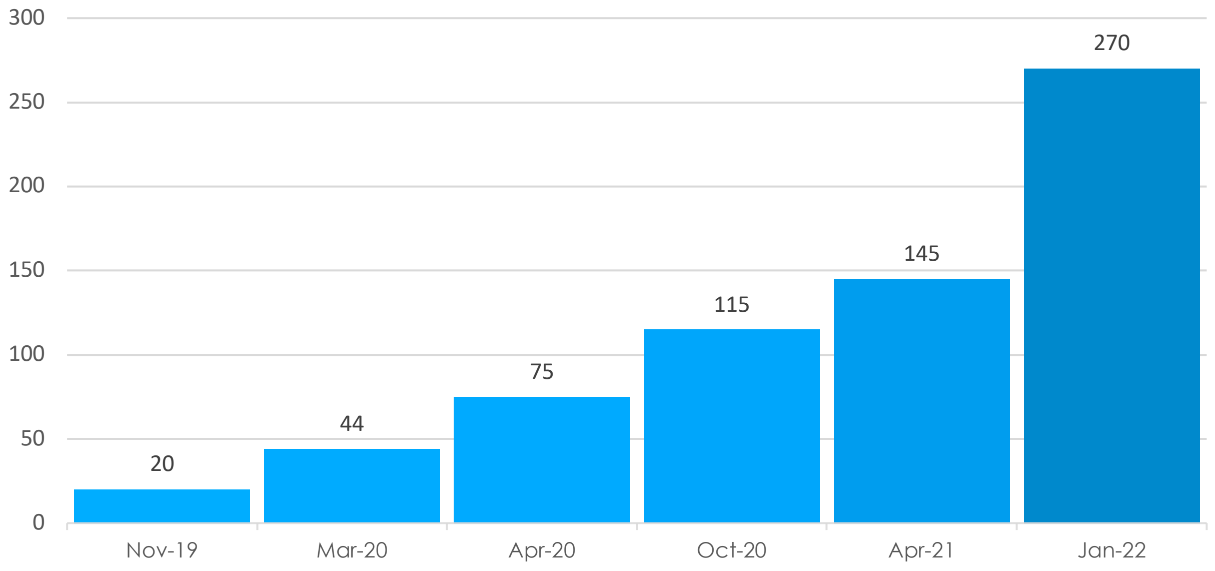
In recent years, a massive shift to towards distributed remote workforce models has propelled the adoption of feature-rich collaborative work platforms like Microsoft 365. With Microsoft's expansive suite of modern work tools, it's no surprise that there are now over 1.4 billion daily active users (DAU). Of these DAUs, over 270 million of them are using Microsoft Teams. It is also no surprise that this has driven increases in ransomware attacks targeted at online users, especially ones that use Microsoft's wide range of tools.

This report explores the challenges of developing a data protection strategy that accommodates the complexity of Microsoft Teams data. It also reviews commonly misunderstood native Microsoft data retention policies, and best practices in guarding Microsoft Teams data against potentially catastrophic data loss.

Microsoft Teams Adoption Sweeps the Remote Workforce

More than ever, organizations are adopting cloud-based solutions like Microsoft Teams to meet their productivity needs. In fact, the number of Microsoft Teams users increased by 50% in 2020 to 145 million active users. As of January 2022, there are over 270 million daily active users (DAU). This acceleration in usage is a result of the flexibility and agility that Microsoft Teams provides for hybrid and remote workforce models.

Microsoft Teams Usage Growth (Users by the Million)

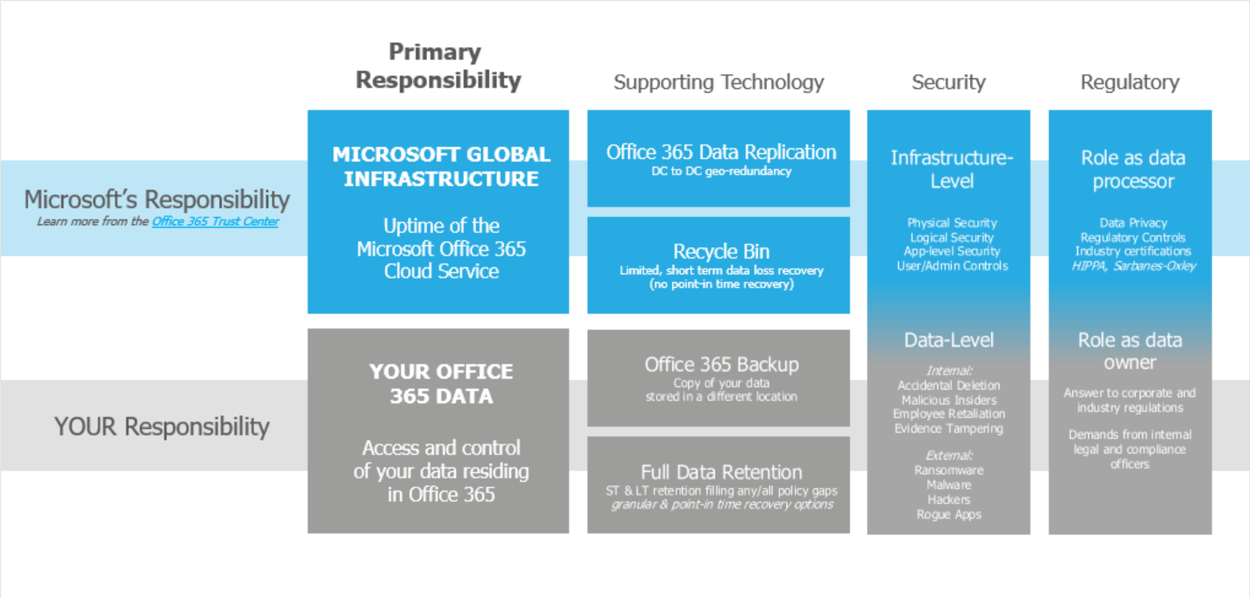


The Shared Responsibility Model – Your Data, Your Responsibility

Software as a Service (SaaS) data can be complicated to back up using traditional backup solutions. In many cases, organizations are unaware that SaaS providers like Microsoft do not backup the data stored within their services, and that it is the customer's responsibility to ensure they protect and backup the data that is created when using them. Microsoft protects data at an infrastructure level. They ensure the safety of their physical data centers, as well as the authentication and identification of their cloud services. They also protect user and admin controls that are part of the Microsoft 365 UI. You can learn more about Microsoft's responsibilities in the Microsoft 365 Trust Center.

The Shared Responsibility Model was designed to clarify each party's role in ensuring that user data remains safe. The diagram below shows this in detail.

The Microsoft 365 Shared Responsibility Model



	Primary Responsibility	Supporting Technology	Security	Regulatory
Microsoft's Responsibility *Learn more from the Office 365 Trust Center*	**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 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 location Full Data Retention ST & LT retention filling 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 data owner Answer to corporate and industry regulations Demands from internal legal and compliance officers

To avoid falling victim to retention policy gaps, ransomware, or internal threats, it's imperative that organizations proactively back up Microsoft 365 data, making it ready for recovery if, and when, it is needed.

Data Loss in Teams: A Closer Look at Cases and Impacts

Ransomware, malware and human error are all very real theats to data. IT departments have reported an increase in malware attacks using Microsoft Teams to distribute trogan files. Organizations without a strategic backup and recovery plan for Teams or other Microsoft 365 applications put themselves at risk of permanent data loss. The following case studies explore two permanent data loss incidents, and the negative impacts that had on the businesses involved.

Employee Accidently Erases over 145,000 Microsoft Teams Users

Human error is one of the top reasons for data loss. KPMG is one of the world's largest accounting firms. They use Microsoft Teams as their main internal communications tool for all employees across the globe. An employee was removing a single user account from an active retention policy, but instead of removing one user, the entire Teams deployment was removed from their account. This resulted in 145 000 users, including their conversational data, to be erroneously deleted. When KPMG engaged with Microsoft for recovery of these users and their data, it was discovered that it was impossible to recover it without a purpose-built backup solution. Although KPMG is actively working with Microsoft to improve their retention policies, it doesn't replace the need for a comprehensive backup solution built for Microsoft 365 data.

Hacker Deletes 1200 Microsoft User Accounts

A San Diego based Carlsbad Company experienced the loss of 1200 of their 1500 Microsoft user accounts after a disgruntled ex-consultant hacked in and maliciously deleted them. They were unable to access email, contact lists, calendars, documents, or video conferencing services. Additionally, this resulted in over two days of downtime and the company was forced to pay over $567,084 USD in remediation fees. Although Microsoft was the SaaS provider in this case, they were not responsible for the recovery of the deleted user accounts.

Lessons learned: Data Loss Can Be Prevented

Both organizations experienced downtime, revenue loss, increased IT expenses, reputation damage, and possible non-compliance due to data loss. This was completely preventable had they implemented a dedicated cloud data protection solution like Veeam Backup for Microsoft 365 from Gibraltar. This service provides a comprehensive cloud to cloud backup of Microsoft 365 including Teams data, to the Gibraltar cloud with quick recovery of data when required.

7 Reasons to Backup Microsoft Teams Data

I. Accidental Deletion

Microsoft has a Data Handling Standard policy for Microsoft 365 that specifies how long customer data is retained after deletion. Whether it happens accidentally, or on purpose – Microsoft doesn’t retain your data for more than 180 days. In some scenarios, that time limit is even shorter. Permanent data loss due to employee error, malware, or any other reason negatively impacts the business. Therefore, it is recommended to back up Microsoft 365 data.

II. Retention Policy Gaps and Confusion

The digital age lends itself to continuously evolving policies that are difficult to keep up with, let alone manage. Just like hard and soft delete, 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. In the case of a catastrophic issue, a backup solution can provide the ability to roll back to a previous point-in-time prior to this issue and saving the day, but unfortunately this is not in scope with Microsoft 365. With the Gibraltar Microsoft 365 backup solution, there are no retention policy gaps or restore inflexibility. Short term backups or long-term archives, granular or point-in-time restores, everything is at your fingertips making your data recovery fast, easy, and reliable.

III. Internal Security Threats

Businesses experience threats from the inside, and they are happening more often than you think. Organizations fall victim to threats posed by their very own employees, both intentionally and unintentionally. 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. In addition, some users unknowingly create serious threats by downloading infected files or accidentally leaking usernames and passwords to sites they thought they could trust. Another example is evidence tampering. Imagine an employee strategically deleting incriminating emails or files — keeping these objects out of the reach of the legal, compliance or HR departments.

IV. External Security Threats

Malware and viruses, like ransomware, have done serious damage to organizations across the globe. Not only is company reputation at risk, but the privacy and security of internal and customer data is also at risk. External threats can sneak in through emails and attachments, and it isn’t always enough to educate users on what to look out for —

especially when the infected messages seem so compelling. Exchange Online's limited backup/recovery functions can't handle serious attacks. Regular Gibraltar O365 backups will help ensure a separate copy of your data is uninfected and quickly recoverable

V. Legal and Compliance Requirements

Sometimes you need to unexpectedly retrieve emails, files, or other types of data amid legal action. Microsoft has built in a couple safety nets, (Litigation Hold) but again, these are not a robust backup solution capable of keeping your company out of legal trouble. For example, if you accidentally delete a user, their on-hold mailbox, personal SharePoint site and OneDrive account is also deleted. Legal requirements, compliance requirements and access regulations vary between industries, but all are subject to fines, penalties, and legal disputes no matter the industry.

VI. Managing Hybrid Email Deployments and Migration to Microsoft 365

Organizations that adopt Microsoft 365 typically need a window of time to serve as a transition between on-premises Exchange and Microsoft 365 Exchange Online. These hybrid email deployments are common yet pose additional management challenges. The Gibraltar Microsoft 365 backup solution can handle hybrid email deployments, and treat exchange data the same, making the source location irrelevant.

VII. Teams Data Structure

Microsoft structures Teams as a user interface that brings together Microsoft 365 services, such as SharePoint Online and OneDrive for Business. Teams has settings, configurations, and membership which all need to be protected and recoverable. A purpose-built backup solution can protect not only the data but also these settings and the associated interconnections between applications. Gibraltar will ensure the protection of Microsoft 365 data, using Veeam Backup for Microsoft 365 Backup.

GIBRALTAR®
DRIVING DIGITAL TRANSFORMATION

6 Microsoft Teams Data Protection Considerations

Choose a Holistic Approach
Centralize data protection to create a comprehensive strategic approach that reduces operational costs.

Simplify Backup Management
Work with a trusted Managed Service Provider to ensure RTO and RPO targets are met, and that backups are properly configured and ready for recovery when you need it most.

Make Security a Priority
Use a robust cybersecurity solution that will detect anomalies within the M365 platform as well as defend against outside cyber threats.

Offsite Backups in a Secure Location
Always keep a copy of data outside of Microsoft's platform. Gibraltar offers 100% cloud-based storage in Tier III Data Centers.

Deploy Purpose-Built Microsoft 365 Backup
Veeam utilizes Microsoft Teams APIs to provide a purpose-built backup, enabling full control and protection over this critical data.

Be Compliance-ready
Easily retrieve Microsoft 365 documents so you can meet regulatory or legal requests in a timely, cost-effective manner.

Conclusion: Data Loss is Preventable. Gibraltar can Help.

Protecting data within Microsoft 365 can be a challenge for even the most backup savvy technical team. Gibraltar's dedicated data protection solution for Microsoft 365 including Teams is backed by Veeam technology – the world leader in data availability.

About Gibraltar

Gibraltar Solutions is a leading Canadian technology provider with over 20 years of experience in the IT industry. Based out of Mississauga, we specialize in the design, integration and optimization of high-quality, enterprise-level IT infrastructure solutions in commercial, industrial and governmental sectors. We help customers to automate, streamline and manage their IT processes and digitally transform their business for improved productivity, performance and profitability. Our solutions range across a broad spectrum from point-solutions to fully managed project implementations, tailored to meet the evolving needs of today's digital economy.

Visit www.gibraltarsolutions.com
Book a demo and claim your 30-day free trial

veeAM
Cloud & Service Provider
Platinum