March 2021

MARKET REPORT

The state of Microsoft 365 backup

Global shift to remote work intensifies data protection challenges. »

Barracuda
Your journey, secured.

Contents

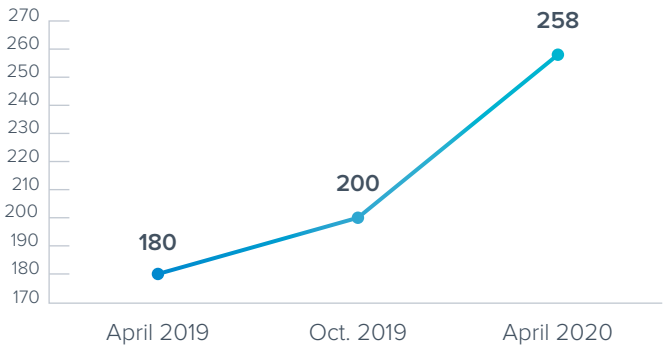
Introduction

Protecting the explosion of Microsoft 365 data

There's an explosion of Microsoft 365 data and a pressing need to protect it.

Microsoft 365 is seeing tremendous growth, particularly with the current world of remote workforces. According to Thexyz blog, in March 2020, the number of Teams meeting minutes increased 380% in just the first 19 days of the pandemic, climbing from 560 million to 2.7 billion per day.

O365 Monthly Active Users (millions)



The average gain in monthly Microsoft 365 users nearly quadrupled from October 2019 to April 2020, in large part due to the increased reliance on collaborative work during the pandemic.

IT leaders understand their organizations' reliance on Microsoft 365 and the need to protect it. However, there is often confusion about which protection features are and aren't included in Microsoft 365's native functionality.

In fact, Microsoft recommends customers use third-party backup, as the company only guarantees the availability of its service, not the retention of your data. As Microsoft does include some native retention, customers might not realize the limitations until there is a problem.

Customers may also find that Microsoft's built-in tools are basic, and restoration with native tools can be difficult and time consuming. Organizations looking to protect fast-growing data express concerns about the completeness of backup and retention solutions, as well as security, compliance, and, most importantly, how easy that solution is to deploy and use.

This report takes a look at the concerns and preferences IT professionals have about Microsoft 365, data security, backup and recovery, software-as-a-service (SaaS) solutions, and related topics.

Methodology

Barracuda commissioned independent market researcher Centropy to conduct a survey of IT decision makers responsible for their organization's cloud infrastructure. Participants included **1,828 IT decision makers** in companies with 50 or more employees in **the U.S., EMEA, and APAC**. The survey was conducted in January 2021.

Key findings

FINDING #1

Protecting data against attack and loss—both from outside actors and inside sources—is a key concern.

Data needs to be protected from outside attacks, such as ransomware, and from internal loss, such as accidental or malicious deletion. Data protection and security for both scenarios is strongly desired by respondents.

Ransomware attacks may not occur every day, but they remain top of mind, which is no surprise based on the ransomware trends in the news. While most news reports describe the fallout, and often the means of attack, they don't describe what is targeted, lest this information be used for future attacks.

Despite not knowing what specifically may be attacked, those surveyed are well aware that Microsoft 365 could be the target of ransomware; 72% of those polled were concerned about such an attack. Concern was highest in the U.S. (83%) and lowest in EMEA (67%), with APAC coming in at 73%.

This is perhaps not surprising, given that more than half of respondents have been a victim of ransomware. The geographic differences align here as well. Nearly two-thirds of U.S. respondents (64%) have fallen victim to ransomware, while 55% of APAC respondents and only 43% of respondents in EMEA have been affected by these attacks. The pain associated with being shut out of email and other collaborative applications is clear, especially with the extent of remote work.

Another factor that ramps up the concern around ransomware is the current ransomware trend of data exfiltration, where the data is stolen before it is locked and the information is sold back to the owner, or in cases where the owner of the data will not pay, it is sold to the highest bidder on the dark web. Data breaches such as these are potentially embarrassing and often expensive.

When it comes to data protection, security against accidental or malicious deletion is a far more common issue and equally concerning. Nearly 80% of those surveyed want multiple layers of role-based access control to limit who has access to potentially harmful actions, such as data deletion and purging.

I am concerned with ransomware locking/attacking my O365 data.
72% agree (n=1,793)

My organization has experienced a ransomware attack.
52% agree (n=1,741)

Multiple layers of role-based access control for backup copies is important to me.
79% agree (n=1,828)

Key findings

FINDING #2

Organizations want granular restore and other functionality not available in Microsoft's native capabilities.

Surprisingly, only a third of respondents have deployed a third-party backup solution; 67% are still relying on built-in Microsoft retention and restoration of deleted folders, despite the complexity of those retention policies and the inability to granularly restore items. This percentage was highest in the U.S., with 74% of respondents relying solely on Microsoft 365 for backup. In comparison, only 61% of respondents in EMEA and 70% in APAC take this approach.

In particular, 81% of respondents indicate that using Teams creates a data-retention concern. During the first full month of the pandemic, for example, Microsoft reported 380% growth in the use of Teams.

More than 80% of respondents want a backup solution that covers Teams and shared files. They also want that solution for Microsoft 365 to offer unlimited storage and the ability to download a copy of recovered items.

According to a report from the IT Policy Compliance Group, more than three-quarters of the time IT is asked to recover something, it's due to accidental deletion. Leveraging existing deleted folders and Microsoft's assisted restoration is time-consuming, difficult, and prone to failure; in many instances, restoring an entire directory to find a deleted item may inadvertently overwrite newer data and thus introduce new issues.

For these reasons, it's no surprise that backup of Microsoft 365 data, including granular recovery, is highly desirable.

Roughly as many indicated that recovering mailboxes to another location or user is important. This is something that can't be done easily with Microsoft's native capabilities. When someone leaves a company, they wind up a "deleted user" after 30 days, and that data can't be saved to another location or another user.

Ease of use also applies to signing in. When it comes to Azure Active Directory services and how they relate to new solutions organizations deploy, 76% of respondents say they want a solution that leverages single sign-on using AAD.

Finally, three-quarters of respondents would like to be able to pull daily reports on all backups, restores, and exports. While this might not seem groundbreaking, it is important to keep track of your backups. For one thing, it can help protect data by providing an early signal of suspicious data activity in your system.

I am relying solely on capabilities built in Microsoft 365 to backup and recover Microsoft 365 data.
67% agree (n=1,779)

Granular restore of Exchange, SharePoint, OneDrive, and Teams is important to me.
77% agree (n=1,828)

Key findings

FINDING #3

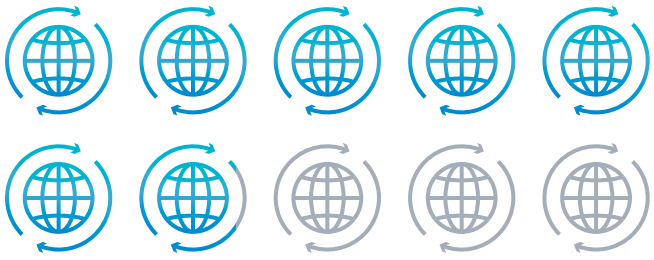
Data protection is both a security and a regulatory concern.

For many organizations, where data is stored has both security and regulatory implications. Data often includes sensitive information, so not only does it need to be secured, but that security needs to adhere to specific governmental compliance concerns and regulations. There are also data residency laws in different countries that regulate how data about their citizens or residents can be collected, used, and stored. Requirements can include timeframes for data storage and a requirement that some data must be purged upon request.

Regulations can vary by country, so organizations need to follow different requirements depending on where they operate — no easy task for multinational organizations. For example, within the European Union certain types of sensitive data must be stored in specific physical or geographic locations.

Nearly 7 in 10 respondents are concerned about this compliance, which is understandable when fines for violations can be as much as €20 million or a certain percentage of the previous year's annual revenue, whichever is greater.

I am concerned about data being backed up outside my geography (geo residency).
69% agree (n=1,787)



Interestingly, respondents in the U.S. show the most concern (80%) about data being backed up outside their geography. In comparison, 69% of APAC respondents and 65% of respondents from EMEA say it is a concern. This is likely due to varying degrees of complexity for these requirements in different geographies. For example, requirements are more comprehensive in France and Germany, but in the U.S. and India they only apply to certain industries or types of data. The results suggest that in countries where the rules vary, people are more concerned because they feel less confident that they are handling it correctly.

The same pattern holds true for concerns around data privacy. A full 85% of U.S. respondents agree that it is a concern, while 75% of APAC respondents and 64% of EMEA respondents agree. This suggests that in countries where GDPR has been in place for several years, IT leaders feel more confident about how they are complying with data privacy laws. In comparison, data privacy regulations still very from state to state in the U.S., so IT leaders are likely more concerned about keeping up with a patchwork of shifting requirements.

I am concerned around complying with data privacy requirements.
73% agree (n=1,802)

Key findings

FINDING #4

Organizations prefer a SaaS solution that is fast and easy to get up and running.

Organizations have made a conscious, significant infrastructure commitment in Microsoft 365 to both SaaS and the cloud. In some ways, it's a mindset change as businesses shift from an on-premises approach to cloud solutions like Exchange Online, and the growth of Microsoft 365 underscores that this decision is a valid and popular one.

When they look at solutions, not only are IT leaders very interested in SaaS-based backup, but they have the expectation of almost immediate gratification. Roughly 8 in 10 want to be able to start running their first backups immediately upon signing up. Other important SaaS considerations include having no hardware or software to maintain. Nearly three-quarters of those responding said that was an important consideration.

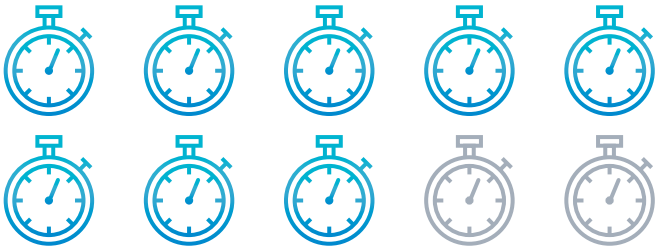
Respondents want to keep their data in the cloud, and 77% indicate they'd prefer to keep Microsoft 365 data in Azure. Performance is part of the reason, so it's not surprising that 76% of these respondents also feel that a close relationship between Microsoft and the backup vendor is critically important. U.S. respondents were the most outspoken on these two points, with 83% and 86% agreeing respectively.

IT pros also stressed the appeal of an all-in-one solution, versus a number of popular solutions that require separate licenses for backup and cloud storage. In addition to potentially being more costly, unbundled solutions also require more administrative maintenance, which is something organizations want to avoid.

SaaS backup for O365—i.e., no hardware or software to maintain—is important to me.
74% agree (n=1,772)

A simple, all-in-one licensing solution—versus requiring me to license storage and compute separately—is important to me.
79% agree (n=1,787)

Being able to sign up and start running my backup right away is important to me.
80% agree (n=1,805)



Conclusion

Global IT leaders want a cloud-native, SaaS backup solution for Microsoft 365 that is comprehensive, easy to use, and fast to get up and running.

Protecting Microsoft 365 data is a growing requirement, and organizations are looking for comprehensive, easy-to-use backup solutions. The growth of Microsoft 365 data isn't only due to the increased number of users, but due to the nature of remote work that relies heavily on SharePoint, OneDrive, and Teams.

Organizations are encouraging the use of collaborative applications, as they increase productivity in this environment and functions as a record of the work done. However, this value is greatly diminished without backup because Microsoft's native retention is not a backup. Customers often find that necessary functions for recovery, as well as everyday functionality, are lacking.

Many organizations discover that relying on those native retention services leaves much to be desired. Respondents showed a strong preference for granular retention, the ability to recover user mailboxes to another location or user, and levels of role-based access control. More than half of respondents want these capabilities, but they're still relying on Microsoft's native retention, which doesn't offer any of them.

Ease of use is a crucial requirement. Easy licensing and quick deployment make the decision to add third-party backup even more attractive and remove possible barriers to entry. At the same time, data privacy and compliance concerns provide additional incentives to add the right kind of data protection.

Finally, the right platform that aligns with their existing Microsoft infrastructure is another key requirement for IT pros. Many have moved from an on-premises Microsoft environment, as they saw the advantages of a cloud-native, SaaS platform. The advantages of keeping the data in the cloud for the entire lifecycle of the data, including better performance, lower total cost of ownership, and zero maintenance, illustrate an understanding of the value of the cloud.

Ease of use is a crucial requirement. Easy licensing and quick deployment make the decision to add third-party backup even more attractive and remove possible barriers to entry.

Appendix

FINDING #1

Protecting data against attack and loss—both from outside actors and inside sources—is a key concern.

I know an organization who has experienced a ransomware attack and struggled with recovery.

66% agree (n=1,758)

FINDING #2

Organizations want a comprehensive backup solution that is also easy to use.

A backup solution with unlimited storage is important to me.

84% agree (n=1,794)

Being able to recover mailboxes to another location or user is important to me.

79% agree (n=1,828)

Ability to download a copy of recovered items is important to me.

84% agree (n=1,792)

Single sign-on with directory services to manage my backup solution is important to me.

76% agree (n=1,797)

I would like to have daily reports on my backups, restores, and exports.

75% agree (n=1,828)

FINDING #4

Organizations prefer a SaaS solution that matches the infrastructure they're already using for Microsoft 365.

A backup solution that runs on Azure and stores Microsoft 365 data in Azure is important to me.

75% agree (n=1,828)

A close relationship between my backup vendor and Microsoft is important to me.

76% agree (n=1,793)

About Barracuda

At Barracuda, we strive to make the world a safer place.

We believe every business deserves access to cloud-enabled, enterprise grade security solutions that are easy to buy, deploy and use. We protect email, networks, data and applications with innovative solutions that grow and adapt with our customers' journey.

More than 200,000 organizations worldwide trust Barracuda to protect them—in ways they may not even know they are at risk—so they can focus on taking their business to the next level.

For more information, visit barracuda.com.

Barracuda
Your journey, secured.