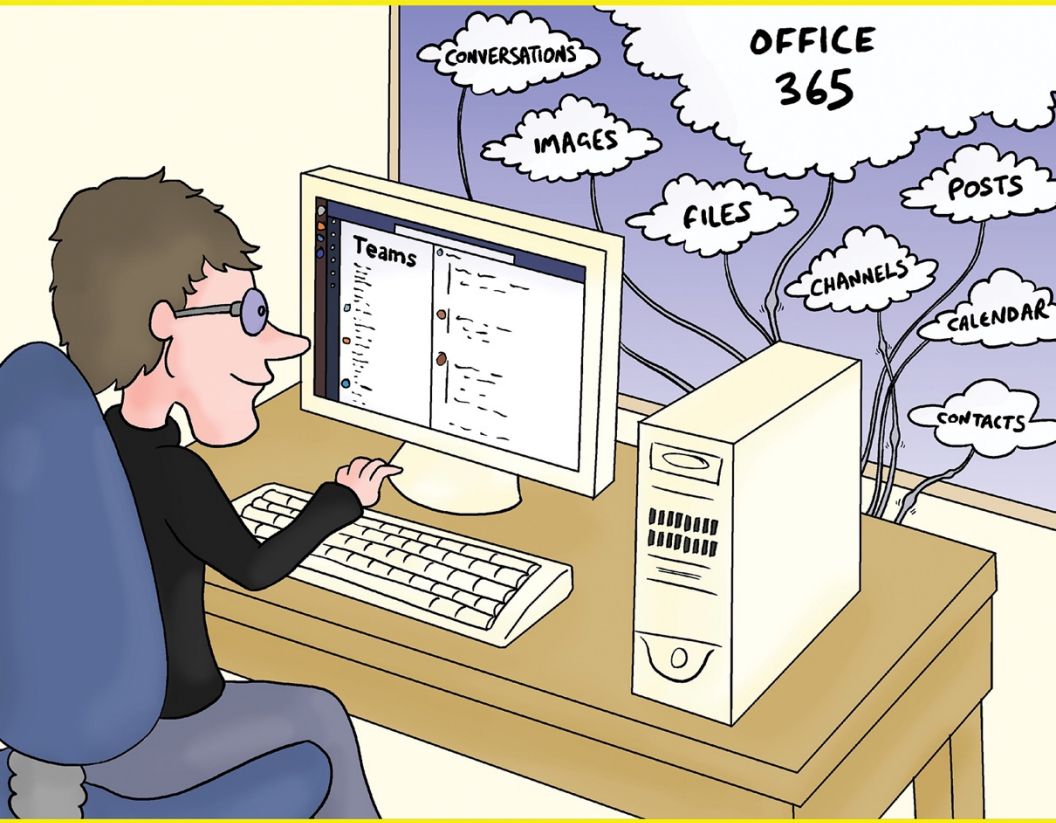
ConversationalGeek

Conversational Microsoft Teams Backup

By Brien Posey (Microsoft MVP, Commercial Scientist Astronaut Candidate)



In this book, you will learn:

- The different types of data you need to back up in Microsoft Teams
- 6 key reasons why it is important to back up Microsoft Teams
- Why the native backup capabilities of Office 365 are not enough

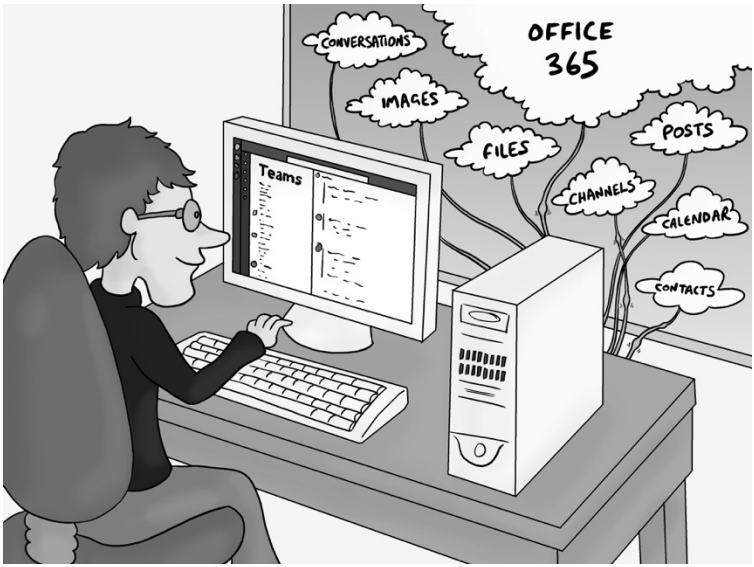
Sponsored by Veeam

Veeam® is the leader in Backup solutions that deliver Cloud Data Management™. Veeam provides a single platform for modernizing backup, accelerating hybrid cloud and securing your data. With 365,000+ customers worldwide, including 81% of the Fortune 500 and 66% of the Global 2,000, Veeam customer-satisfaction scores are the highest in the industry at 3.5x the average. Veeam's global ecosystem includes 70,000+ partners, including HPE, NetApp, Cisco and Lenovo as exclusive resellers. Veeam has offices in more than 30 countries.

To learn more, visit **www.veeam.com**
or follow Veeam on Twitter **@veeam**

Conversational Microsoft Teams Backup

Brien Posey



ConversationalGeek®

Conversational Microsoft Teams Backup

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Authors:	Brien Posey
Project Editor:	Pete Roythorne
Copy Editor:	Pete Roythorne
Content Reviewers:	Edward Watson
	Denisa Dan
	Russ Kercher

Note from the Author

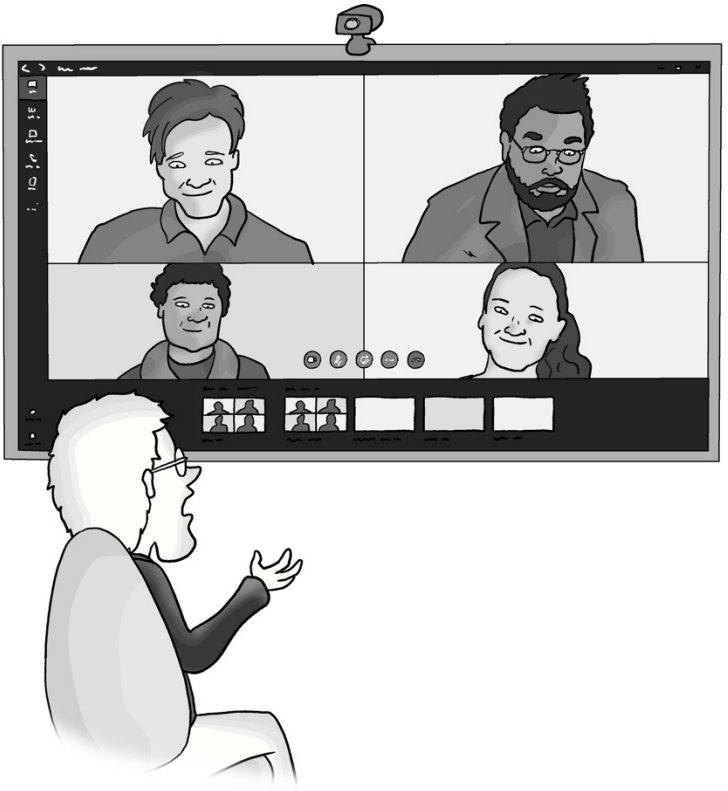
Hi, I'm Brien. For those of you who don't know me, I am a long-time Conversational Geek author, and 19-time Microsoft MVP. My professional background is in both IT and commercial astronautics. It's an odd combination for sure. I sometimes find myself setting up virtual machines one day, and being strapped into a space capsule the next day (seriously). Thankfully, my friends at Conversational Geek have embraced my unorthodox (dare I say eccentric) career choices and have allowed me to author books on subjects ranging from AWS to rocket science.

In this book, I wanted to write about some of the challenges associated with backing up Microsoft Teams. On the surface, this probably sounds like a really simple thing to do. Teams is a part of Microsoft Office 365, so if you want to back up Teams, all you have to do is to back up Office 365, right? But what do you actually back up? Exchange? SharePoint? Something else? Like so many other things in the world of IT the answer is anything but clear. As such, I wanted to take the opportunity to talk about some of the finer points of Microsoft Teams backups.

Oh, and one more thing… This book is not intended to be a vendor product pitch. My goal here is to take a vendor neutral approach to the subjects at hand.

Brien M. Posey

Backing Up Teams



“Did anyone backup that old team project before it was deleted?”

One of the business side effects of the global pandemic of 2020 has been the increased reliance on remote working. Face-to-face meetings have become practically nonexistent and businesses have begun relying extensively on video, voice and chatting communications applications such as Microsoft Teams. Microsoft Teams was already beginning to gain rapid popularity even before the pandemic. However, it has quickly become indispensable, and like any other business-critical

application Microsoft Teams needs to be protected by regularly backing up its data.

How Do You Back Up Teams?

One of the first things that needs to be considered is how to back up Microsoft Teams. As I'm sure you know, Teams is a part of Microsoft 365, or Office 365, or whatever Microsoft is calling it this week. So, if you want to back up Teams, you will need to back up Office 365.

One of the things that makes backing up Microsoft Teams so interesting though, is that Teams isn't what I would consider to be a self-contained application. To show you what I mean, consider the way that Microsoft Exchange Server works. Whether it's running on premises or in the Office 365 cloud, Exchange Server is designed to store user mailboxes within the Exchange Information Store databases. These databases are a part of the Exchange Server application.

Microsoft Teams works differently. Rather than Teams data being stored within the Teams application, it is widely scattered throughout the Office 365 cloud. Different types of Teams content are stored in different locations. Here is a breakdown of where Teams data is stored:

- Message Data – Message data is currently stored in a chat service table, but will eventually be stored in Cosmos DB. The chat data is also brought into Microsoft Exchange for compliance reasons.

- Images – Images are stored within the Media Services on Azure (in Blob storage). Like message data, images are imported into Exchange for compliance reasons.

- Files – Microsoft Teams stores files in different locations depending on the file type. Team files are

stored in SharePoint, while chat files are stored in OneDrive for Business.

- Voice Mail Messages – Voice mail messages are stored inside individual users' Exchange mailboxes.
- Recordings – Like images, recordings are stored in the Media Service on Azure in Blob storage. However, whereas images are imported into Exchange, recordings are instead encoded to Stream.
- Calendar Meetings – Calendar meetings are stored in user's Exchange mailboxes.
- Contacts – Contacts are stored in Exchange
- Telemetry Data – Telemetry data is stored in a Microsoft data warehouse.

If you want to learn more about where Teams data is stored, be sure to check out this Microsoft blog post: **https://docs.microsoft.com/en-us/microsoftteams/location-of-data-in-teams**

Six Reasons Why You Need to Back Up Teams

The bottom line is that if you want to back up Teams, then you have to back up Office 365. There is just no getting around that requirement. Early on though, most people didn't realize that they needed to back up their deployments.

I think there were probably a couple of reasons for this. The first reason has to do with the way that the cloud was being

marketed at the time. I'm not trying to say that Microsoft was engaged in false advertising, but rather that the cloud was still relatively new and that the way that cloud services were being marketed led at least some people to make some incorrect assumptions.

At the time, cloud service providers were working overtime to convince potential customers that cloud services were some sort of utopian solution to all of their problems. Many such providers gave people the impression that if they opted to run their software as a service rather than running it on premises, then they no longer had to worry about doing any sort of software-related maintenance.

Of course, there is some truth behind this idea. If you run a software application as a managed service in the cloud, then there are a lot of things that the provider handles for you. Consider Microsoft Teams for example. Microsoft handles things like software upgrades, patch management, hardware maintenance, and deals with outages so that you don't have to.

I think that because cloud providers like Microsoft handle so many maintenance tasks on behalf of their customers, it gave many people the idea that if they opted to run software as a cloud-based managed service then they didn't have to worry about a thing. They could simply use the software and allow the provider to worry about everything else. Ultimately, I think this probably gave a lot of organizations an incorrect perception that they didn't have to worry about backing up their cloud-based resources.

The other reason why I believe that Office 365 backups didn't catch on initially, was because there really wasn't a good way to back it up. After all, the backup software of the time was purely designed to back up resources residing on premises. The cloud was brand-new, and the backup vendors and providers had not yet caught up.

In any case, history has conclusively demonstrated that it is extraordinarily important to back up your resources residing within the Office 365 cloud – especially if you are using Teams. In fact, there are at least six different reasons why Office 365 backups are so important.

Reason 1: Accidental Deletion

The first reason why it is so important to back up Office 365 is that users can accidentally delete data that they need. For example, a Teams user might accidentally delete an important contact or a file that they need. We've all seen this sort of thing happen in on-premises environments, and it can happen just as easily in the cloud. Similarly, a user might overwrite good data with bad data. It happens. And when it does, you need a way of getting the user's data back.

Even though I am ashamed to admit it, I accidentally over-wrote good data with bad data just last week. I was working on a different book, and accidentally saved my notes in place of the chapter that I was working on. Since I had just written the chapter, it had not yet been backed up and I had to rewrite it. Needless to say, that wasn't much fun. As painful as the incident might've been, it underscores the importance of backing up data as a way of protecting it against mistake-related losses.

The good news is that Microsoft does give you a way of getting back data that was deleted accidentally. If a user accidentally deletes a file from within OneDrive, they may be able to use the OneDrive Recycle Bin to get their file back. Similarly, if a user accidentally deletes an email message that they need, they can recover it from the Deleted Items folder.

As helpful as these types of mechanisms may be, they aren't perfect. First, end users might not even realize that those mechanisms exist. Second, Office 365 only retains deleted items for so long. Once that period of time expires, the item is permanently deleted and there is no way of getting it back without restoring a backup. It's also worth noting that the recovery mechanisms that Microsoft provides might not be of any use if a file was accidentally overwritten rather than being deleted.

The bottom line is that Microsoft's native recovery tools will likely work at a pinch, but they really aren't well suited for day-to-day use. They simply lack the features and capabilities of a true backup solution.

Reason 2: Legal and Compliance Requirements

A second reason why you need an Office 365 backup is because it can be really tough to enforce retention policies without one. Many organizations are subject to regulatory requirements mandating that they retain data for a specific length of time. At least some of these regulations were originally designed to require organizations to retain email communications, but such regulations almost always extend to Teams as well. And as we all know, there can be severe financial penalties imposed if an organization fails to retain data for the required length of time.

While it's true that not every organization is subject to regulatory data retention requirements, some organizations have their own internal data retention requirements. An organization may wish to ensure for example, that data cannot be permanently deleted unless it is of a specific age. Such requirements can help to protect the organization against malicious users or legal challenges.

One of the best ways to make sure that data is retained in compliance with any regulatory or business requirements is to

back that data up and associate a data retention policy with the backup. That way, the organization can be sure the data within the backup will be preserved for the required amount of time.

Reason 3: Retention Policy Confusion and Gaps

A third reason why it is so important to back up your Office 365 deployment is because of the potential for gaps and other types of confusion within your retention policy.

I talked a bit about retention policies in the previous section and mentioned that some organizations adhere to data retention policies because of a regulatory compliance mandate, while other organizations base retention policies on their own operational requirements. Regardless of why a retention policy might have been put in place, strictly adhering to a retention policy can be surprisingly difficult.

The main reason for this is that there is no such thing as a centralized mechanism for managing retention policies across your entire organization. Think about it for a moment. A mechanism that establishes a retention policy for one of your line-of-business applications has no impact on the retention policies associated with things like Microsoft's Exchange Online or SharePoint.

The problem with this is that because retention policies cannot be centrally enforced, the potential exists for inconsistencies or gaps in coverage. It's really difficult to verify that retention policies have been enabled for every application and data source in your entire organization, and that those retention policies have all been set to the same duration.

On the surface, the challenge of maintaining retention policies would seem to have nothing to do with backing up Office 365 or Microsoft Teams. Remember though, Teams stores data across the various Office 365 applications.

A good backup application can actually help you to enforce your retention policies. When you create a comprehensive backup of your Office 365 environment, all of the Office 365 data is copied to a centralized backup location. In other words, your backup will likely contain data from Exchange, SharePoint, OneDrive, and the other Office 365 applications – all of the places where Teams data is stored. Because the backup is acting as a repository for so many different types of data, you can apply a retention policy to the backup, and that retention policy will in turn extend to the data that exists within the backup.

Reason 4: Internal Security Threats

Yet another reason why it is so important to back up your Office 365 environment is because backups act as a line of defense against internal security threats.

Internal security threats come in a variety of forms, but they are generally tied to a user who has malicious intent. We've probably all heard stories of employees that know that they are about to be fired and delete as much data as they possibly can on their way out the door. I have also heard some stories of employees who disagree with some of their company's business practices and have set out to sabotage IT systems as an act of revenge.

I was once fired from an IT job for putting in my two-week's notice. I was told that the fact that I was resigning made me a security risk. I had no ill feelings toward the organization, but apparently the upper management was paranoid about IT employees going rogue and had established a policy of immediately terminating anyone in the IT department that was planning to leave the company.

Unfortunately, it's probably impossible to completely put a stop to internal security threats. You just can't predict when an employee might go rogue. Sure, there are occasionally signs that an employee might have bad intent, but even if you notice that something seems amiss it's hard to predict what that employee might actually do.

One of the most important things that you can do to counter internal security threats is to establish a really solid backup and disaster recovery plan. Backups won't stop a rogue employee from doing something malicious, but they will give the organization a way of putting things back to normal if such an incident should occur.

Reason 5: External Security Threats

Just as security threats can originate internally with a rogue employee, security threats can also come from the outside world. These are the types of threats that people seem to be the most familiar with. I'm talking about things like hackers and ransomware, here.

The only way to truly keep ransomware at bay is to adopt a zero-trust security model. Unfortunately, zero trust security simply is not a good fit for every organization because it can be disruptive to business processes and can get in the way of things that employees are trying to do.

The best thing that an organization can do to counter external security threats (short of employing a zero-trust security model) is to practice defense in depth. If you're not familiar with defense in depth, it's based on the idea that you shouldn't count on any one single security mechanism to keep you safe. Instead, you should use a layered approach that uses a variety of security products and techniques. That way, if an attacker or malware ends up penetrating one of your defenses, other defensive measures will be in place to help prevent the attack from being successful.

Having a good backup strategy is an essential part of countering external security threats. Your backups are your last line of defense and are crucial for putting everything back to normal in the event that an attack is successful.

Imagine for example that your organization's data is encrypted by ransomware. When this happens, you generally have two choices: you can pay the ransom, or you can restore a backup. Paying the ransom is usually a bad idea. It emboldens the attacker, and there is no guarantee that you will get your data back. It is far better to have the ability to restore your data from backup than to be forced into paying a ransom.

I have heard stories of organizations becoming re-infected by ransomware only minutes after paying the ransom.

Reason 6: Managing Hybrid Deployments and Migrations

A sixth reason why it is so important to back up your Office 365 environment is that doing so is an important part of maintaining consistency. Imagine for a moment that you have a hybrid environment with half of your Teams users' mailboxes residing in an on-premises Exchange Server, and the other half existing in the Office 365 cloud. Does it really make sense to only back up the on-premises environment, protecting only half of the mailboxes? Remember, these mailboxes don't just store email. They also store Teams data.

Ideally, organization should use the same backup solution and technique to protect their on-premises and Office 365 assets. This not only helps to ensure that data is protected regardless

of its location, but it also gives you the option of moving resources to the Office 365 cloud if necessary.

Backups can play a role in a planned migration to the cloud, but they can also come in handy in times of disaster. If an organization's on-premises Exchange Servers were damaged or destroyed, for example, a backup could be used to move those mailboxes that had resided on premises to the Office 365 cloud.

The Shared Responsibility Model

Perhaps the best reason of all for backing up Office 365 is that Microsoft expects you to. Office 365 is based around something called the shared responsibility model. The essence of this model is that Microsoft and its Office 365 customers both play a role in maintaining the environment.

Microsoft's primary job is to protect the Office 365 infrastructure. They make sure the hardware is running properly, and that the Office 365 applications are healthy. They also handle ongoing maintenance tasks such as version upgrades and patch management. Conversely, Office 365 customers are expected to be responsible for backing up their own data, and that includes the data associated with Teams. If someone in your organization accidentally deletes a file, you can't simply call Microsoft and ask them to restore it. It's your job to back up your own data, and to restore that data should the need arise.

Teams Recovery

When it comes to having the ability to restore Microsoft Teams data, there are three main things that you need to be thinking about – The Recovery Point Objective (RPO), the Recovery Time Objective (RTO), and backup application support.

Recovery Point Objective (RPO) refers to the frequency with which backups are made, while Recovery Time Objective refers to how long it takes to perform a restoration.

Backup Application Support

Backup application support is important because it addresses how well the backup application supports recovery operations for Microsoft Teams. As previously discussed, Microsoft Teams data is scattered across a variety of locations including Exchange, SharePoint, and OneDrive for Business. Given the way that Office 365 stores Teams data, any Office 365 backup application should theoretically be able to protect the data that is associated with Microsoft Teams.

The good news is that Microsoft has very recently released an API for Teams! This API means that for the first time, it will be possible for backup vendors to back up and restore Teams natively.

To truly understand this API's significance, consider the difference between backing up and restoring Microsoft Exchange and Microsoft Planner. Both are Office 365 applications, but most backup vendors natively support backing up and restoring Exchange. In contrast, I don't know of any vendor who offers native support for backing up Planner.

Microsoft's new Teams backup API has finally made it possible for backup vendors to give their customers a first-class Teams backup and recovery experience. Keep in mind however, that this API is brand new, and most backup vendors have yet to integrate it into their Office 365 backup solutions.

eDiscovery

Nobody likes to think about the possibility of being subjected to litigation, but if someone does take legal action against your company then it will be critically important to have a reliable eDiscovery solution.

For those who might not be familiar with the term, eDiscovery refers to the practice of locating all documents and other data that have been the subject of a subpoena.

Microsoft Office 365 actually has its own built-in eDiscovery engine that allows an authorized user to search for any required data. With regard to Microsoft Teams, the eDiscovery engine is able to locate chat data, as well as messaging, files, meeting summaries and call summaries.

You can read more about eDiscovery for Microsoft Office 365 and Microsoft Teams at: **https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview**

As useful as Office 365's eDiscovery capabilities might be, they aren't perfect. Office 365 includes a mechanism called Legal Hold that allows documents that are surfaced during eDiscovery to be "put on hold" thereby preventing them from being deleted. The problem is that if you delete a user's account then their Exchange mailbox is also deleted, even if it has been placed on legal hold. Remember, Microsoft Teams stores a lot of its data in Exchange mailboxes, so if an Exchange Mailbox is deleted then any Teams data residing in that mailbox is also deleted.

Backup applications were never designed to act as eDiscovery tools. Even so, a good backup application not only has the

potential to act as an eDiscovery tool. Its capabilities might even surpass those of the tools that are built into Office 365.

To show you what I mean, consider all of the things that normally happen as a part of the eDiscovery process. When an organization receives a mandate to produce certain documents, the first thing that it does is to use an eDiscovery interface to search for the requested documents. Once the search is complete, the organization will typically place those documents under legal hold to prevent them from being altered or deleted. The last step in the process is usually to export copies of the documents so that they can be shared with whoever requested them.

Searching data

With that in mind, consider how a good backup application can perform these same tasks. Even though a backup application was never designed to act as an eDiscovery tool, a good backup application will likely include a search interface that allows an administrator to search for the data that has been backed up. As such, an administrator could conceivably use such an interface to perform eDiscovery within the context of a backup. Even if the native Office 365 search interface is limited in its scope, a search tool that is integrated into an Office 365 / Teams backup should be able to locate any data within the backup, even if that data is not something that would normally be surfaced by the native Office 365 search tool.

Of course, it isn't just administrators who sometimes need to locate data. A backup search interface can be useful to end users too. Think about it for a moment… How many times has someone sent you a file that you just can't seem to locate when you need it most? Did they email the file to you? Did they share it through SharePoint? Having access to a backup search interface can make it easy for users to track down otherwise illusive files.

Legal hold

As previously noted, the next thing that typically happens is that an administrator will place the discovered documents on legal hold. Backup applications do not typically have a legal hold feature, but you can establish a retention policy for your backups. If backup data needs to be put on legal hold, you could conceivably apply an indefinite retention policy to that data. Depending upon your backup architecture, another option might be to export the requested data to tape, so that you have a tangible copy of the data that isn't going to expire.

Another thing to keep in mind is that a legal hold does more than just keep data from being deleted. It also prevents data from being modified. Copying backup data to a tape for safekeeping fulfills this requirement.

Data Immutability

Many modern backup solutions also support data immutability within the backup. Data immutability has become increasingly important as a ransomware defense mechanism. Some ransomware is specifically designed to target an organization's backups. The idea is that if the ransomware is able to encrypt the backups then the organization will have no choice but to pay the ransom. Consequently, backup vendors are increasingly supporting data immutability as a way of preventing backup data from being modified by ransomware. The same immutability can also serve to protect data if a legal hold is issued.

Sharing data

The last step in the eDiscovery process is that of exporting and sharing data. A backup application is perfect for this purpose. You could simply select the documents that you want to restore, and then specify where you want to restore them to. The restoration process is essentially identical to the process

that eDiscovery engines use for exporting data. One thing that makes a backup tool different from the native eDiscovery engine, however, is that a good backup tool can help you to export data in whatever format makes the most sense. This might include .ZIP format, .PST format, or perhaps something else.

Why Native Capabilities Are Not Enough

There are countless backup applications on the market today and selecting one for your Office 365 and Teams backups can be a daunting process. While I'm not going to go so far as to endorse any one specific product, I do want to mention a few things that you should look for.

First, make sure that the backup software is purpose-built for Office 365. It is technically possible to back up some of your Office 365 data without the backup software being Office 365 aware, but Office 365 awareness will make the process a lot easier. Additionally, I would also recommend making sure that your product of choice is Teams aware. There aren't a lot of Teams-aware backup tools yet, but if you are really serious about protecting your Teams data, you really need to be using a Teams-aware backup product.

And speaking of easy, make sure that whatever solution you choose is intuitive and easy to use. There was a period of time in the early to mid 2000s when it seemed as though the backup vendors were all working to make their products as complicated as possible. However, excessive complexity doesn't help anyone. Having a simple and intuitive interface helps to minimize the chances that you will make a mistake that leads to data loss. Remember, your backup application should be able to help you put things back to the way that they were, as quickly as possible. Excess complexity can cause the recovery process to be slow and error prone.

Finally, make sure that the product that you choose is storage agnostic and designed to work in hybrid environments. Ideally,

the software should make almost no distinction between your servers running on premises, and the resources that you are protecting in the Office 365 cloud, nor should it care what type of storage the data is physically residing on. You should be able to use the same interface and techniques to back up both environments, and you should be able to restore data from one environment to the other environment if necessary.

The Big Takeaways

Microsoft Teams is a little bit different from most applications, because its data is located in a bunch of different places. While it's easy to assume that Teams data is stored in a SQL database somewhere, the data is actually scattered across a variety of Office 365 applications. Therefore, if you want to back up Teams, you have to back up the different components in which it is stored (i.e. Exchange, SharePoint, and OneDrive) and the backup intelligence and metadata to connect the dots

Backing up Office 365 is important. Microsoft does not back it up for you. It's up to you to protect your Teams data and the data associated with other Office 365 applications. Of course, to do that you are going to need a reliable Office 365 backup application, and most importantly, one that includes purpose-built support for Teams.

Microsoft

VEEAM

#1 Office 365 Backup
Built for Microsoft Teams

NEW Veeam® Backup *for Microsoft Office 365* v5 has added **purpose-built backup and recovery for Microsoft Teams.**

Veeam Backup *for Microsoft Office 365* v5 now includes:

- ✓ **Full control and protection** over Teams data
- ✓ **Faster and easier recovery** that is built for Teams
- ✓ **Unmatched eDiscovery** across Teams components

30-DAY FREE TRIAL — GET STARTED

Quickly become conversational about Microsoft Teams backup.

Over the past few years, businesses have become increasingly reliant on video and voice communications apps, such as Microsoft Teams. Like any other indispensable application, Teams needs to be protected by regularly backing up data. But with so many different types of data involved – from message and voice data, to images and contacts – all stored in different areas, how exactly do you go about effectively backing up Teams? Read this book to find out!

About Brien Posey

Brien Posey is a 19-time Microsoft MVP, a published author and conference speaker with 20+ years of IT experience, and a Commercial Scientist Astronaut candidate.