Brought to you by:

VEEAM

Microsoft 365® Backup

for dummies®
A Wiley Brand

Manage and safeguard your data

Understand data loss in the cloud

Choose a third-party backup solution

Veeam Compact Special Edition

Jennifer Reed
Edward Watson

About Veeam

Veeam® is the leader in backup, recovery and data management solutions that deliver Modern Data Protection. The company provides a single platform for Cloud, Virtual, Physical, SaaS and Kubernetes environments. Veeam customers are confident their apps and data are protected and always available with the most simple, flexible, reliable and powerful platform in the industry. Veeam protects over 400,000 customers worldwide, including 81% of the Fortune 500 and 69% of the Global 2,000. Veeam's global ecosystem includes 35,000+ technology partners, resellers and service providers, and alliance partners and has offices in more than 30 countries. To learn more, visit www.veeam.com or follow Veeam on LinkedIn @veeam-software and Twitter @veeam.

Microsoft 365® Backup

Veeam Compact Special Edition

by Jennifer Reed and Edward Watson

for dummies®
A Wiley Brand

Microsoft 365® Backup For Dummies®, Veeam Compact Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-88990-8 (pbk); ISBN 978-1-119-88991-5 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom *For Dummies* book for your business or organization, contact info@dummies.biz or visit www.wiley.com/go/custompub. For details on licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner
Associate Publisher: Katie Mohr
Editorial Manager: Rev Mengle
Business Development Representative: Karen Hattan
Production Editor: Siddique Shaik

IN THIS CHAPTER

- Comparing high availability and redundancy to backup
- Clarifying the shared responsibility model
- Defining data protection gaps

Chapter 1
Understanding the Need for Data Backup in Microsoft 365

Cloud technology is great. It has freed IT departments from implementing and managing complex and critical IT infrastructure by outsourcing those tasks to a cloud provider. What isn't great, however, is when there is a mismatch between what you think your cloud provider backs up and what the provider is contractually responsible for backing up. Microsoft 365 is a great example of this unclear shared responsibility.

This chapter explains why data backup in Microsoft 365 is crucial, helps you understand the high cost of data loss, and introduces the most common data protection gaps in Microsoft 365.

Comparing High Availability and Redundancy to Backup

Cloud service providers pride themselves on having the infrastructure to offer a highly available system that ensures their services will always be available no matter what happens. One of

the principles they apply to achieve high availability is to build redundancy into the design of the infrastructure.

Redundancy can be on a physical or data level. On a physical level, for example, a replica server is present, ready to take over if the main server fails. The replica can also act as a load balancer for an overloaded main server.

On the data level, redundancy is achieved by replicating copies of data in multiple systems or locations so that users are not affected when a server or data center goes down.

In contrast, a backup is simply a copy of data on a disk, a tape, or in cloud storage. With the right tools and processes, you can restore backup data into a new system in case of a failure to minimize business disruptions.


REMEMBER

Redundancy is the game plan in case something fails. In Microsoft 365, this capability is built in to minimize downtime and ensure rapid recovery in the event of a failure. The replica server and replicated copies, however, do not solve for data loss. If something is deleted or corrupt on the production side, then you'll also get deleted and corrupt data on the replica servers!

Having your own separate backup, in addition to Microsoft's redundancy and replication, is the ticket to a comprehensive and complete approach to data protection in Microsoft 365. That should be the focus for your IT teams.

Clarifying the Shared Responsibility Model

When you buy a new car, you expect certain security features from the manufacturer, such as brakes that work to help prevent you from running into another car. It is your responsibility as the driver, however, to step on the brakes when needed to avoid a collision.

Using Microsoft 365 is similar. You can expect certain things from Microsoft as the cloud service provider, and certain things are expected from you as the cloud customer. These expectations are rooted in the notion of a *shared responsibility* model.

In a software-as-a-service (SaaS) solution like Microsoft 365, Microsoft is responsible for maintaining the global infrastructure to keep its services running. You, on the other hand, are responsible for maintaining and protecting the data you store in Microsoft 365. For example, identity and access management is built into the service, but you must enable features such as Zero Standing Access policies to realize the value of those features.

Microsoft creates replicas of your data to achieve redundancy and to minimize (or ideally eliminate) downtime of its cloud services. That replica lives in Microsoft's infrastructure. They own it, you don't. They have access to it and use it as a failover when a server is down. But you don't have access to that replica to restore a report you're working on if your laptop encounters the blue screen of death and causes you to lose data. Replicas don't solve for data loss. Do you have deleted and corrupt data in the production server? If so, your replica server will have those as well.

Demystifying Backup and Retention in Microsoft 365

One of the reasons people need backup is to mitigate accidental file deletions. If that's all you're worried about, then the Microsoft 365 Recycle Bin should save you from a disaster, right? Unfortunately, no. Here's why.

In Outlook, permanently deleted items are moved to a Recoverable Items folder, which can be configured to retain data up to 30 days. If you need to recover an item older than 30 days, you're out of luck.

In SharePoint Online or OneDrive for Business, you have 93 days to restore a deleted item before it's gone. Don't be misguided by talks of Stage 1 and Stage 2 Recycle Bins in SharePoint. They simply mean that if an end-user deletes an item from a SharePoint site, that item goes to the site Recycle Bin where it's retained for 93 days, during which it's recoverable by the end-user. If you delete that item in the site Recycle Bin before the 93 days are up, that item is moved to the site collection Recycle Bin where it stays recoverable by a SharePoint admin for the remainder of the 93 days.

Realizing the Cost of Data Loss

WARNING

Data loss has severe impacts. It's expensive and unproductive, raises compliance risks, and harms your organization's reputation. The consequences can be so dire that according to a study conducted by the University of Texas, 94 percent of companies that suffer data loss do not survive — 43 percent never reopen, and 51 percent close within two years.

Defining Data Protection Gaps

In Microsoft 365, Microsoft is responsible for ensuring the infrastructure is always up and running. You, on the other hand, are responsible for protecting the data generated and stored in Microsoft 365. You'll face consequences if there is a mismatch on the understanding of who does what. To help you understand those consequences, this section explores the most common data protection gaps in Microsoft 365.

Addressing accidental deletions

A customer who writes speeches for politicians came to one of the authors of this book in frustration because he couldn't find a beautiful speech he'd written a month earlier and saved in OneDrive. He had assumed the Autosave feature in Microsoft 365 was his insurance and he'd be able to get lost files back with the Files Restore feature. He had spent at least an hour with his IT admin trying to recover the file before going the destructive Files Restore route. When that effort failed, they proceeded with the Files Restore to a date 30 days prior, knowing that he'd lose the files he'd created after the restore point. In the end, after spending three hours on the effort, they still couldn't find the file. Rather than invest more time, the customer concluded that further troubleshooting was not worth it, so he started from scratch and rewrote the speech.

REMEMBER

The moral of this story is that accidental deletions and user errors are a gap in Microsoft 365. Although the speechwriter can recreate his work, no matter how many hours of painstaking work it may have taken, the productivity loss is not desirable.

Accounting for internal and external threats

The headline news about security breaches in the past few years may have led some to believe that cybersecurity threats are mostly coming from hackers. Although it's true that bad actors have inflicted a lot of damage, not just on companies but also on people's personal lives, a data breach report from Verizon shows that 50 percent of security incidents were caused by people inside an organization.

Consider the cautionary tale of a hapless executive admin. She received an email from her traveling CEO to process payment of an overdue invoice so the CEO's credit card wouldn't be blocked during travel. She did as she was asked, as any well-meaning admin would. As it turned out, however, she was a victim of a spoofing attack that resulted in a breach that took six months to recover from. Key data were lost in the process, as well as a few customers who lost confidence in the company's commitment to data security.

REMEMBER

Spoofing and phishing attacks are successful only if a hacker has an unwitting accomplice: your end-user. The frailties of human nature usually pose the weakest link in any security strategy.

Discovering the gaps in retention policies

Threats don't just come from external bad actors. You could also be dealing with a disgruntled employee who purposefully deletes or tampers with data on his way out of the door. You might be thinking you've done your job retaining the ex-employee's data through archiving, but all you really have is a false sense of security because data would have already been lost by then.

Maybe you have a salesperson who left the company four months ago to join the competition. When she left, she took with her an Excel file that contains a list of key accounts she developed through your proprietary sales methodology and then deleted the original file. You might think you'd be able to find that list by going through her retained OneDrive folder. Think again. If the file was deleted and the deletion happened more than 93 days ago, you're out of luck.

That's because when you set a retention policy in a SharePoint Online site collection or a user's OneDrive account, and a user either edits or deletes a file, a copy of that file is created in the

Preservation Hold library. When the retention period for that copied file is up, it is then moved to a Recycle Bin (or two, depending on whether you made edits to the file while it was in retention) where you have 93 days to retrieve it. You cannot extend the 93 days so after that grace period, your file is destroyed and utterly unrecoverable.

But wait, there's more. Teams has its own retention policies, too, and they're managed separately. That's because Teams data is stored in multiple places: Exchange, SharePoint, OneDrive, and Azure.

These are clear examples of a gaping hole in Microsoft 365 backup. They also illustrate that retention policies and a backup solution are not one and the same.

Complying with legal and regulatory requirements

In Microsoft 365, you play a critical role in the shared responsibility model when it comes to data. In terms of regulatory compliance, Microsoft plays the role of the data processor while you play the role of the data owner in this model.

As the data processor, Microsoft's focus is on ensuring measures are in place to keep your data private, regulatory controls are implemented to meet requirements, and industry certifications are current.

You, as the data owner on the other hand, are responsible for ensuring that when a compliance requirement states data should be kept forever, then that data is immutable regardless of what the user tries to do with that data. The user can delete the content, or soft-delete, or hard-delete, or even throw the laptop into a river. The data still must exist to meet compliance requirements.

Managing hybrid Microsoft 365 environments

Digital transformation is a journey. It doesn't happen overnight, so organizations usually implement new technologies in stages to minimize risks and provide the best employee experience. Therefore, it's common to find a hybrid Microsoft 365 environment where an on-premises environment continues to run alongside the cloud. These hybrid scenarios increase the surface area of the data that need protection.

IN THIS CHAPTER

- Knowing what to look for in a backup solution
- Purchasing a backup and recovery solution
- Developing your backup strategy from a checklist

Chapter 2
Choosing an Microsoft 365 Backup Solution

Microsoft 365 has a robust set of capabilities to protect customer data, but there is no workload, service, or app designated specifically as a complete backup and recovery solution.

If you're serious about backup and recovery in Microsoft 365, you must implement a third-party solution. A research paper from IDC entitled "Why a Backup Strategy for Microsoft 365 is Essential for Security, Compliance, and Business Continuity" makes the same recommendation.

Finding the Provider to Match Your Needs

Entrusting your valuable company data to a third party is like having a trusted daycare for your child. You're responsible for taking your child to the daycare center and while he's there, the daycare center is responsible for his safety.

The difference between a daycare provider and a backup provider is that the backup provider is much more flexible and the options are plenty. At the bare minimum, backup solutions include options for automation so you don't need to do repetitive tasks that take up a lot of time and are prone to errors.

In this section, we cover key considerations for choosing an Microsoft 365 backup provider. The topics are not listed by order of importance because priorities differ from one company to another.

Considering the technical completeness of the solution

The Microsoft 365 backup solution that you choose should address, at the very least, the gaps identified in Chapter 1. The technical completeness of the backup solution determines how successful you will be in implementing a sound backup and recovery strategy. Will the solution back up everything in Microsoft 365, or just a few of the workloads? Is the provider stable enough in the market to assure you that two or three years from now, they'll still be around and continuing to push updates that match the pace of Microsoft 365 improvements?


TIP

About 23 admin centers exist in Microsoft 365. The question to ask your backup provider is: "Which of these workloads are covered in your solution?" If it's a challenge to find one backup provider that is 100 percent technically complete, then prioritize what's important to you and pick the solution that will back up the workloads in your risk threshold.

Factoring the ease of implementation

Your IT team will assume the brunt of the work managing the backup solution, keep it in tip-top shape, and be ready to spring into recovery mode whenever the need arises. With a good third-party backup solution, managing and executing backup and recovery can be simple enough for one person to do — even one with little to no experience.


TIP

If you have multiple people managing your backup solution, find a backup provider whose solution has a low learning curve. PowerShell scripts are great, but an intuitive user interface with tasks automated as much as possible may save you if, at the critical moment, you have to deploy a junior member of the IT team to perform the recovery.

REMEMBER

A big part of what constitutes ease of implementation is the support you'll get from the provider on a regular basis. Is support part of the package? What are the service-level agreements? Especially on D-Day, which you hope never comes, you'll need to understand the escalation path. It's better to have backup support figured out now, and not need it, than need backup support later and not have it.

Keeping the bottom line in mind

If IT budgets were unlimited, you wouldn't need to justify your vendor selection to those who will approve the expense. The good news is that competition for your business is healthy, so you have a good range of vendors to choose from. For less than the price of a cup of coffee per day, you can cover two or three Microsoft 365 users with a robust backup solution for a whole month.

On the flip side, the bad news is that having so many vendors to choose from can make your decision challenging. If you're considering price alone, the comparison won't be clear-cut. Although most vendors charge on a per-user per-month pricing model, others offer backup as part of a managed services package.

Furthermore, some vendors allow you to bring your own storage, which can reduce the fees, and others allow you to choose the workloads to back up, which then dictate the price.

TIP

Don't be tempted to rank your list of vendors based on the cost. Look for the right fit because ultimately, you're looking to calculate your total cost of ownership, not just the monthly fees. If a solution is cheap but requires a highly paid engineer to manage it, then it isn't cheap. Read the fine print. Maybe the per-user per-month license fee is low but there are additional costs for storage and data transfer.

REMEMBER

As you consider vendors for a backup solution, don't lose sight of the goal, which is to protect your data and your organization. The "cheaper" solution you pick today may not be cheap at all if you experience a data breach.

If you want to increase the odds of getting approval for a backup budget, you must first properly educate your business decision-makers as to why backup of Microsoft 365 is so important. Use this book to bolster your argument. Once your boss fully understands the notion of shared responsibility in Microsoft 365, you'll have a more receptive audience when you talk about picking a backup solution vendor.

Most reputable backup providers offer a free 30-day trial. You can also stand up a new Microsoft 365 tenant on a 30-day trial along with your backup trial. At zero cost, you can build a test environment, run some backups, and practice some restores. This is a great way to see how each product performs. This due diligence will pay off for you because only after you've determined the fit of a solution will you be able to calculate the total cost of ownership and compare that with the cost of the status quo.

Purchasing a Backup and Recovery Solution

You've done your homework and you've vetted potential backup solutions. You're now ready to go in front of your leaders to get the budget for a backup solution. In this section, we dive a little deeper into the considerations for picking a vendor so you'll rock your budget meeting. We also tie everything up with a checklist that you can customize or build from as you develop your backup and recovery strategy for Microsoft 365.

To BaaS or not to BaaS?

Backup-as-a-service (BaaS) can reduce the burden on the IT staff because infrastructure is outsourced to a BaaS provider. There are no servers to manage, patch, update, secure, or maintain, which works well for small and medium business (SMB) organizations that have little or no IT staff.

As Oleg Kuperman, Solution Architect for Softchoice Corporation (a recognized Microsoft Azure Expert MSP and BaaS provider), puts it:

SMB customers are not any less susceptible to data loss and malware attacks than large organizations. Unfortunately, most of them don't have the time, energy, or skillset to properly architect and manage a comprehensive disaster recovery, backup, and data lifecycle management infrastructure.

BaaS, however, may not be a good option for you if you already have an IT team that can handle the backup process and need shorter service-level agreements (SLAs). If you have compliance concerns related to online backup, then you'll need to do due diligence to determine if BaaS is for you.

Taking control of the backup tool

Web-based tools are great for work on the go. You aren't tethered to your desk to do search and recovery tasks, but these tools often come with some backup and recovery limitations. You can be on vacation in Cabo and still do backup and recovery tasks using your Internet-connected iPad. Or maybe not.


TIP

The tools I've seen that require server installation tend to have more robust capabilities than the web-based ones. Some tools like Veeam use the familiar Windows Explorer interface, so the learning curve is low.

The tool is where stuff happens. Heed the feedback from websites like G2 Crowd (`www.g2.com`), TrustRadius (`www.trustradius.com`), and Gartner Peer Insights (`www.gartner.com/en/products/peer-insights`) on the ease of using the tool because these comments come from IT admins who manage their organization's backup and recovery processes.

Putting What You've Learned Into Action

If you're reading this book, then most likely you understand the importance of protecting data in Microsoft 365 and have a desire to do something about it. I'd like to help turn that desire into action, so I've compiled the salient points in this chapter into a list of factors to consider when choosing a backup provider. This list is by no means exhaustive, so feel free to add to it and delete the points that are not relevant in your scenario.


TIP

If you're reading a PDF version of this book, you may be able to cut and paste the following content into a table in Word or directly into Excel. We suggest adding a column for each vendor you're considering and note what they have to offer against the items on the list.

Consider asking prospective vendors these questions:

- **Data sources.** Will the solution back up the following data sources?
  - Exchange Online: email, calendar, contacts, tasks, notes, public folders, shared mailboxes

- One Drive for Business: files, photos, folders
- SharePoint Online: files, folders, libraries, lists, sites, subsites
- Microsoft Teams: channels, tabs, posts, files
- On-Premises data: Exchange, SharePoint

» Data properties

- Will the backup retain the metadata for the items such as date created, date modified, and so on?
- If the items were shared — for example, as a Word document — will the permissions for the document be retained during the restore process?
- Will SharePoint sites, lists, and libraries retain their permissions upon restore?

» About the solution

- When can I back up? How often?
- Is the backup tool web-based, or a server that needs to be installed?
- Where and how is the tool deployed (if it isn't web-based)?
- What are the requirements for deploying the tool?
- What is the architecture of the solution? How is data protected?
- Where is my data stored? Do I have an option on where (or how — object storage for example) it's stored?
- What is your strategy to address Microsoft 365 throttling?
- What type of retention policy settings or options do I have?
- How fast is data restored?
- Can an end-user do self-service restore?

» About the company

- Will I have 24/7/365 support?
- What are your service-level agreements?
- If we cancel or don't renew our subscription, can we take our data?
- What is the cost? Does it include the storage of the backup data?

IN THIS CHAPTER

- Reinforcing the shared responsibility model
- Closing the gaps in Microsoft 365 backup
- Taking action on what you've learned

Chapter 3
Six Takeaways

The takeaways in this chapter are a quick summary of actions you can take to get started on a path to better data protection in Microsoft 365. They aren't listed in order of priority, so use these insights as you see fit in your awareness campaigns, budget discussions, and backup vendor conversations:

- **Microsoft is not responsible for backup — you are.** A common misconception people have about the value of using Microsoft 365 is that there is no need to back up data because Microsoft does all that work. Chapter 1 clarifies the shared responsibility model and outlines what Microsoft is responsible for versus what you are responsible for.

  You don't own, nor do you have access to, the replicas Microsoft creates for redundancy purposes. To make copies of your data and store those copies in a separate location, you need to implement a backup and recovery strategy using a third-party solution.

- **Data loss is costly — don't let it happen to you.** When people you talk to start balking at the cost of implementing a third-party backup solution, remind them that a Verizon report suggests that "small" data breaches can cost as much as half a million dollars while "large" data breaches can top at $200 million! Beyond dollars and cents, data loss harms your organization's reputation.

For such high stakes, it doesn't take much to avoid the pitfalls of data loss. There is no shortage of backup solution vendors today, so engage one of them and save yourself a lot of grief.

- **Microsoft 365 has backup gaps — close them.** You can't do much about the tendency of human beings to make mistakes, but you can help ensure that when mistakes happen, you'll recover quickly and minimize the harm done.

  In Chapter 1, we outline the backup gaps in Microsoft 365, one of which is accidental deletions. More disturbing than human error, however, is the malicious intent of bad actors, internally and externally, to wreak havoc in your environment. Stolen data is much more insidious than deleted data, so make sure you have controls in place to prevent that from happening.

- **Compliance is real — take it seriously.** Thompson Reuters, in a recent "Cost of Compliance" report, states that there are now more than 1,000 regulatory bodies worldwide that send out more than 200 regulatory updates every day. Predictions for the next ten years related to compliance point to continuing regulatory changes and an enhanced role for compliance in business. Undoubtedly, the IT team will play a role in this new normal. So, if you're still fighting the compliance mandate, give it up and fall in line. It is your responsibility as a data owner to govern your company data and ensure they meet compliance requirements.

- **Bad actors want to enlist your end-users — don't let them.** Phishing and spoofing campaigns are successful only if end-users fall for them, so help your end-users not play a part in breaching your environment. Remember, even IT professionals fall for these scams. No one is immune.

- **There is no shortage of backup solutions — pick one today!** Get started on your backup and recovery for Microsoft 365 initiative today. There is no shortage of backup vendors eager to help you out. You can even use 30-day trial licenses if you want to test and compare. Every minute you wait to back up your data is a minute you leave open for disaster to strike.


TIP

If you suffer from "analysis paralysis" from having to deal with too much information, too many vendors, and too many options, then you can narrow your options by using services such as G2 Crowd (`www.g2.com`), Trust Radius (`www.trustradius.com`), and Gartner Peer Insights (`www.gartner.com/en/products/peer-insights`) to find reviews of backup providers.

VEEAM

Gold
Microsoft Partner

Veeam Backup *for Microsoft 365*

#1 Microsoft 365 Backup and Recovery

Your data, your responsibility.

Veeam® Backup *for Microsoft 365* eliminates the risk of losing access and control over your Microsoft 365 data, including Exchange Online, SharePoint Online, OneDrive for Business and Microsoft Teams, so that your data is always protected and accessible.

- The Market Leader in Microsoft 365 Backup, with 14 million users protected
- Complete protection of Exchange, SharePoint, OneDrive and Teams data
- Deploy as-a-service or manage it yourself: Veeam gives you the choice!

Get started with
a 30-day FREE trial!

Drive productivity while protecting your data

The role IT professionals play in a landscape where data loss, security breaches, and invasion of privacy are the new normal has never been more critical. This book addresses the data security challenges in today's computing landscape by outlining the out-of-the-box security features in Microsoft 365 and uncovering the gaps that require action to achieve an effective backup and recovery strategy.

Inside...

- Understand shared data responsiblity
- Explore data loss prevention policies
- Enhance compliance
- Mitigage data loss in the cloud
- Identify data protection gaps
- Develop a backup and recovery strategy

VEEAM

Jennifer Reed is a technology business leader who helps businesses achieve their goals by developing innovative solutions using the latest cloud technologies. **Edward Watson** is a Product Marketing Manager at Veeam Software.

ISBN 978-1-119-88990-8
90000
9 781119 889908

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.