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 2nd Compact Special Edition

Jennifer Reed
Edward Watson

About Veeam

Veeam® is the #1 global market leader in data resiliance with 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 550,000 customers worldwide, including 77% of the Fortune 500 and 67% 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 X @veeam.

Microsoft 365® Backup

Veeam 2nd Compact Special Edition

by Jennifer Reed and Edward Watson

for dummies®
A Wiley Brand

Microsoft 365® Backup For Dummies®, Veeam 2nd Compact Special Edition

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

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-394-35350-7 (pbk); ISBN 978-1-394-35351-4 (ebk); ISBN 978-1-394-35352-1 (ebk)

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: Rebecca Senninger

Acquisition Editor: Traci Martin

Editorial Manager: Rev Mengle

Business Development Representative: Matt Cox

Production Editor: Tamilmani Varadharaj

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 an unfortunate 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. On the data level, redundancy means replicating copies of data in multiple systems or locations so that users aren't affected when a server or data center goes down.

In contrast, a backup is 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

In Microsoft 365, redundancy is built in to minimize downtime and ensure rapid recovery in the event of a server failure. The replica server and replicated copies, however, don't solve for data loss. If something is deleted or corrupt on the production side, then you'll also get deleted or 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.

Clarifying the Shared Responsibility Model

When you buy a new car, you expect certain security features from the manufacturer, such as brakes that work. It's 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.

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.

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.

What makes matters even more urgent is how long it can take to realize something's wrong. According to a recent Microsoft report, it takes organizations an average of 207 days to detect a data breach and another 70 days to contain it. That's a span of nearly nine months, which is far longer than the limited retention periods Microsoft 365 offers for deleted or altered data. If a breach goes unnoticed for that long, critical data may already be irretrievable through native tools by the time you realize it's gone. That's why having a true backup solution that operates independently of Microsoft's built-in retention timelines is essential to protecting your data long-term.

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 IBM and the Ponemon Institute, the average cost of a data breach is just under US$5 million in recovery costs and lost business.

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 the human error gap

Human error is one of the most common and costly causes of data loss. Whether it's an employee mistakenly deleting the wrong folder or overwriting a file with an earlier version, these small slip-ups can have major consequences. Microsoft 365 offers limited tools to help recover from these events, such as the Recycle Bin in OneDrive or SharePoint. But many user errors aren't discovered immediately. A file might be overwritten or deleted today, but not noticed until weeks or months later, well beyond the window of native recovery tools.

This is where the gap lies: Microsoft 365 wasn't designed to be a comprehensive backup solution. Its native features are useful for quick fixes, but not for true, reliable recovery when it matters most. A dedicated backup solution fills that gap by giving you granular restore capabilities long after the native recovery window has closed.

You can't stop human error, but you can stop it from becoming a disaster.

Accounting for internal 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, a data breach report from Verizon shows that 50 percent of security incidents were caused by threats inside an organization, including phishing attack victims, disgruntled current or former employees, and gaps in retention policies.

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.

You could be dealing with a disgruntled employee who purposefully deletes or tampers with data on their way out of the door.

Maybe you have a salesperson who left the company four months ago to join the competition, took an Excel file containing a list of key accounts 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 Recycle Bin, but if the file was deleted 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's then moved to a Recycle Bin where you have 93 days to retrieve it. You can't extend the 93 days, so after that grace period, your file is destroyed and utterly unrecoverable.

Expanding protection to include identity

When we talk about protecting Microsoft 365 data, it's easy to focus solely on the files, emails, and documents stored within the environment. But access to that data is just as critical as the data itself. Without strong identity and access management protections, even the most robust file backup strategy can be compromised.

In recent years, there has been a sharp increase in identity-based threats, including credential theft, token hijacking, and unauthorized privilege escalation. These attacks often serve as the gateway to broader data breaches. If an attacker gains access to an admin account, for example, they can manipulate permissions, delete data, or disrupt services, all without triggering traditional file-level alarms.

That's why a modern Microsoft 365 protection strategy must also include safeguards around Entra ID user identities and authentication systems. Identity and access data, including roles, group memberships, and permissions, should be considered just as vital to back up and recover as documents and emails.

Bridging the gap between operational and disaster recovery

It's helpful to distinguish between two distinct but complementary approaches to recovery: operational and disaster. Both play vital roles in a complete Microsoft 365 data protection strategy, yet they serve very different purposes.

Operational recovery is your first line of defense when everyday issues arise. It's the digital equivalent of an "undo" button. It addresses smaller-scale incidents such as accidental file deletions, incorrect file rewrites, and system crashes. These events are disruptive but not catastrophic. The goal of operational recovery is speed: Get users back to work with minimal downtime and as little data loss as possible.

Disaster recovery, by contrast, is your safety net for large-scale data loss events. It comes into play when entire systems are compromised or wiped out by events such as ransomware or other cyberattacks, or catastrophic human errors. In these scenarios, the recovery approach shifts from reactive fixes to full-scale system restoration. Disaster recovery requires secure, preferably offsite backups that are isolated from the production environment and ready to deploy. The aim is to restore continuity for the organization at large, not just recover a file or folder.

Although Microsoft 365 provides some native tools for data retention and limited recovery (such as the Recycle Bin or version history), these tools aren't designed to handle the full spectrum of operational and disaster recovery needs. Microsoft's first-party backup solution isn't included in a standard Microsoft 365 license, and lacks the comprehensive nature that a third-party backup can provide, which can deliver upon both operational and disaster recovery scenarios.

To bridge this gap, organizations need to go beyond what's natively available. Implementing a third-party backup solution ensures that both day-to-day hiccups and worst-case scenarios are covered, giving businesses peace of mind and a path to uninterrupted productivity.

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 a Microsoft 365 Backup Solution

Microsoft 365 has a robust set of capabilities to protect customer data, but its first-party solution isn't included in a standard Microsoft 365 license. Microsoft has integrated this powerful disaster recovery solution with specific backup solutions providing the best of both worlds to ensure optimal business continuity and ongoing compliance.

Finding the Provider to Match Your Needs

In this section, we cover key considerations for choosing a Microsoft 365 backup provider.

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'll be in implementing a sound backup and recovery strategy.

Will the solution back up your most critical apps 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?

Just as important, consider whether the solution extends beyond content to protect your organization's broader Microsoft 365 environment. For example, does it safeguard Entra ID and access management (IAM) configurations, such as user roles, group memberships, and permissions? With the rise in identity-based threats, the technical completeness of your backup strategy must also account for how users access data, not just the data itself.

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 if the need arises. With a good third-party backup solution, managing and executing backup and recovery policies can be simple enough for one person to do. Even better is a solution that offers a quick initial setup similar to SaaS backup solutions and configuration process, so your organization can begin protecting its Microsoft 365 environment almost immediately.

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. The more streamlined and simplified the user experience, the more likely your team is to manage the backup solution effectively and consistently. A well-designed, intuitive interface reduces the chance of human error and ensures essential tasks don't become unnecessarily complicated.

REMEMBER

A big part of what constitutes ease of implementation is the support you'll get from the provider. Is support part of the package? What are the service-level agreements? Especially on D-Day, 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 plenty 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.

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. Vendors charge by storage consumption or by per-user per-month models and today's leading solutions go even further by bundling backup, recovery, and unlimited storage into a single, all-inclusive price, removing the need to manage multiple vendors and helping reduce your total cost of ownership. This consolidation not only simplifies billing and support but can also reduce administrative overhead and the hidden costs that come with managing fragmented tools.

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. Don't be tempted to rank vendors based on 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 license fee is low but there are additional costs for storage and data transfer.

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

Purchasing a Backup and Recovery Solution

You've done your homework and you've vetted potential backup vendors. You're now ready to go in front of your leaders to get the budget you need. 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 up everything with a checklist that you can customize or build from as you develop your backup and recovery strategy for Microsoft 365.

To SaaS or not to SaaS?

SaaS backup can reduce the burden on IT because your infrastructure is outsourced to a SaaS provider. There are no servers to manage, patch, update, secure, or maintain, which works well for organizations of any size, regardless of the scale of their IT team. Besides the operational convenience, cloud-based storage also enhances your security posture. Data is stored offsite in highly secure, redundant environments, reducing the risks of local data compromise and providing stronger protection against cyber threats.

Modern SaaS backup platforms have evolved to offer even greater ease of management, not just for small businesses, but for larger, multi-scope organizations as well. With Microsoft 365 already delivered as a SaaS product, integrating a SaaS-based backup solution enables your IT team to manage protection across multiple services with minimal overhead. That means experienced IT pros can shift focus from routine backup tasks to more strategic initiatives that support your organization's long-term goals.

Another advantage of a comprehensive SaaS backup solution is the predictability it brings to your budgeting process. By consolidating backup, recovery, storage, and management into a single service, organizations benefit from consistent, transparent pricing and a reduction in vendor sprawl. This streamlined approach not only simplifies procurement and billing but also ensures unified support when issues arise.

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 limitations. You can be on vacation in Cabo San Lucas and still do backup and recovery tasks using your Internet-connected iPad. Or maybe not.

TIP

The best backup solutions in market typically offer the ability to leverage backup software or SaaS backup to meet your requirements.

The backup tool is where everything 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 importance of the backup tool being easy to use because these comments come from IT admins who manage their organization's backup and recovery processes.

Putting What You've Learned into Action

This book assumes you understand the importance of protecting data in Microsoft 365 and have a desire to do something about it. To help turn that desire into action, we've compiled the salient points to consider when choosing a backup provider. This list is by no means exhaustive, so feel free to add to it and delete whatever isn't relevant in your scenario.

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, memberships, settings, and team structures

  - On-Premises data: Exchange, SharePoint
  - Microsoft Entra ID: Users, role assignments, groups
- **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 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

- Why backup is a business imperative, not just IT hygiene
- The game-changing impact of SaaS backup
- Taking action on what you've learned

Chapter 3 Ten Takeaways

In earlier chapters, you learned about the shared responsibility model in Microsoft 365, the gaps in native protection, and how to choose a strong backup solution. Organizations of all sizes are rapidly moving away from traditional on-premises backup tools in favor of cloud-native, service-driven platforms.

Here are ten key takeaways to guide your backup strategy given how fast the space is evolving and where it's going:

- **Backup isn't optional, it's foundational.** Microsoft 365 offers great uptime and built-in redundancy, but redundancy isn't the same as recoverability. If you lose data due to accidental deletion, ransomware, or malicious activity, Microsoft isn't on the hook. You are. Backup isn't a nice-to-have anymore. It's a business-critical requirement.
- **Modern backup solutions are growing — *fast*.** Newer, agile vendors offering cloud-first backup services are growing rapidly because they simplify what used to be complex. They deliver not just backup but full peace of mind with less hardware, less hands-on time, and more automation.
- **Ease of use is the new power feature.** Simplicity isn't a tradeoff anymore; it's the key advantage. The best solutions are ones that junior IT staff can operate confidently. Web-based dashboards, guided restore tools, and low learning curves make modern platforms attractive to SMBs and large enterprises alike.

- **Identity is the new perimeter, so back it up.** As attackers increasingly target user credentials, protecting data means protecting access. Leading vendors now include support for backing up Entra ID — including roles, group memberships, and permissions — to ensure your access layer is just as recoverable as your files.
- **Automation reduces errors and saves time.** Manual backup tasks are prone to mistakes and busy IT teams don't always have the bandwidth to double-check every setting. Modern backup platforms eliminate complexity by automating routine jobs like backup scheduling, data classification, and even retention enforcement.
- **SaaS backup cuts through the noise.** SaaS-based backup eliminates infrastructure maintenance, patching, and scale issues. Losing those issues means less burden on IT, faster deployment, and built-in support. It also means you only pay for what you use, with predictable pricing and fewer surprise costs.
- **You can't afford to wait.** According to Microsoft, the average data breach goes undetected for more than 200 days. That's long past the point when Microsoft's native recovery tools stop working. You need backup that's not only independent of Microsoft but is also under your control. And you need it *today*.
- **Not all backup platforms cover all workloads.** Microsoft 365 includes more than just Exchange and OneDrive. A comprehensive backup platform should also cover SharePoint, Teams, and Entra ID (formerly Azure Active Directory), and other SaaS workloads. Be sure to ask potential vendors tough questions so that coverage gaps don't come back to bite you.
- **Don't be tempted by the cheapest option.** A low price may sound too attractive to pass up, but does it include storage, retention, support, and recovery? Cheap tools that require expensive daily babysitting or fail to restore data fast aren't saving you money — they're costing you more in the long run *and* exposing you to more risk.
- **To back up is human; to recover, divine.** Backup is your safety net, but when disaster strikes, recovery is what determines whether your business bounces back or stalls out. To that end, your vendor should offer granular restores, rapid recovery times, and self-service tools so you can start the recovery process right away. After all, this isn't just about data; it's about keeping your business moving no matter what.

veeam | Gold Microsoft Partner

Future-Ready Data Protection for Microsoft 365 & Entra ID

Your company's productivity and identity is your responsibility.

Veeam Data Cloud *for Microsoft 365* and Entra ID delivers the industry's most comprehensive, modern SaaS backup solution to combat today's cyberthreats and data loss mishaps. Protect Microsoft Exchange, SharePoint, OneDrive for Business, Teams and Entra ID all within a single solution.

Choose from flexible packages to fit your needs, all with unlimited storage included. Pricing is simple — per Microsoft 365 user, with any additional Entra ID users protected for FREE!

Most trusted, industry leading backup solution

All-in-one backup service with unlimited storage

Unified protection for **Microsoft 365 and Entra ID**

23.5M+ Microsoft 365 Users Protected

#1 IDC Market Leader

Request a live demo:

Take control of your data security with Veeam by not only safeguarding your critical information but also ensuring quick recovery. **Request a personalized demo today!**

Request now

Drive productivity while protecting your data

In the new cloud-based digital landscape where data loss, security breaches, and privacy risks are the new norm, the role IT professionals play has never been more critical. This book addresses the data security challenges in today's computing landscape by breaking down the native security features in Microsoft 365 and uncovering the gaps that require action to achieve an effective backup and recovery strategy.

Inside…

- Understand shared data responsibility
- Identify data protection gaps
- Explore data retention strategies
- Mitigate data loss in critical SaaS apps
- Simplify Microsoft 365 data management
- Find a backup and recovery solution

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: 978-1-394-35350-7
Not For Resale

9 781394 353507

for dummies®
A Wiley Brand