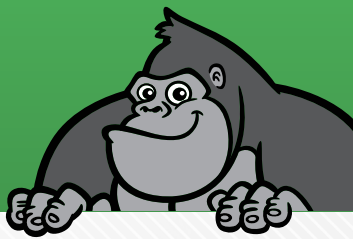
ActualTech Media

druva

THE GORILLA GUIDE TO...®

EXPRESS EDITION



Comprehensive Microsoft 365 Backup

Lawrence Miller

Inside the Guide

- Discover the Microsoft 365 Data Protection Gaps that Expose Your Organization to Risk
- Explore Different Microsoft 365 Backup Use Cases and Challenges
- Learn Why a Cloud-Native Solution Might Be Your Best Bet

THE GORILLA GUIDE TO...

Comprehensive Microsoft 365 Backup

Express Edition

By Lawrence Miller

ACTUALTECH MEDIA

6650 Rivers Ave Ste 105 #22489
North Charleston, SC 29406-4829
www.actualtechmedia.com

PUBLISHER'S ACKNOWLEDGEMENTS

EDITOR
Keith Ward, ActualTech Media

PROJECT MANAGER
Wendy Hernandez, ActualTech Media

EXECUTIVE EDITOR
James Green, ActualTech Media

LAYOUT AND DESIGN
Olivia Thomson, ActualTech Media

TABLE OF CONTENTS

Introduction: You're Not As Safe As You Think You Are 8

Chapter 1: Modern Business Challenges in the Cloud Era 10

- The Shared Responsibility Model 11
- Microsoft 365 Data Protection Gaps 14
- Microsoft 365 Data Is Everywhere 17

Chapter 2: Microsoft 365 Backup Requirements 19

- Data Backup and Retention 19
- Data Recovery 20
- Data Security and Privacy 22
- Ransomware Recovery 23
- Legal Hold and eDiscovery 25
- Compliance 26

Chapter 3: Microsoft 365 Backup Use Cases 28

- Managed Services: Easy, Self-Service Email and File Recovery 28
- Education: Unified Backup Across Multiple Environments 31

Human Resources Management: Data Privacy at Cloud Scale....33

Consumer Technology: Data Retention and Legal Hold....36

Financial Services: Regulatory Compliance....38

Chapter 4: Benefits of a Cloud-Native Microsoft 365 Backup Solution....41

Streamlined End-User and IT Admin Productivity....41

Lower TCO....42

Going Beyond Backup and Recovery....44

Get Protected—for Real....47

CALLOUTS USED IN THIS BOOK

The Gorilla is the professorial sort that enjoys helping people learn. In the School House callout, you'll gain insight into topics that may be outside the main subject but are still important.

This is a special place where you can learn a bit more about ancillary topics presented in the book.

When we have a great thought, we express them through a series of grunts in the Bright Idea section.

Takes you into the deep, dark depths of a particular topic.

Discusses items of strategic interest to business leaders.

ICONS USED IN THIS BOOK

DEFINITION

Defines a word, phrase, or concept.

KNOWLEDGE CHECK

Tests your knowledge of what you've read.

PAY ATTENTION

We want to make sure you see this!

GPS

We'll help you navigate your knowledge to the right place.

WATCH OUT!

Make sure you read this so you don't make a critical error!

TIP

A helpful piece of advice based on what you've read.

You're Not As Safe As You Think You Are

Welcome to The Gorilla Guide To...® Comprehensive Microsoft 365 Backup! This short book will be an eye-opener for most. That's because if you're using Microsoft 365, and you think your data is fully protected from disaster, you're most likely wrong.

Microsoft 365 is a foundational product for many organizations, but it's surprising how many of those companies don't understand its inherent limitations when it comes to backup and disaster recovery. Microsoft doesn't do all the work for you—you are responsible for making sure that your data doesn't go *poof* if there's an outage, accidental erasure, security breach, or other event that causes data loss.

This Gorilla Guide spells out in detail why you're not safe if you're relying on built-in protection. The reality is that you need to go far beyond that if you want to be able to recover from data loss in a way that doesn't harm or even destroy your business.

But this book doesn't just dissect the problem—it points to solutions. Those solutions include case studies showing how companies have upgraded their Microsoft 365 data protection for more peace of mind that, should the worst happen, they won't have to hang a virtual "Closed for Business" sign on their door.

There *are* solutions out there to help you, and we'll explore them in depth, as well. So, if you're ready to find out more, let's dive right in, starting with an overview of how business has changed and how it impacts you.

CHAPTER 1

Modern Business Challenges in the Cloud Era

The application landscape has changed dramatically as organizations increasingly adopt cloud and mobile computing strategies. Software-as-a-Service (SaaS) applications, in particular, have grown exponentially and are largely replacing traditional multi-tier enterprise applications and web applications deployed in on-premises data centers.

According to the Blissfully "SaaS Trends 2020" report,[1] overall SaaS spend per company is up 50% over 2018, averaging nearly $4.2 million annually ($2,047 per employee) for enterprises. Since 2016, Microsoft has been the SaaS market leader according to Synergy Research, with its Microsoft 365, Dynamics, and LinkedIn SaaS offerings now accounting for 17% of the $101 billion SaaS market.

[1] blissfully.com/saas-trends

Yet despite the overwhelming popularity of Microsoft 365, there's much confusion about its built-in data protection capabilities. Backup and restore functionality is often a misunderstood aspect of Microsoft 365. Let's get started by taking a look at some of the reasons why.

Microsoft recently rebranded Office 365 as Microsoft 365 for its consumer and business subscription bundles. However, the Enterprise, Government, Education, and Firstline Worker plans are still referred to as Office 365. Microsoft 365 for these plans refers to a full suite of solutions that includes Office 365, Windows 10, and Enterprise Mobility + Security. To keep things simple, this guide will use "Microsoft 365" to refer to all Microsoft 365 and Office plans.

The Shared Responsibility Model

Although enterprise cloud adoption has grown over the years, there's still a great deal of confusion about the shared responsibility model. Perhaps surprisingly, many business leaders today still mistakenly believe

that moving to the cloud somehow eliminates the need for many core IT functions.

Migrating your applications, workloads, and/or data to the cloud does not eliminate your responsibility for the security, privacy, governance, compliance, and protection (backup and recovery) of your data.

The shared responsibility model defines the cloud provider's responsibilities and the customer's responsibilities pertaining to the cloud services offered. For example, in an Infrastructure-as-a-Service (IaaS) offering, the customer is typically responsible for managing the operating systems, applications, and data on any virtual machine (VM) workloads deployed in the cloud, as if they were deployed in the customer's own data center. The cloud provider is responsible for managing the physical data center and the networking, storage, and compute infrastructure (see **Figure 1**).

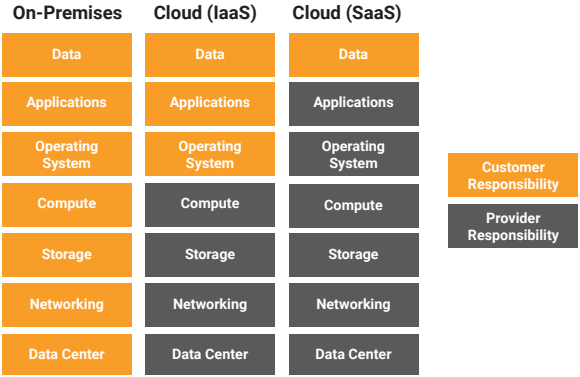


Figure 1: Examples of the shared responsibility model for on-premises, cloud (IaaS), and cloud (SaaS) environments

Microsoft maintains a shared responsibility model for Microsoft 365. As shown in **Figure 2**, Microsoft is responsible for managing the performance and uptime of Microsoft 365, and the customer is responsible for the protection and long-term retention of its Microsoft 365 data (including Exchange, SharePoint, and Microsoft OneDrive).

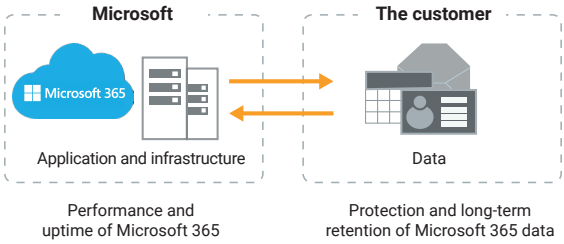


Figure 2: The shared responsibility in Microsoft 365

Microsoft 365 Data Protection Gaps

Microsoft's service-level agreements (SLAs) are primarily designed to protect Microsoft, not you. Its SLAs apply to data *Microsoft* loses, not that *you* lose. Recovery capabilities for basic and mid-level plans are limited, and expire within 30 to 93 days. Microsoft itself says it

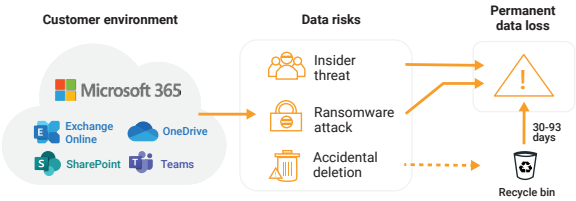


Figure 3: Microsoft 365 data protection gaps expose customers to data risks including insider threats, ransomware attacks, and accidental deletion

The Recycle Bin Isn't Data Protection

The Recycle Bin itself can be accidentally (or maliciously) cleared—it also lacks any data retention policy enforcement. Recovering lost or corrupt data can be an involved process, and restoring SharePoint sites requires Microsoft support.

best in its SLA: "*We recommend that you regularly back up your content and data that you store on the services or store using third-party apps and services.*"

Microsoft 365 contains some native data protection tools, but they require users to have knowledge of versioning, recycle bins, and the different default retention policies for each application. Relying on these tools places your organization's data and projects at risk from the following (see **Figure 3**):

- Accidental data loss caused by human error
- Malicious data loss caused by employees deleting data before departing the organization

- Malware infection, including ransomware, proliferated by excessive file sharing and periodic synchronization
- Data compromise, regulatory non-compliance penalties, and brand reputation damage due to gaps in data governance, legal hold, eDiscovery, and retention

SharePoint Online is the back-end storage for Microsoft Teams, so technically it isn't really a separate data footprint that needs to be backed up apart from your SharePoint content. However, to most of your users Teams is different from SharePoint—they don't necessarily understand (or need to understand) that Teams is just an overlay for SharePoint. You need to understand this relationship between SharePoint and Teams so that you know where to look when a user frantically calls you because "someone deleted all of my Teams content!"

Microsoft 365 Data Is Everywhere

Exchange emails and Office files stored in OneDrive are perhaps the most obvious and common examples of Microsoft 365 data, but they aren't the only ones. Microsoft 365 data also includes SharePoint data and OneDrive cache files stored in local folders on laptops and mobile devices for offline access. A comprehensive third-party Microsoft 365 backup solution needs to extend protection to all of these data sources, and, ideally, to other data sources in your on-premises environment.

Some organizations may instruct their users to save all their Microsoft 365 files to OneDrive, and warn them that their local devices aren't backed up. While this is often an effective strategy to discourage users from saving important files locally (for example, on their Windows desktops), it doesn't eliminate the organization's need to govern the data on user devices.

Learn more about how a comprehensive third-party Microsoft 365 backup solution can help organizations go beyond backup and recovery to address legal hold, eDiscovery, and compliance challenges in Chapters 2, 3, and 4.

Although restoring a locally saved file may be an increasingly less common use case, discovering data everywhere it exists—whether in the cloud, in an on-premises data center, or on an end user's laptop or mobile device—is crucial for legal discovery and regulatory compliance purposes. That can include responding to a data subject access request (DSAR), exercising an individual's "right to be forgotten" under the European Union's General Data Protection Regulation (GDPR).

CHAPTER 2

Microsoft 365 Backup Requirements

With an understanding of some of the business challenges in the modern cloud era, let's turn our attention to business requirements for protecting your Microsoft 365 data.

Data Backup and Retention

Ask any of your IT administrators about your company's backup strategy, and it's likely they'll confidently rattle off your backup schedules, technologies, capabilities, and features, and how quickly they can recover a file that was deleted six months ago.

Ask the same question about your Microsoft 365 backups and that confidence quickly fades. In much the same way that many business users have a limited understanding of the shared responsibility model, Microsoft 365 backups may be all "smoke and mirrors" to your IT administrators.

Simply stated, Microsoft 365 doesn't meet the standards that virtually all security professionals recommend for

data backup and retention (aka, the "3-2-1 Rule"): maintain three independent copies of your critical enterprise data on two different platforms/media, and in at least one remote location.

In fact, the native data protection capabilities in Microsoft 365 provide organizations with very little control over data backup and retention policies, which are largely determined by your Microsoft 365 subscription plan and may only approximate your business requirements.

Data Recovery

It's inevitable. End users (and even IT admins, on occasion) accidentally—or maliciously—delete files and emails, overwrite documents as they collaborate with team members, synchronize different file versions incorrectly, or otherwise corrupt files and data. Even an entire team site in SharePoint or Microsoft Teams may be inadvertently deleted. The bottom line is that without a comprehensive third-party Microsoft 365 backup solution, your valuable data is vulnerable.

In many cases, an end user may immediately realize their mistake and be able to recover an inadvertently deleted email or file from their Outlook Deleted Items folder or Recycle Bin. They may even be savvy enough

to recover items deleted from their Delete Items folder after they've emptied the folder.

But, in far too many cases, they may not realize that business-critical data was accidentally deleted until months later. For example, a well-intentioned intern may try to clear up some storage space in a shared OneDrive location by deleting a bunch of old files. Or IT may run an automated script that deletes inactive SharePoint and Teams sites that haven't been used for more than six months.

In both cases, it may be months before someone realizes that an important file has been deleted or an inactive project is suddenly active again. Unfortunately, in both situations the data would most likely be lost forever without a comprehensive third-party Microsoft 365 backup solution that provides:

- Regular point-in-time backups and unlimited retention
- Bulk and granular point-in-time restores
- Quick recovery and self-serve options to meet SLAs and operational-level agreements (OLAs)

Data Security and Privacy

It's an unfortunate reality: malicious insiders account for nearly one-third of all security incidents and approximately one-fifth of all data breaches according to the Verizon *2019 Data Breach Investigations Report*[2] *(DBIR)*.

A disgruntled or departing employee may delete, hide, alter, or steal sensitive data, often months before being discovered or "walking out the door." Unfortunately, simply archiving the user's mailbox or OneDrive account when an employee leaves is not an effective solution, since the data may already be lost or compromised by that time.

Without a comprehensive third-party backup solution, your ability to recover business-critical and/or sensitive Microsoft 365 data, review the history of the incident and scope of data loss, and conduct a thorough forensic investigation may be severely limited. A comprehensive third-party Microsoft 365 backup solution allows you to:

- Constantly capture data (including deleted files or versions) with continuous backups and unlimited retention

[2] https://enterprise.verizon.com/resources/reports/dbir/2020/introduction

- Isolate a copy of historic data outside of the Microsoft 365 environment
- Restore data sets back to the manager or even outside the Microsoft 365 environment
- Conduct data investigations and forensic analysis with built-in search and analytics capabilities

Ransomware Recovery

Ransomware attacks have increased exponentially over the past several years. Ransomware as a Service (RaaS) is one disturbing trend that makes it easy—but no less criminal—for practically anyone to target an organization with ransomware.

If your organization becomes a victim of ransomware, your single best defense is a reliable data backup. Even if you pay the ransom—which you should *never* do—there's no guarantee that your data will be restored.

Ransomware threats to Microsoft 365 are exacerbated by the fact that OneDrive is designed for collaboration and sharing, which makes it particularly susceptible to malware propagation.

OneDrive's file synchronization and sharing capabilities can facilitate the rapid spread of ransomware (and

other types of malware) to other files, including files in Recycle Bins.

Microsoft provides native protection against ransomware and other attacks at the Microsoft 365 perimeter, but as with any protection, it isn't foolproof. If ransomware hits your organization, recovering your organization's data is your responsibility.

With only the native data protection capabilities in Microsoft 365, by the time a ransomware attack is detected (or reported by an end user), many of your organization's files may already be corrupt and unrecoverable. At best, Microsoft 365 native data protection allows recovery from versions at an individual file level.

However, this approach is painful and impractical if multiple files—perhaps thousands—have already been corrupted. If the attack isn't detected until long after the default Microsoft 365 retention period, you have no recourse or means to restore your data. A comprehensive third-party Microsoft 365 backup solution can help you quickly recovery your data and return users to full productivity with capabilities that include:

- Anomaly detection and data forensics to conduct investigations, alert on unusual activity, and pinpoint the time and scope of a ransomware attack

- Indefinite data retention that enables full and quick recovery to pre-attack "point in time" data
- Recovery in minutes through single-click bulk recovery
- Self-service recovery and admin-initiated recovery
- Flexible recovery options, including "in place," "as a copy," or "outside" Microsoft 365 using bulk, flexible, and granular recovery options as needed
- Full data isolation in an external location to ensure recovery to clean data, regardless of the scope of the attack

Legal Hold and eDiscovery

When your organization is involved in litigation, it must comply with court-ordered eDiscovery and legal hold requirements. Without the right tools, compliance can be painstaking and fraught with risk. eDiscovery requires all relevant end-user data across the organization to be quickly accessible and protected from deletion or alteration, to avoid potential penalties and/or liability.

Microsoft 365 Business subscription plans do not offer legal hold capabilities, and although Microsoft 365 Enterprise subscription plans do offer some legal hold

capabilities, they're limited to Microsoft 365 data only. Data retention gaps—such as departing employees or intentional deletion—may also impede full compliance.

- Only a comprehensive third-party Microsoft 365 backup solution can fully support end-to-end legal hold and eDiscovery requirements across enterprise data workloads, with no disruption to employee productivity, including:
- Comprehensive legal hold support with no data retention limitations
- Automatic and complete data collection across enterprise workloads, not just Microsoft 365 data
- Fast export speeds, multiple file formats, and bulk custodian holds
- Easy integration with third-party eDiscovery tools

Compliance

Every organization has data governance policies that define data retention requirements. Within highly regulated industries—such as healthcare and biotechnology, critical infrastructure, and government and defense—organizations must comply with stringent state and federal regulations as well.

Unfortunately, Microsoft 365 Business subscription plans limit data retention to 30 to 93 days, depending on your licensing tier and use case. Microsoft's data retention policies differ for Exchange, SharePoint, and OneDrive, and Microsoft 365 only offers a maximum audit history of 90 days. Microsoft 365 data is also retained in the same primary environment, which does not provide sufficient data isolation for disaster recovery.

Data retention gaps such as these expose your organization to non-compliance risks with government regulations and organizational policies. Some Microsoft 365 Enterprise tier plans offer data governance capabilities, but they require complex data retention and policy tag configurations.

A comprehensive third-party Microsoft 365 backup solution helps organizations retain data and audit logs to ensure compliance with the following capabilities:

- Unlimited, flexible, and automated data retention policy options
- Flexible audit history and data retention that supports compliance requirements
- Data isolation through an immutable and independent copy, stored in a different environment from Microsoft 365, to comply with disaster recovery requirements

CHAPTER 3

Microsoft 365 Backup Use Cases

It's one thing to read about what a comprehensive Microsoft 365 backup solution can do for your business, but quite another to experience it. Unfortunately, it's not really possible to fully experience any technology solution in a book, so this chapter provides the next best thing—you can experience it through real-world customer success stories addressing different use cases in a variety of industries that are perhaps similar to your own company.

Managed Services: Easy, Self-Service Email and File Recovery

One case involves a managed services company that's a global leader in delivering legal, business, and research support services for law firms, corporations, financial institutions, and professional services companies. It provides customized programs for its clients leveraging emerging best practices, technology, and a data-driven approach to re-engineer core business processes.

Data protection is critical to the company's business operations, as well as its reputation, as it provides services to customers worldwide. To protect data on hundreds of laptops, it implemented the Veritas Desktop and Laptop Option. But Veritas' legacy approach didn't deliver full visibility or provide centralized management of endpoints, which made it very IT resource-intensive and time-consuming and exposed the company to vulnerabilities. In addition, the company experienced several data loss incidents with Veritas, in which too much time was required to find and restore data.

Without a dependable backup and recovery solution in place, the organization was at risk of losing corporate data due to accidental deletion, laptop thefts, fire, hard drive failures, viruses, and malware. They needed a new solution that would deliver high-performance backup, remote wipe, and geolocation capabilities for their laptops, as well as SaaS applications. They also needed to enable proactive data collection and preservation across endpoints and cloud applications to address legal holds and eDiscovery requirements.

The company started adopting cloud applications to support its increasingly mobile workforce and client operations on four continents. To protect its SaaS data and laptops, they wanted a backup and recovery solution that would deliver the same scale, cost, and

agility benefits of the cloud. The company found Druva and quickly recognized that it delivers the benefits and economies of scale in the cloud.

The company initially implemented Druva to simplify backup, archiving, compliance, and device management for its laptops. Druva has enabled the company to mitigate data loss and intellectual property theft, as backups run automatically in the background with no disruption to the end user. Not only can data on stolen devices be remotely wiped, but the centralized management of all backup data gives the organization the visibility and control it needs to maintain the business's reputation with its clients.

Druva's single pane of glass for protecting, preserving, and discovering information across endpoints made it the obvious choice when the organization migrated to Microsoft 365. The company relies on Microsoft 365 to house business-critical corporate data, but its native data protection capabilities weren't enough so it expanded its Druva deployment to unify Microsoft 365 backups into a single data pool that simplifies search, eDiscovery, and legal holds.

Druva also allows the business to support its own protection needs without involving IT. End users can select a backup, identify what data and devices need to

be protected, and what needs to be restored. The typical way people come to IT to restore the data is no longer required. It's all automated.

The benefits of the Druva comprehensive Microsoft 365 backup solution include:

- Improved global workforce productivity enabled through fast, self-service data recovery
- Extended cloud-native data protection, governance, and recovery for Microsoft 365 and hundreds of end-point devices deployed worldwide
- 25% reduction in labor costs through automation of tedious and repetitive tasks, and 25% overall operational savings due to elimination of costs associated with hardware upgrades, software licensing renewals, and maintenance costs

Education: Unified Backup Across Multiple Environments

In another case, an independent grammar and secondary school leverages information technology to deliver dynamic and interactive curriculum to its 1,000 students. It has large volumes of education-related data in its systems, as well as personal student data that must

adhere to strict government data security and privacy regulations.

Being a forward-thinking, innovative institution, the school saw the changing landscape of the way data was being protected and managed, and made the decision to begin its journey to the cloud, starting with Exchange, then migrating its data centers to the cloud.

The school was previously using Veeam for data protection of multiple on-premises workloads. As it began to migrate from Exchange to Microsoft 365, school learned that it would have had to purchase and deploy multiple products to manage data center workloads and Microsoft 365—Veeam doesn't provide a single pane of glass solution. The school would also have to find a cloud provider to store its backup data offsite.

To facilitate the school's cloud strategy, it needed a comprehensive backup solution built for the cloud—one that didn't require it to purchase and implement separate products and one in which storage was included as part of the solution.

After learning about the Druva Cloud Platform, the school immediately saw what differentiated Druva: the ability to achieve data protection and management for Microsoft 365 email and many other physical and virtual data center workloads through a cloud-native

approach. As a 100% SaaS platform built on Amazon Web Services (AWS), Druva enables cloud-to-cloud backup for Microsoft 365, as well as incremental backups for other data sources without ever needing to do a full, second backup.

The benefits of the Druva comprehensive Microsoft 365 backup solution include:

- Significantly faster backups for cloud-to-cloud Microsoft 365 data backup, and incremental backups for other on-premises data center physical and virtual workloads
- Lower total cost of ownership (TCO) through long-term data retention and built-in cloud storage, without the need to upgrade hardware infrastructure every three years
- Single pane of glass management enables IT to easily recover server data, down to the file level, and restore deleted emails fast

Human Resources Management: Data Privacy at Cloud Scale

The next case study involves a leader in cloud-based personnel management solutions that provides SaaS-based offerings to customers globally. With offices

everywhere, the company's IT operations team needed a comprehensive backup and archive solution to centrally protect the company's critical Microsoft 365 end-user data, as well as employee laptops, desktops, and mobile devices. The solution also needed to allow for easy recovery from time-indexed snapshots.

As a SaaS provider itself, the company was acutely aware of the inherent risks of utilizing Microsoft 365 as a business tool—one risk being that storing data in the cloud doesn't automatically guarantee its safety and security. Having the ability to actually own and control your data is very important.

The company previously used a legacy onsite product to handle its backup and archiving needs. However, the legacy solution was difficult to use and individual users' data often wouldn't get backed up—a fatal flaw for any solution. Another headache was the time it took to administer the legacy product; it required a lot of manual intervention.

Key challenges for the company included:

- Constant worries about critical data loss due to gaps in Microsoft 365
- Painfully complex physical tape management for archiving purposes

- Frustrating lack of central visibility and control
- Rising infrastructure costs and manual effort to meet business demands
- Lack of controls to address compliance requirements such as specific data residency regulations

Initially, the company implemented Druva inSync as a solution to back up the company's endpoints. They were extremely satisfied with its performance and ease of use, and quickly realized that Druva's comprehensive backup and archive solution could provide the same advantages when protecting their cloud application data as well.

A key consideration was the ability of inSync to scale along with the organization—incorporating global offices and new cloud business tools—and ensure that data residency requirements were being met.

The benefits of the Druva comprehensive Microsoft 365 backup solution include:

- All offices across the globe now have central data protection for cloud applications and end-user devices, aligning with regional policies

- Single pane of glass management simplifies compliance issues for Microsoft 365, Google, and end-user device data
- Engineering time previously spent supporting backup and archiving has been virtually eliminated
- Cloud-native scalability and security have decreased costs and provided peace of mind

Consumer Technology: Data Retention and Legal Hold

Another case is that of a leading supplier of consumer technology solutions that was rapidly expanding into innovative new technology sectors. Like many businesses, the company has embraced cloud computing and SaaS applications, including Microsoft 365, to support its geographically dispersed workforce of more than 200 employees worldwide, including many remote workers.

Key challenges for the company included:

- Endpoint backup and data management of all resources—many employees mistakenly believed that cloud SaaS applications like Microsoft 365 automatically and adequately backed up all their work

- Legal hold and data compliance management—the company needed to retain data for 10 years to comply with eDiscovery requirements
- Limited time and resources—the company's small, but highly responsive IT group needed a solution that would be easy to get up and running, and then easy to manage

As part of its migration to Microsoft 365, the company wanted IT to have a single point of access for viewing, managing, and recovering end-user data, whether on-premises or in the cloud. Its Druva inSync deployment brought disparate data sources together and empowered the organization to quickly identify data risks, place legal holds, and monitor and track its data to better adhere to company data governance and industry compliance regulations.

With inSync, remote teams in Europe and Asia have been able to back up to local clouds while IT maintains a unified view of what's going on across all instances.

In addition, the organization's IT administrators can determine how much control users have regarding their backups, such as whether the backup schedule can be changed, backups can be paused, backup folders can be altered, or settings can be changed. Administrators can also set a per-user quota, set limits on the number

of devices users can back up with inSync, and control when a device is considered inactive.

The benefits of the Druva comprehensive Microsoft 365 backup solution include:

- Fully automated legal hold workflow without involving end users
- Full data lifecycle management to meet strict 10-year retention policies
- Faster backup performance with less IT overhead
- Cloud-native offsite scalability and security

Financial Services: Regulatory Compliance

Finally, we look at an independent financial advisory firm that offers its services to both financial advisers and policyholders. For advisers, the company offers online access to client account information, which helps advisers reduce their in-house costs and obligations. For policyholders, it provides administrative services and market advice.

The firm's IT team is responsible for ensuring that the entire technology infrastructure runs smoothly, and without interruption. This means ensuring that more than 3,000 advisers and 400,000 clients can access

their policies via a web portal, and making sure that approximately 3.5TB of data is safe, backed up, and recoverable in the event of a disaster.

The firm's IT infrastructure consisted of physical Linux servers and network-attached storage (NAS) appliances, which were being manually backed up nightly to a remote physical server. It had transitioned to Microsoft 365 several years earlier, but email for strategic users was only being archived using Mimecast, which meant IT couldn't easily retrieve individual emails.

To effectively manage significant data growth, support the GDPR requirement for timely responses to DSARs, and meet stringent recovery time objectives (RTOs) and recovery point objectives (RPOs) for disaster recovery, the firm needed to migrate data protection to the cloud.

With Druva, the firm has complete confidence that its data is safe. Before Druva, it could take a couple of days to fully restore an inbox. Now, the firm can get individual emails and restore full inboxes either to the same inbox, a different inbox, or as a download in just minutes.

Druva sits in the background, backing everything up twice a day for the users' email inboxes—and none of the users notice any impact.

The benefits of the Druva comprehensive Microsoft 365 backup solution include:

- 95% faster time to restore emails and inboxes with self-service recovery capabilities
- Significant reductions in hardware infrastructure costs and streamlined business processes, which improve the bottom line
- Easily searching, collecting, preserving, archiving, or deleting data to support legal and GDPR compliance requirements

CHAPTER 4

Benefits of a Cloud-Native Microsoft 365 Backup Solution

There are many business and IT benefits of a comprehensive third-party, cloud-native Microsoft 365 backup solution. This chapter summarizes several of these key benefits.

Streamlined End-User and IT Admin Productivity

Recovering a corrupted file or deleted email is often a significant productivity drain for both end users and IT administrators. Finding and restoring the right data using traditional backup and recovery solutions can take hours or days under the best circumstances.

A comprehensive cloud-native Microsoft 365 backup solution can streamline these often-tedious processes and allow your users—and IT administrators—to get back to more productive work quickly. Key benefits include:

- Granular, user-friendly self-service data recovery in a streamlined UI empowers end users and increases IT productivity
- IT teams can meet data recovery RPOs, RTOs, SLAs, and OLAs in minutes
- SaaS solutions can be deployed in less than 15 minutes, and are always kept current with the latest Microsoft 365 features without requiring patches, updates, or maintenance
- Extends data protection across SaaS, IaaS, on-premises data centers, and remote/mobile endpoint devices—all managed in a single pane of glass
- Automatically scales to meet your data protection needs so you don't have to deploy and manage software clusters, or purchase additional storage capacity

Lower TCO

Traditional backup and recovery solutions often require companies to invest heavily in backup infrastructure such as backup media servers, high-capacity storage targets (for example, NAS appliances), tape cartridges and libraries, and backup networks, as well as backup software, agents, and other components.

Reduce Storage Usage and Right-Size Your Microsoft 365 Subscription

Microsoft 365 retention policies can cause a significant increase in storage use within SharePoint and OneDrive, which can exceed your subscription plan. If additional storage is priced at $0.20 per gigabyte per month, an additional 50GB of storage per user in a 1,000-user company will cost $10,000 per month.

A comprehensive third-party Microsoft 365 backup solution that uses rich metadata to enable global deduplication can reduce data volume significantly while addressing your data retention requirements. Combining a comprehensive third-party Microsoft 365 backup solution with a less-expensive and appropriately sized Microsoft 365 subscription plan can be the most cost-effective solution to address your data protection needs and more.

These solutions don't scale easily, and typically don't extend to SaaS applications (such as Microsoft 365) and cloud environments. A comprehensive cloud-native

Microsoft 365 backup solution can lower your TCO with benefits that include:

- No hardware or software needs to be purchased, installed, or maintained—ever
- Operational simplicity reduces administrative costs of data backup and recovery, enabling IT staff to be better utilized for strategic initiatives that deliver business value
- No data egress or restore fees. If a third-party Microsoft 365 backup solution provider you're using or considering charges these fees, find a better provider
- Cloud scale on demand with no investment in upfront capacity
- Cloud-to-cloud backups eliminate performance impacts of backup traffic on corporate wide-area networks (WANs)

Going Beyond Backup and Recovery

A comprehensive third-party Microsoft 365 backup solution can go well beyond an organization's backup and recovery needs to address requirements such as archiving, eDiscovery, legal hold, and compliance. When evaluating different vendors, look for a solution

that provides robust, built-in capabilities and benefits including:

- Single pane of glass management that provides complete visibility in a single view of all user data—not just Microsoft 365—for search, legal hold, and compliance
- Robust eDiscovery integration and fast download times that enable legal holds to be efficiently administered across the entire data ecosystem
- Managed keys that use enterprise-grade digital envelope encryption for data in transit (for example, 256-bit Transport Layer Security [TLS]) and at rest (for example, 256-bit Advanced Encryption Standard [AES]) for the highest levels of data security and privacy
- Federated search of metadata attributes to enable IT administrators to quickly locate Microsoft 365 content for legal and forensic investigations. It should also enable security teams to search through Microsoft 365 files across users, devices, and storage locations to track infected files, determine sequences of events, and analyze the scope and location of attacks

When evaluating third-party Microsoft 365 backup solutions, look for a provider that offers an enterprise-grade SaaS platform to deliver:

- Infinite, unmatched scale to grow with your business as you add users, data, systems, and locations
- Unified protection and rapid recovery for Microsoft 365 and key SaaS applications, public cloud IaaS (such as AWS), on-premises data center workloads, and user endpoints and devices
- Best-in-class certifications and compliance for relevant security and privacy standards such as International Organization for Standardization (ISO) 27001, GDPR, Payment Card Industry Data Security Standards (PCI DSS), U.S. Health Insurance Portability and Accountability Act (HIPAA), U.S. Federal Information Processing Standards (FIPS), and Service Organization Control (SOC) Levels 1, 2, and 3
- Choice of storage regions to meet data residency, compliance, and data isolation requirements

Get Protected—for Real

Throughout this Gorilla Guide, you've learned some important things about data protection for Microsoft 365. The most important takeaway is undoubtedly the understanding that the built-in offerings aren't sufficient to fully protect your precious data from potentially catastrophic loss.

If you've been using Microsoft 365 this way, it's crucial to re-examine your backup and disaster recovery strategy. You don't want to find out the hard way that much of what you thought was protected was not.

You've also seen that there is an answer. Druva delivers comprehensive cloud-native data backup and protection for Microsoft 365 including Microsoft OneDrive, Exchange Online, SharePoint, and Microsoft Teams, as well as endpoints, data centers, SaaS applications, and cloud-native workloads. Visit druva.com/microsoft365 to learn more.

ABOUT DRUVA

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California, and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva[1] and follow us @druvainc.[2]

[1] https://www.druva.com/

[2] https://twitter.com/druvainc

ABOUT ACTUALTECH MEDIA

ActualTech Media is a B2B tech marketing company that connects enterprise IT vendors with IT buyers through innovative lead generation programs and compelling custom content services.

ActualTech Media's team speaks to the enterprise IT audience because we've been the enterprise IT audience.

Our leadership team is stacked with former CIOs, IT managers, architects, subject matter experts and marketing professionals that help our clients spend less time explaining what their technology does and more time creating strategies that drive results.

For more information, visit
www.actualtechmedia.com