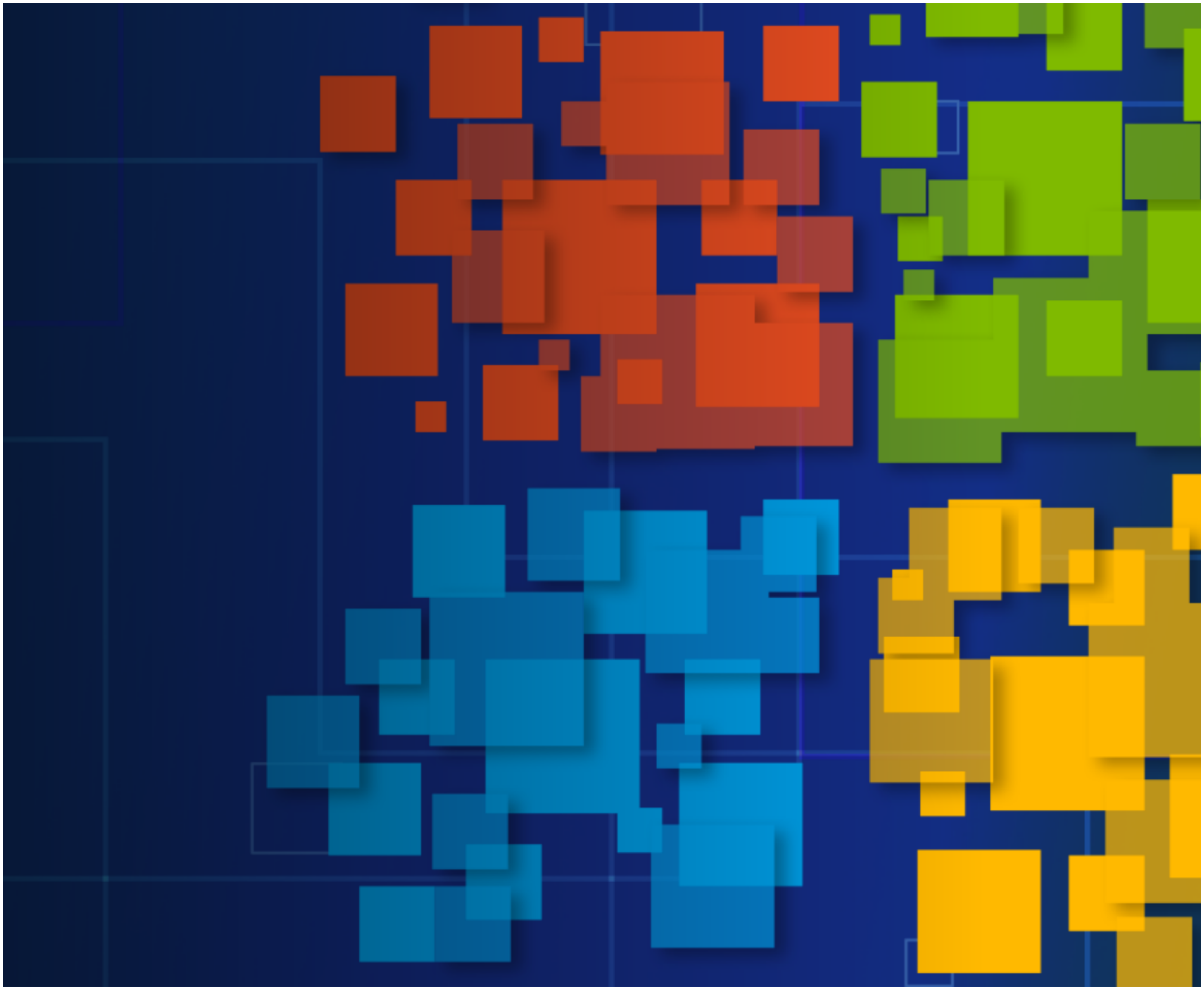
druva

White paper



Understand the top 3 threats to your Microsoft 365 productivity data

Fill the holes in your Microsoft 365 data protection strategy

How valuable is your organization's Microsoft 365 data?

Most businesses use Microsoft 365 for more than email. Microsoft 365 has become the centerpiece driving an organization's productivity as it provides email, calendaring, and file storage (up to 1 TB of online storage per user). Microsoft Teams is a hub for teamwork, providing group chat, online meetings, and even calling. This is in addition to its ever-popular business applications such as Word, Excel, PowerPoint, OneNote, and SharePoint.

Currently, there are over 58 million Microsoft 365 subscriptions, which is a testament to the trust businesses put in Microsoft's productivity cloud. Since the data created on the platform is what keeps business running smoothly, it is vital to understand all potential risks to this data. It is even more important to have a plan in place to recover from any data loss caused by ransomware, user error, or malicious insiders.

Doesn't Microsoft protect the data on its platform?

The Microsoft 365 platform is a SaaS service that operates on a shared responsibility model. Microsoft is responsible for the physical security, host infrastructure, network controls, and application-level controls. Microsoft states that the responsibility for data, endpoints, accounts, and access management is retained by the subscribers. What does this mean for ***your*** organizational data?

> SaaS applications like M365 house some of your customer's most critical data and yet, according to Gartner
>
> **70%** **of organizations will experience business disruption due to unrecoverable SaaS data loss.**

Most organizations don't realize Microsoft doesn't protect their data and that they need to back up and protect it themselves. Threats to organizations' data typically fall under three categories explored further in this white paper.

1. Manage the gap

Since Microsoft has a shared responsibility model, you must understand what they will and will not do when it comes to your organization's data. Then, you need a plan to help you manage any gaps.

Microsoft retention times

Managing your own cloud data means managing the contract expectations. So let's explore what Microsoft promises when it comes to M365 data retention policies.

This is how Microsoft defines customer data in their retention policies:

> *Content directly provided/created by admins and users. Includes all text, sound, video, image files, and software created and stored in Microsoft data centers when using the services in Microsoft 365.*

This is the retention time given for customer-created data:

> *Active Deletion Scenario: at most 30 days,*
> *Passive Deletion Scenario: at most 180 days.*

This means, at most, data that is deleted on purpose will be retained by Microsoft for at most 30 days. Data that is deleted due to policies will be retained at most 180 days.

The times depend on the application. But this is a great example of how not understanding how the shared responsibility model works may result in your data being deleted. Let's review how the retention time in different applications could impact your organization.

User leaves the company

When an employee leaves the company, you'll need to remove them from Microsoft 365 for business. Before doing so, you should block them from accessing company files, preserve the documents they created, and perform several other admin tasks associated with removing a user. Once you unassign an M365 license, you have 30 days to move that user's data. If you don't, Microsoft will permanently delete the data after 30 days. Due to regulatory and compliance requirements, it will be important to be able to access their data long after 30 days.

If you need to keep the user's mailbox longer than 30 days, an admin must either export it to a PST or put the account in litigation hold, which will require a license.

For a user's OneDrive account, an administrator can access the OneDrive files for 30 days, but if they are not assigned to a user within that time frame, they will be deleted forever. This becomes a problem if shared documents were stored in the OneDrive of the employee who leaves. All of the collaboration will stop if the files are deleted!

Deleted email

Email can be deleted accidentally. For example, maybe a user decides to clean up their mail, calendar, or messages by deleting messages or items. Per Microsoft retention rules, items first go to the deleted items folder. By default, email is kept for 14 days, although an admin can modify that to 30 days. By default, calendar items are kept for 120 days before they are purged from the platform.

> Researchers from Stanford University and a top cybersecurity organization found that approximately
>
> **88%** **of all data breaches are caused by an employee mistake.**
>
> Human error is still very much the driving force behind an overwhelming majority of cybersecurity problems.

If a user realizes they need an email after 30 days, Microsoft deletes it. You won't be able to recover it unless you're using a third-party backup service. This could be really frustrating if the email had attachments yet to be shared to OneDrive or SharePoint. Also, emails have to be restored one at a time to a different folder. So if the user deleted folders of emails, they will have to reorganize them once an administrator has restored them.

But what if the emails are deleted maliciously by a disgruntled employee? If they delete and purge all of their emails on their way out, and the clock runs down, the messages will be permanently deleted. Without foresight, an admin may not have the chance to preserve the user's email messages before the retention period concludes. Depending on the employee's role in the company, this could lead to a disruption in business.

Deleted files (OneDrive/SharePoint)

Organizations also rely on M365 to collaborate on business files using applications such as Word, PowerPoint, and Excel. These files are shared in OneDrive and SharePoint.

A OneDrive for Business account is associated with an individual user's account. As we discussed earlier, if a user's account is deleted, all of the files that they own in OneDrive will be deleted in 30 days if no plan has been made to move them.

Deleted files can be found in the recycle bin, but this can't be considered a backup option. In most cases, Microsoft's retention time for items in the recycle bin is 93 days. Once the retention period has expired, the files are deleted from the platform.

Sharepoint Online also holds organizational files. Additionally, a SharePoint site is created for each Microsoft Team that is created, offering more ways to work collaboratively on files. What is the retention time for these items?

In general, the retention time for SharePoint Online is also 93 days. Microsoft offers the following retention policies for SharePoint and the recycle bin:

- When Items are deleted, they are sent to the site recycle bin. They stay here for 93 days. The 93-day retention time for items in the recycle bin is not configurable.
- If the items are deleted or someone empties the site recycle bin, the items go to the site collection recycle bin. They will stay here for the remainder of the 93-day time period that started when the items were first deleted.
- Site collections can also be deleted. They are not recoverable after 93 days.

Microsoft does offer the ability to set retention periods. However, you must have at least an E3 or F5 license to take advantage of these. Importantly, retention will count against your storage costs. This may get expensive if you are storing data to stay in compliance with governmental regulations.

2. Insider threats

Disgruntled employees have been destroying data in acts of revenge for as long as we've had office work. This doesn't change just because you're using a collaboration cloud to create business data. You need to ensure your data is protected from internal malicious threats.

Microsoft cannot tell if data was deleted maliciously. And if you only discover the bad faith activity after the M365 retention period has expired, you're facing a data loss event. In this case, you must have a third-party data protection solution in place to mitigate the damage.

3. Ransomware

Ransomware attacks are increasing at a faster pace than most IT organizations can handle. In the majority of ransomware attacks, an attacker encrypts your most important business files. In many cases, the attack targets your backup data, making sure you don't have an easy way to recover these files. Finally, they hold this data hostage until you pay a ransom. Even after you pay, there's no guarantee the attacker will make the data available to you again.

> While Microsoft 365 has grown to nearly 300 million users, ransomware is growing as well, and Cybersecurity Ventures **expects payouts to reach**
>
> **$1.75T by 2025**

Microsoft has sophisticated defenses to protect its platform. However, the shared responsibility model means you're still responsible for your data if it is encrypted by a ransomware attack. In fact, Microsoft recommends third-party solutions as the best defense against ransomware, and states that "if you have offline backups, you can probably restore the encrypted data after you've removed the ransomware payload (malware) from your environment and after you've verified that there's no unauthorized access in your Microsoft 365 environments."

The first step after an infection is to disable Exchange and OneDrive sync so you can stop the spread of data encryption. This is because if your files are encrypted on your laptop, they can sync to OneDrive. Of course, email can also be used to spread the attack to other users.

Microsoft tells you the best protection you have from ransomware on their platform is offsite backups. Microsoft 365 does have some built-in retention and versioning capabilities that help you retain data after deletion or modification, but they are not backups. Since ransomware attacks and encrypts file data, let's look at the protections provided by OneDrive and SharePoint Online retain deleted items for 93 days by default, only OneDrive specifically offers the ability to recover back to a point in time up to 30 days. This may seem like a good way to "roll back" to a file version pre-infection, but ransomware can infect and hide for weeks or months before launching an attack. More importantly, versioning provided by OneDrive and SharePoint is not suitable to recover from ransomware because Recovery needs to happen from a specific point in time on the entire data set and not individual files to ensure all data is clean. Your responsibility is to find the platform that will best protect your vital collaboration data.

Druva Data Resiliency Cloud closes the gap

Microsoft 365 is SaaS provided by Microsoft. However, becoming a subscriber to this service does not absolve you of all security responsibilities. There is shared responsibility for security. In particular, the responsibility for accounts, identities, information/data, and devices is always borne by the subscriber.Since Microsoft expects you to be responsible for the critical data your organization creates on their platform, it only makes sense to use a third-party application to meet your own business continuity needs.

The Druva Data Resiliency Cloud is a secure, scalable, and cost-effective solution that provides comprehensive Microsoft 365 backup.

Critical SaaS platforms require cloud-native protection

To start with, if you rely on Microsoft 365 to be your productivity cloud, you should protect it with a cloud-native solution.

This means using a solution that is based in the cloud, and stores your backups in the cloud. You should not have to purchase additional cloud storage or hardware. A cloud-native solution will easily connect to your Microsoft 365 tenant and have an easy-to-use centralized console.

This describes Druva's Data Resiliency Cloud. Admins have complete global visibility of Exchange Online, OneDrive for Business, Sharepoint, Teams, and endpoint backup snapshots. Even better, end users are empowered to restore Exchange Online and OneDrive without IT intervention.

Microsoft 365 files are backed up directly from Microsoft Azure to the Druva Data Resiliency Cloud on high-performance AWS infrastructure, providing the offline backups that Microsoft recommends.

Our platform elastically scales compute and storage resources as your organization creates more data on the Microsoft 365 platform. Druva offers a flexible pricing model — users only pay for the storage used within the platform, allowing compelling cost savings as resources scale with **customers receiving TCO savings of 30% to 50%**.

eDiscovery and compliance

In addition to protecting your Microsoft 365 data from deletion or malicious encryption, it is prudent to ensure you can respond to requests from legal and compliance teams in a timely manner.

While Microsoft offers legal hold and eDiscovery solutions, there are gaps that can make it difficult to comply with these requests.

- Only Enterprise licenses can subscribe to legal hold capabilities
- Holds only apply to Microsoft 365 data
- There are no connectors to third-party eDiscovery applications
- Common data tasks can be very slow
- Prohibitive costs outside of normal IT budgets

Druva goes above and beyond backups to help with legal hold and eDiscovery. This is because Druva backs up all Microsoft 365 data into a single pool. In fact, other SaaS solutions and endpoints can also be part of this federated search, providing a comprehensive, simplified view for legal teams.

This data retention collects data from departing employees, even if there are intentional deletions. Druva also integrates with third-party eDiscovery tools for added functionality.

Ensure your data is secure, scalable, and always available

A collaboration cloud such as Microsoft 365 helps businesses move faster. But it's important to remember that you **are responsible for the data your organization creates in Microsoft 365.**

Protecting your Microsoft 365 data is critical to the success of your business and Druva provides a complete solution to address your data protection needs. Threats to your data are real and require time-intensive recovery in the event of data loss or ransomware. Druva helps you bounce back from ransomware attacks with our automated recovery of clean, complete data sets. The Druva Data Resiliency Cloud is a cloud-to-cloud solution to fulfill the responsibility of protecting your Microsoft 365 data.

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300

Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com