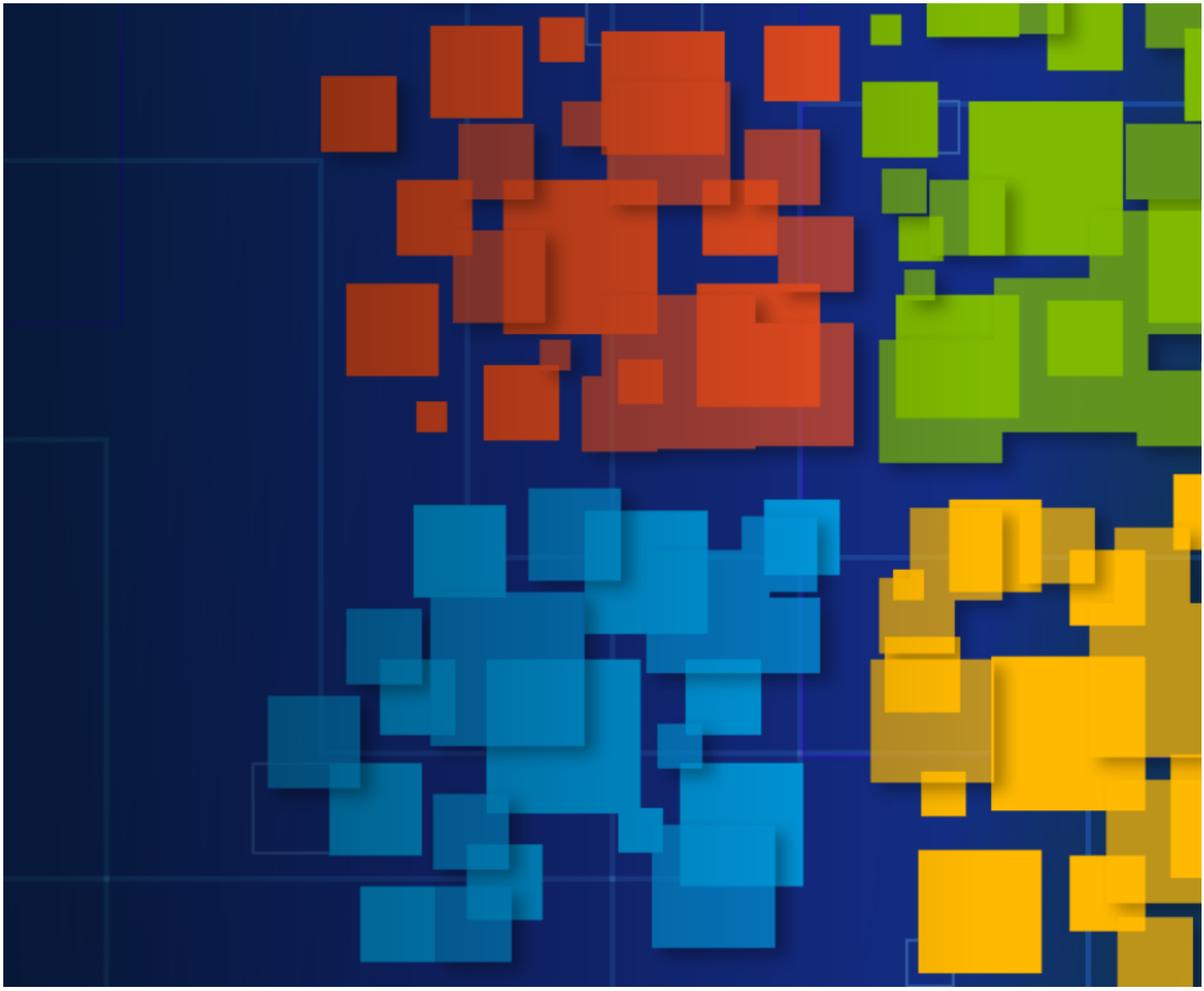
druva

White paper



Best Practices Guide: Microsoft 365 Data Protection

Protect your workforce productivity and IP — address critical data protection gaps in Microsoft 365

Q222-20283

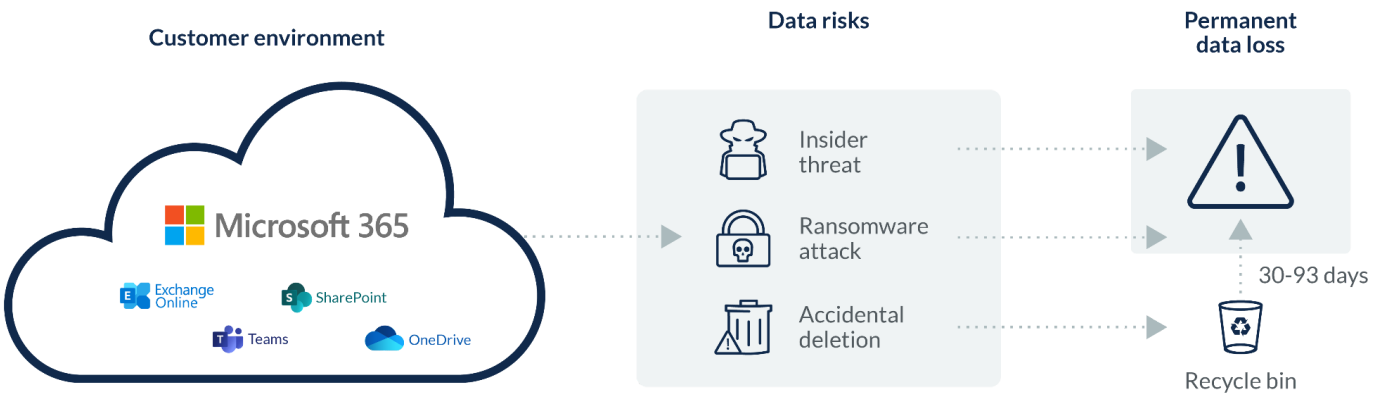
Why protect Microsoft 365 data?

Many organizations are adopting Microsoft's highly successful Microsoft 365 (previously known as Office 365) productivity and collaboration suite of tools in the cloud. But many companies don't realize the inherent data risks that must be addressed to safeguard intellectual property while maintaining end-user productivity. The responsibility for data protection within Microsoft 365 falls squarely on the customer's shoulders, as stated by Microsoft in their services agreement, "We recommend that you regularly backup your content and data that you store on the services or store using third-party apps and services".[1]

Because of Microsoft's shared responsibility model, the most prudent course of action for organizations is to protect their Microsoft 365 data using a dedicated third-party solution.

> *"Office 365 does not create an independent, accessible external copy of the data. Thus, the recycle bins do not meet Gartner's definition of backup... In addition, Office 365's native capabilities offer limited recovery from ransomware or file corruption."*
>
> — Gartner report: *Prevent Data Loss by Assessing Your Office 365 Backup and Recovery Needs*[2]

Druva provides a comprehensive, secure, scalable 100% SaaS platform for the enterprise that cost-effectively protects data for Microsoft 365, along with other SaaS applications, cloud applications, endpoints, and data centers, all from one simple solution. With Druva, you can rest assured that critical data protection gaps are addressed and your organization is protected from key risks like human error, internal threats, and ransomware. Druva also helps ensure the enterprise is compliant with regulations for data privacy, retention, and residency, as well as legal hold and eDiscovery. Druva's goal is to protect end-user productivity and ensure business continuity.



[1] Microsoft Services Agreement, April 1, 2021

[2] Gartner report: *Prevent Data Loss by Assessing Your Office 365 Backup and Recovery Needs*; 12 August 2019/Jerry Rozeman, Michael Hoeck

Closing Microsoft 365 data protection gaps

There are five key Microsoft 365 data risk considerations when planning your data protection strategy.

1. Human error

Microsoft 365 is fundamentally a productivity and collaboration tool. Thus, Microsoft leaves backup and recovery responsibilities in the hands of its users. It is prone to human errors such as accidental file deletion and overwrites by employees and their collaborators, and potential deletion of a whole SharePoint site by an administrator. Information can also be corrupted by OneDrive synchronization and third-party apps. Microsoft 365 native data recovery relies on end-user knowledge, versions, and recycle bins, and is subject to Microsoft's limited data retention policy. Accidentally deleted or corrupted data is lost forever if it is discovered after 30-93 days, depending on your Microsoft 365 solution. Microsoft support may need to get involved in attempting to retrieve lost data, and even if possible, Microsoft SLAs may not meet your business continuity goals. These risks can be mitigated by leveraging a comprehensive third-party data protection solution.

Druva protects against accidental deletion, overwrites, and data corruption:

- Unlimited data retention
- Complete data isolation in an external environment
- Ongoing automatic backups of data
- Flexible and granular recovery with unlimited "time travel"
- Easy-to-use self-service user recovery or IT-led recovery
- Many recovery options, including individual file or bulk recovery, "in-place," "as a copy," or "point in time" recovery, as well as recovery outside Microsoft 365

> *"... the security I feel having Druva now, compared to before when I just relied on Microsoft, is life changing for me!... Peace of mind is the biggest ROI I can think of!"*
>
> — Marty Goldstein, IT Director, Trascent Management Consulting, via TrustRadius

2. Insider threats

Data stored in Microsoft 365 should be safeguarded against internal malicious threats. Departing employees may intentionally delete data as an act of revenge, and rogue admins with higher access levels may bulk-delete files causing extensive loss of intellectual property. Microsoft cannot detect malicious Microsoft 365 user actions, and it may take your team time to discover that damage was done or to identify the scope of the data loss. If the threat is detected outside Microsoft's retention window of 30-93 days, the data may be lost forever. Once an employee leaves the company, their Microsoft 365 account is suspended, so IT cannot easily access it to assess and undo the damage. Archiving departing employee accounts does not retain previously deleted data. Conversely, a third-party data protection solution allows you to fall back on a clean copy of data.

Druva helps prevent insider attacks so you can detect, assess, and quickly recover from data loss:

- Data anomaly detection alerts of suspicious insider activities
- Data forensics determines the extent of the damage and best recovery options
- Employee investigations of prior activities adds insights

- Data off-boarding to departing employee's manager
- Unlimited data retention and isolation offers "time travel" as far back as needed to recover data, even if outside Microsoft's retention window
- Audit logs monitor unauthorized data restores to identify data leaks

3. Ransomware

Not surprisingly, ransomware is a major concern for organizations today. Ransomware threats to Microsoft 365 are exacerbated by OneDrive's characteristics (such as file synchronization and sharing), making the platform prone to malware propagation, infecting more files including those in recycling bins. Microsoft 365 offers tools to protect your perimeter against attacks. However with increasingly sophisticated attacks, no prevention is full-proof. When ransomware strikes, your organization may be exposed. By the time the attack is detected, many files may be corrupt and unrecoverable, with the time and scope of the attack unknown. In the best case scenario, Microsoft 365 allows recovery from versions at the individual file level. This approach is painful when dealing with multiple corrupt files. In the worst case scenario, if the attack started outside the Microsoft retention window, you have no recourse or means to return to clean data. Only a third-party solution can quickly recover your system to clean data and meet your business continuity SLAs.

If Microsoft 365 data is attacked by ransomware, Druva's enterprise-class solution is designed to quickly recover your data and return users to full productivity:

- Anomaly detection and data forensics to conduct investigations, alert on unusual activity, and pin-point time and scope of a ransomware attack
- Indefinite data retention enables full and quick recovery to pre-attack "point in time" data
- Recover in minutes through single-click bulk recovery, and meet your SLAs
- Easy-to-use self-service recovery as well as admin-initiated recovery
- Extensive recovery options, including "in place," "as a copy," or "outside" Microsoft 365 using bulk, or flexible restore, with granular options as needed
- Full data isolation in an external location ensures recovery to clean data, regardless of the scope of attack

4. Data retention gaps and compliance

In regulated industries, such as pharmaceuticals and healthcare, data retention is a core requirement. Data retention is also a key component in many organizations' data governance policies. Microsoft Business editions have a data retention policy limited to 30-93 days, depending on licensing tier and use case, whereby data retention differs for Microsoft Exchange, SharePoint, and OneDrive. Additionally, Microsoft 365 only offers 90 days' maximum audit history, which may be insufficient. And not to mention that Microsoft 365 data is retained in the same primary environment, thus not providing sufficient data isolation to comply with disaster recovery requirements. Such data retention gaps expose your organization and put you at risk of non-compliance with government and organization policies. More expensive Microsoft Enterprise tier plans offer some data governance capabilities, but they require complex data retention and policy tag configurations. On the other hand, a third-party data protection solution helps retain data and audit logs to ensure compliance with regulation and protection in the event of a disaster.

Druva enables compliance with data retention regulation and your organization's data governance requirements:

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

5. Legal hold and eDiscovery

When your organization is involved in litigation, you must comply with court-ordered eDiscovery and legal hold requirements. Without the right tools, compliance can be painstaking. eDiscovery requires legal teams to have immediate access to all user data related to the case in order to avoid penalties. Microsoft Business editions do not offer legal hold capabilities, while common Microsoft Enterprise plans do, limited to Microsoft 365 data only. Data retention gaps may also impede full compliance, such as departing employees or intentional deletion. Legal hold capabilities, if included in Microsoft 365, do not integrate with eDiscovery third-party tools. Therefore, only a third-party data protection solution can support end-to-end legal hold and eDiscovery requirements across enterprise data workloads, with no disruption to employees.

Druva provides comprehensive support for legal hold and eDiscovery requests, not only for Microsoft 365 but across enterprise workloads:

- Unified legal hold for Microsoft 365 and other SaaS solutions and endpoints
- Centralized, automated, complete data collection with no disruption to employees
- Bulk custodian holds, faster export speed, and support for multiple file formats
- Data retention capabilities allow unlimited "time travel" and data collection from departing employees, or in spite of intentional deletions
- Fully integrated with third-party eDiscovery tools and offering accelerated download

> *"Druva — complete and easy solution for Microsoft 365 backups! We use Druva to solve the "problem" of Microsoft 365 backups. We use it to back up all the content that all of our users have in not only their Microsoft 365 email but also their OneDrive and SharePoint... with the adoption of Microsoft Teams, we are now using Druva to back up the files that users keep in Teams... ROI has been positive overall. [Our previous solution] was several times more expensive than Druva, and appeared to be a lot more complex and time-hungry to manage."*
>
> — Martin Tillbrook, IT Operations Engineer, UK Broadband, via TrustRadius

The Druva advantage

Protect SaaS with SaaS

Gain the same cloud benefits that led you to choose Microsoft 365:

- On-demand scalability and elasticity and automatic clustering
- Rapid biweekly product updates to support new Microsoft 365 applications and features
- 15 minutes to deploy, then scale performance and capacity on-demand
- Simple to manage; one platform that provides data resilience and AI/ML-powered data intelligence across the enterprise

Reduce TCO by 50 percent

True 100% SaaS data protection and backup improves cost efficiencies and reduces TCO by 50 percent:

- No upfront investment in hardware, infrastructure or storage; pay for what you use.
- Limitless, automated scale up or down delivers dramatic storage savings
- Eliminate administration overhead cost — no hardware or software installation; no upgrades, patches, software monitoring, capacity planning, or cluster management

Protect your key workloads

Comprehensive, central control from a single pane of glass for:

- Microsoft 365 — SharePoint, Exchange Online, OneDrive, Teams
- Additional SaaS applications — Salesforce, Google Workspace
- Hybrid — VMware, NAS, Nutanix, Oracle, MS SQL
- AWS workloads — Amazon EC2, Amazon RDS, Amazon DynamoDB
- Endpoints

Protect productivity

Simplicity and security to enhance your productivity with Microsoft 365:

- Easy to use, flexible, and granular self-service backup and recovery
- Streamlined UI for IT with central, automated control, flexible, granular backup, recovery options, and less tickets in IT queue
- Zero administration overhead for IT, no patching, maintenance, or upgrades

Secure and retain data

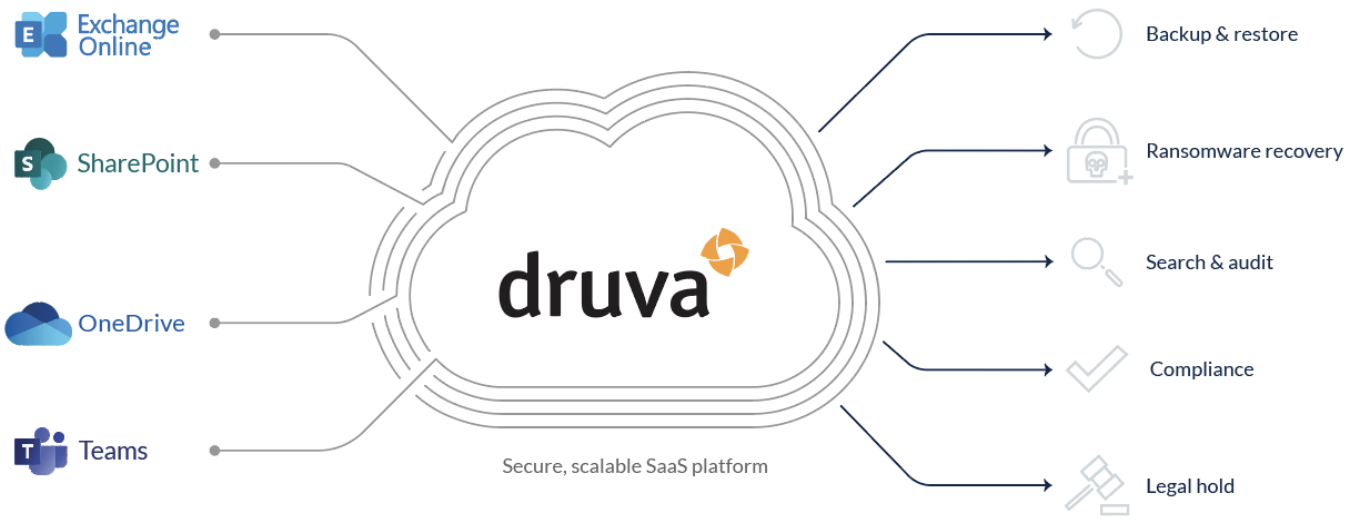
Keep your data safe with AWS-provided security and privacy standards:

- Compliant with SOC 1 (SSAE 16), ISAE 3402 (formerly SAS 70), SOC 2, SOC 3, ISO 27001, PCI DSS Level 1 (Cloud), and HIPAA
- Continuous backups and unlimited data retention
- FedRAMP ATO-certified SaaS data protection solution

Data isolation

Druva provides full data isolation with an independent copy of your data in an environment outside of Microsoft 365:

- Offers full data recovery in the event of a major catastrophe
- Meets disaster recovery regulation compliance



Turn to Druva for a comprehensive, scalable, cost effective, 100% SaaS platform to protect Microsoft 365 data and other workloads from common risks like accidental deletion, file corruption, insider attacks, ransomware, and non-compliance with data retention, legal hold, and eDiscovery.

Druva helps some of the world's largest enterprises protect their investment in Microsoft 365 — including Exchange Online, SharePoint, OneDrive, and Teams, from data loss and compliance violations.

Close the gaps in your Microsoft 365 data protection, keep your employees productive, and meet your business continuity SLAs.

For more information, visit druva.com/microsoft365

aws marketplace

Find Druva in AWS Marketplace

Get started

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: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva enables cyber, data and operational resilience for every organization with the Data Resiliency Cloud, the industry's first and only at-scale SaaS solution. Customers can radically simplify data protection, streamline data governance, and gain data visibility and insights as they accelerate cloud adoption. Druva pioneered a SaaS-based approach to eliminate complex infrastructure and related management costs, and deliver data resilience via a single platform spanning multiple geographies and clouds. Druva is trusted by thousands of enterprises, including 60 of the Fortune 500 to make data more resilient and accelerate their journey to cloud. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.