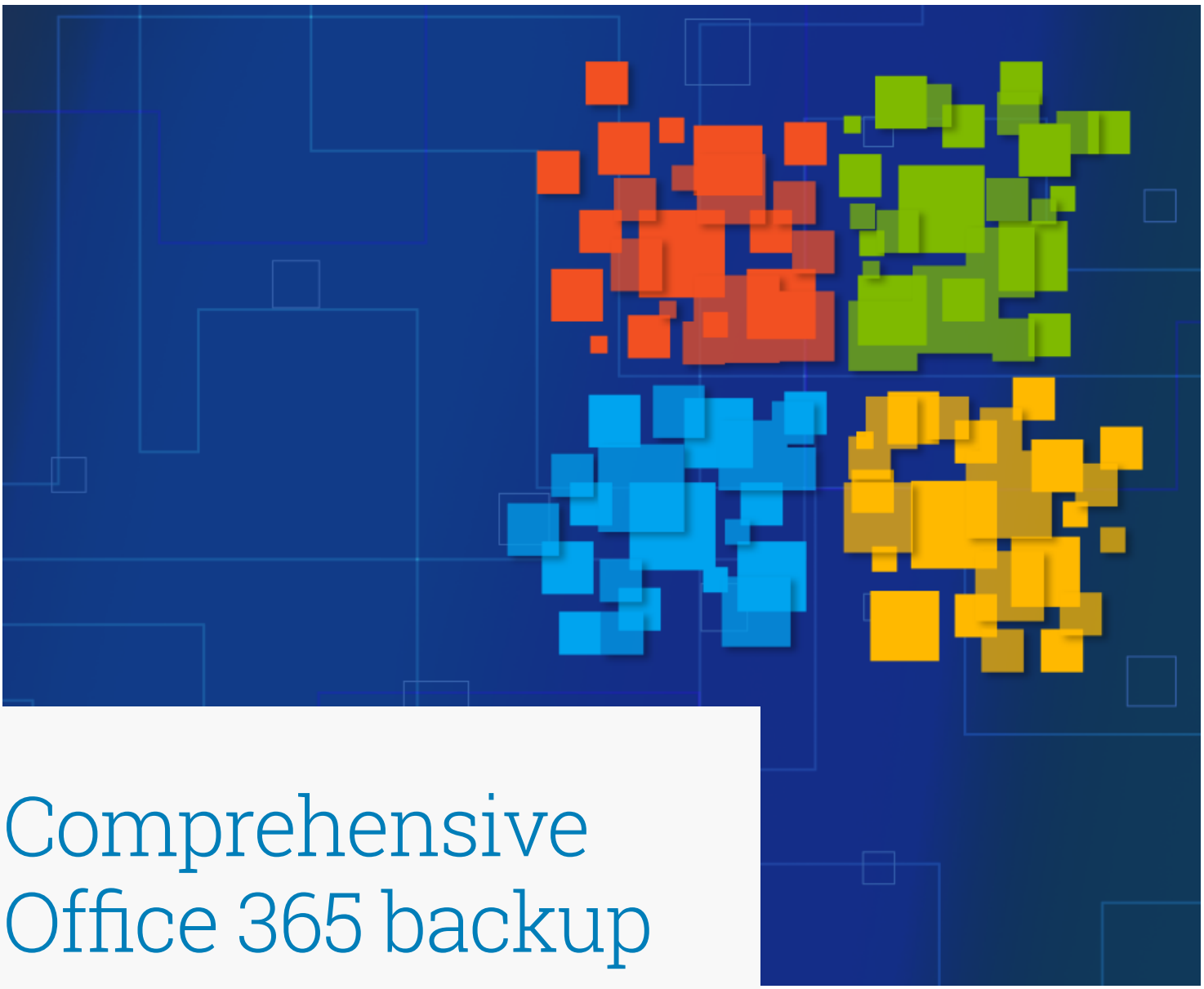
druva

Solutions white paper



Comprehensive Office 365 backup

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

Q120-20061

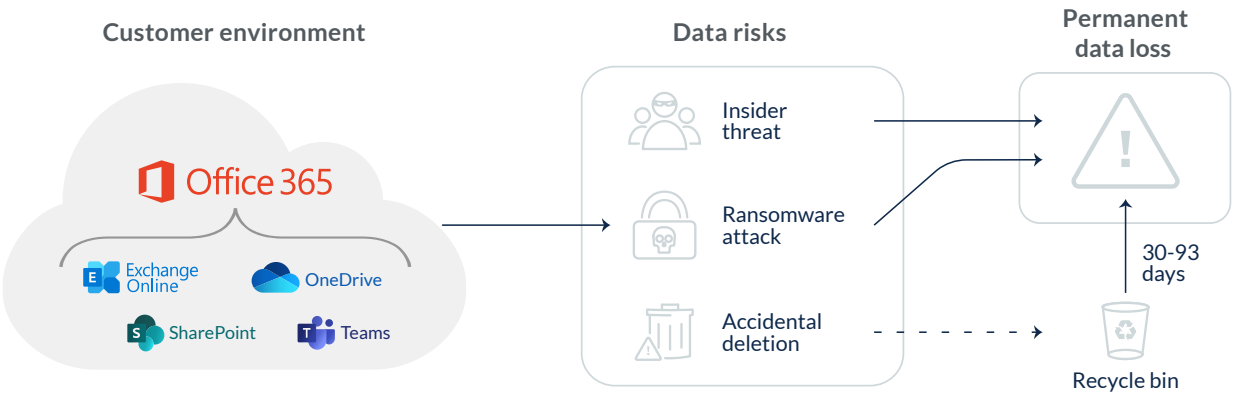
Why protect Office 365 data

Many organizations are adopting Microsoft's highly successful Office 365 productivity and collaboration suite of tools in the cloud. But not all of them realize the inherent data risks that must be addressed to ensure ongoing end-user productivity and to safeguard intellectual property. Further, data protection responsibility for Office 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 Office 365 data by 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 and scalable SaaS solution that cost-effectively protects Office 365 data, along with other cloud workloads, such as other SaaS applications, enterprise endpoints, and data center servers, all from a single point of control. With Druva, you can rest assured that critical data protection gaps are addressed and your data is safe against key data risks like human errors, internal threats, and ransomware. Druva also helps your organization be compliant with regulation for data privacy, retention, and residency as well as legal hold and eDiscovery. Our goal is to help your organization protect end-user productivity and ensure business continuity.



Closing Office 365 data protection gaps

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

[1] https://www.microsoft.com/en-us/servicesagreement
[2] Gartner report: *Prevent Data Loss by Assessing Your Office 365 Backup and Recovery Needs*; *12 August 2019/Jerry Rozeman, Michael Hoeck*

1. Human error

Office 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 potentially deletion of a whole SharePoint site by an admin. Information can also be corrupted by OneDrive synchronization and third-party apps. Office 365 native data recovery relies on end-users' knowledge, versions, 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 Office 365 solution. Microsoft support may need to get involved in attempting to retrieve your lost data, and even if possible, Microsoft SLAs may not meet your business continuity goals. These risks can be mitigated when you turn to a comprehensive third-party data protection solution.

Druva protects you 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 Office 365

> *"We value the Microsoft O365 cloud platform, but when it comes to restoring deleted files, their restoration process is awful!… 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

In addition to worrying about external attacks, internal malicious threats should also be safeguarded. 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 identify malicious Office 365 user actions and you may not discover for a while that damage was done, or be able to identify the scope of 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 Office 365 account is suspended, so IT cannot easily access it to try to assess and undo the damage. Archiving departing employee accounts does not retain previously deleted data. Therefore, a third-party data protection solution allows you to fall back on a clean copy of data that may get deleted.

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 the 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 the attack happens outside of Microsoft's retention window
- Audit logs can be used to monitor unauthorized data restores, which could indicate data leaks

3. Ransomware

Not surprisingly, ransomware is a major concern for many organizations. Ransomware threats to Office 365 are exacerbated by OneDrive's characteristics, making it prone to malware propagation. As a collaboration tool, OneDrive's file synchronization and sharing rapidly spreads malware, infecting more files, including files in recycling bins.
Office 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, and time and scope of attack is unknown. In the best case scenario, Office 365 native only allows recovery from

versions at an 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 Office 365 data is attacked by ransomware, Druva's 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 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
- Flexible recovery options, including "in place" or "as a copy," or "outside" Office 365 using bulk, flexible, and 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 your licensing tier and use case, whereby data retention differs for Microsoft Exchange, SharePoint, and OneDrive. Additionally Office 365 only offers 90 days maximum audit history, which may be insufficient. And not to mention that Office 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 exposes your organization and puts 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 during a disaster.

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

- Unlimited, flexible, and automated data retention policies for Office 365
- Flexible audit history and data retention that supports compliance requirements
- Data isolation through an immutable and independent copy, stored in a different environment from Office 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 offer some legal hold capabilities that are limited to Office 365 data only. Data retention gaps may also impede full compliance, such as departing employees or intentional deletion. Legal hold capabilities, if included in Office 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 Office 365, but across most enterprise workloads:

- Unified legal hold for Office 365 and other SaaS solutions, endpoints, datacenter, and AWS
- 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 offers speedy download times

> *"Druva inSync—complete and easy solution for Office365 backups! We use Druva inSync to solve the "problem" of Office365 backups. We use it to backup all the content that all of our users have in not only their Office365 email but also their OneDrive and SharePoint… with the adoption of Microsoft Teams, we are now using Druva inSync to back up the files that users keep in Teams… ROI has been positive overall. Veeam was several times more expensive than the Druva inSync 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 Office 365

- On-demand scalability and elasticity and automatic clustering
- Rapid innovation velocity with biweekly product updates, to support new Office 365 applications and features
- 15 minutes to deploy

Reduce TCO by 50%

True SaaS improves cost efficiencies and reduces TCO by 50%

- No upfront investment in hardware, infrastructure or storage; pay for what you use
- 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

- Office 365—SharePoint, Exchange Online, OneDrive, Teams
- Additional SaaS applications—Salesforce, Slack, G Suite
- Datacenter servers
- AWS workloads
- Endpoints

Protect productivity

Office 365 is all about productivity and we are all about protecting it

- Easy-to-use, flexible, and granular self-service backup and recovery
- Streamlined UI for IT with central, automated control, flexible, granular or bulk backup and recovery options and less tickets in IT queue
- Zero administration overhead for IT

Secure and retain data

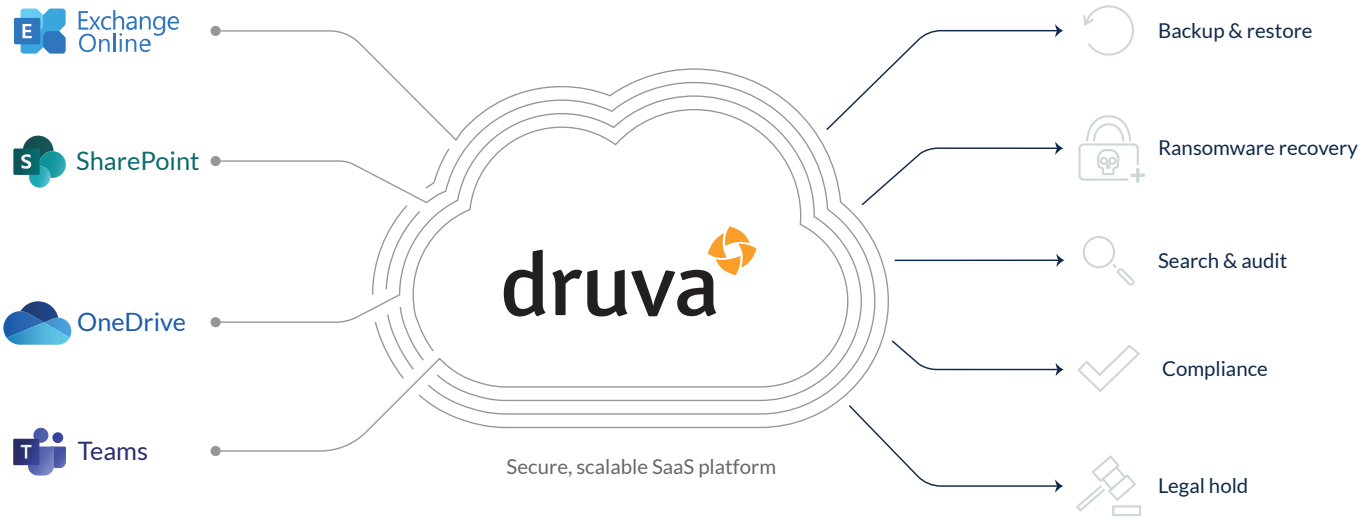
Keep your data safe with AWS-provided security and privacy standards

- 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
- Only 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 Office 365

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



Turn to Druva for a comprehensive, scalable, and cost effective SaaS platform to protect Office 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 organizations protect their investment in Microsoft Office 365, including Exchange Online, SharePoint, OneDrive and Teams, from data loss and compliance violations. Check out druva.com/office365—find out how we can help close the gaps in Office 365 data protection, keeping your employees productive and meeting your business continuity SLAs.

druva

Sales: +1 800-375-0160 | 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™ 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 and follow us @druvainc.