



Unlock the value of Office 365 data protection

Why cloud-native data
protection and management
is essential



Office 365 productivity + cloud scalability

Office 365 is a brilliant way for you to combine the comprehensive productivity benefits of Microsoft software with the scalability and efficiency of the cloud. Its feature set is broad, yet it is not a data protection and management program. As a cloud app, it maintains a copy of your current work, and you can pay extra for longer retention times, but it is simply not designed to provide full-featured protection, archiving, and compliance capabilities.

This eBook discusses a number of reasons why a third-party cloud data protection and management solution is an essential part of your Office 365 deployment:

- **Productivity vs. protection** — Understanding the difference
- **Malware protection** — Reducing cybersecurity vulnerabilities
- **Regulatory compliance** — Staying on top of regulatory requirements
- **Cost reduction** — Don't pay more for less



Productivity vs. protection

Understanding the difference

In an environment where secure, available data is the starting point for virtually all enterprise business processes, data protection is a fundamental requirement for your IT group. As enterprises like yours increasingly adopt Office 365 and other SaaS productivity tools, they often mistake the benefits of Office 365 cloud availability with the true data protection available from SaaS third-party apps that are dedicated solely to that purpose. Consider the following:

The “3-2-1 Rule”

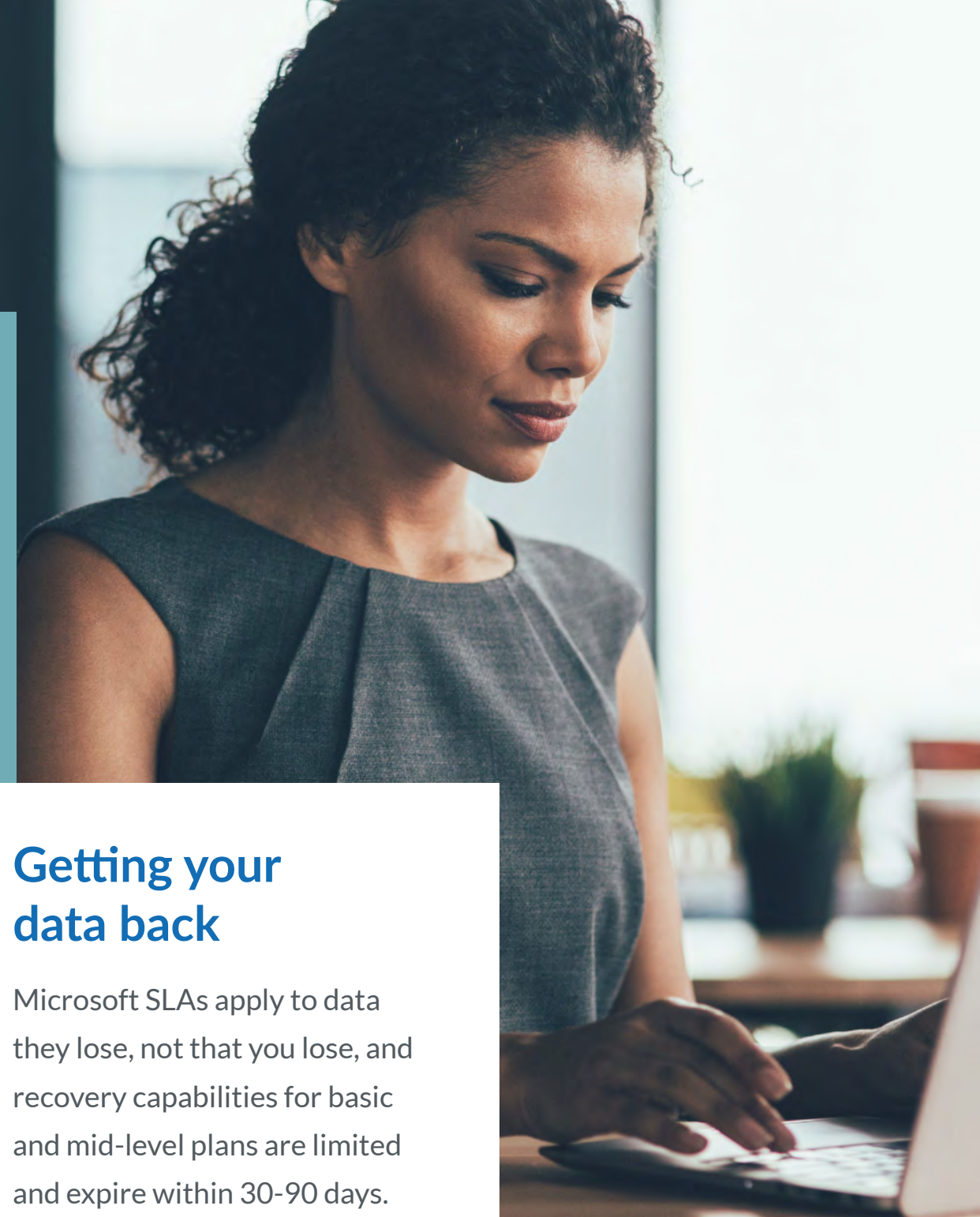
Office 365 doesn't meet the standards virtually all security professionals recommend: maintain three independent copies of your critical enterprise data: two on different platforms/media and one in a remote location.

The Recycle Bin isn't data protection

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

Getting your data back

Microsoft SLAs apply to data they lose, not that you lose, and recovery capabilities for basic and mid-level plans are limited and expire within 30-90 days.



Malware protection

Reducing cybersecurity vulnerabilities

Avoiding exposure to the never-ending stream of ransomware, viruses, bots, and other threats lurking in email messages and the web requires a layered, “defense-in-depth” approach. Firewalls, physical security, software, and educated end-users all help you protect your enterprise network from malware. But sooner or later, hackers will compromise some of your data and Office 365 lacks the tools to effectively protect or recover from malware attacks.

The answer is to prevent what attacks you can and back-up time-indexed snapshots of all your enterprise data that can be quickly restored when data is corrupted or held for ransom.



Prevention

A malware attack typically starts to rename, delete, or encrypt files en masse. In the process of backing up data to the cloud, a third-party SaaS data protection solution can automatically monitor file status and detect odd changes (anomalies) and proactively alert IT to take action.



Restoration

Backups hosted by a cloud service provider (CSP) are protected from infections impacting your enterprise network. A time-indexed backup at the CSP allows you to recover a pristine (before malware) version of your data, and minimize downtime and loss.

druva

Office 365

Regulatory compliance

Staying on top of regulatory requirements

Compliance, regulatory, and eDiscovery challenges are sometimes exacerbated by cloud productivity apps like Office 365. For example, your backups of government data may need to reside in a FedRamp-authorized facility and other data may have residency restrictions to meet GDPR and eDiscovery requirements.

- **eDiscovery** — The core of eDiscovery is the process of mining through data to identify/isolate information that is relevant to a legal matter. Office 365's mail app, Exchange, maintains separate indexes for each mailbox which creates performance challenges for searching across mailboxes. A third-party app that backs up email files as a whole and adds metadata enables thorough yet very simple and quick searches and access.
- **Legal hold for all data** — Office 365 litigation hold capabilities deal only with content in Office 365, not content stored elsewhere. A third-party solution can enforce legal hold policies across all data sources, eliminating the need for multiple, disparate systems for setting and applying legal holds.
- **Legal inquiries** — Having timely and easy access to current and historic data for collection and review purposes is critical during the litigation process. Collect data with third-party backup can protect against "data spoliation," ensuring defensible data handling and preservation.



Cost reduction

Don't pay more for less

The most common reason why enterprises neglect to comprehensively protect Office 365 data is the mistaken presumption that “it’s all taken care of” simply because it’s a SaaS platform. Your organization may be unaware of the significant gaps in protection and lost productivity from not deploying a full-featured cloud data protection solution. You may also be unaware of how using a third-party solution can enable deploying more economical Office 365 plans. Consider the following when balancing the costs of Office 365 plans and complementary third-party data protection SaaS:

Right size your subscription

Only the Office 365 E5 offers data protection capabilities, yet it still lacks important data protection features. Cost-wise, the least-expensive solution is to combine a third-party data protection app with a less-expensive Office 365 plan.

Reduce storage usage

Office 365 retention policies result in 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 50 gigabytes of storage per user in a 1,000-user company will cost \$10,000 per month.

Reduce duplication

Corporate users typically keep identical copies of the same data, with the same files duplicated on hundreds and sometimes thousands of endpoints worldwide. A cloud data protection solution that uses rich metadata to enable global deduplication can reduce data volume significantly.



Your Office 365 content needs cloud data protection

Your company's productivity depends on more than Office 365 alone. It has a broad feature set and takes full advantage of the benefits of the cloud. However, you wouldn't dream of using it to replace apps for content management, graphic design, or software coding. Your data protection and management solution is no exception. It is an extremely important, highly specialized application, and effective software can't just be added on to programs that are designed to do something completely different.

Druva's SaaS data protection and management is designed to do one thing exceptionally well: protect precious enterprise data across endpoints, data center, and cloud workloads such as Office 365 — without any dedicated hardware, software, or skilled resources.

Read this white paper by Osterman Research, [Filling the Gaps in Office 365](#), to learn more about cloud data protection for Office 365.

- **Protection** — Architecturally, Druva fulfills the 3-2-1 standard for backups and enables fast and easy restores by both end users and admins.
- **Malware** — Druva anomaly detection helps prevent malware losses and rich time-indexed metadata ensures you never have to pay off ransomware.
- **Compliance** — It enables full compliance with eDiscovery, legal hold, FedRamp, and other stringent archiving requirements.
- **Cost** — There's no reason to pay extra for a top-tier plan when it doesn't do what you need it to do. Druva delivers, and the combined cost is less.

Built on AWS, Druva delivers globally accessible, infinitely scalable, and completely autonomous enterprise data resiliency and compliance. It is a vital and natural complement to Office 365, offering unmatched simplicity, savings, scalability, and security.





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](#) and follow us [@druvainc](#).