White Paper

OFFICE 365: THE CRITICAL GAPS

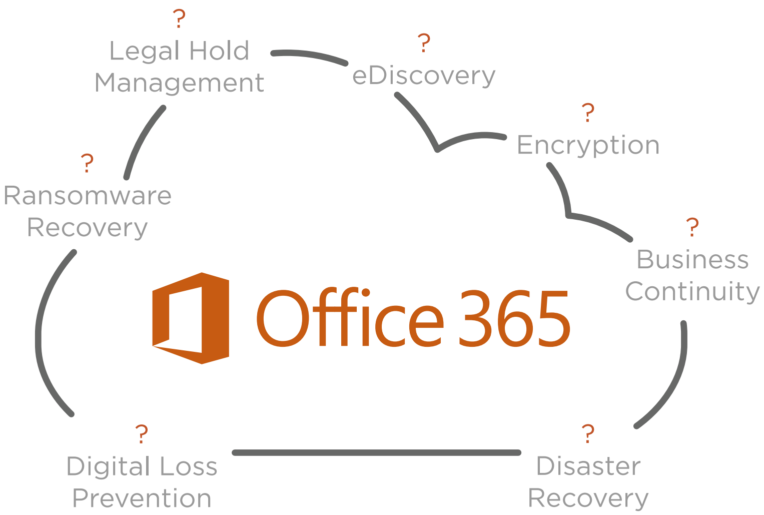
How Druva Addresses the Missing Layers of Data Protection

Q319-CON-10934

Understanding the Gaps of Cloud Applications

While the rapid adoption of SaaS-based applications has been fueled by the unique advantages of the cloud, it is essential to note that no offering—cloud-based or otherwise—can be all things to all customers. For instance, even though Office 365 comes in a variety of packages with different capabilities and at a wide range of price points, decision-makers must remember that the offering is intended to serve certain needs of a large, enterprise audience. The core capabilities of Office 365, while powerful, are not necessarily built to be a comprehensive solution for companies' data availability and governance requirements. This is why many businesses still need to supplement the native capabilities of Office 365 to establish a strong data protection solution in the cloud in order to maintain a position of compliance in their industry.

The Missing Layers of Cloud Data Protection



In fact, Gartner Research strongly recommends organizations deployed on Office 365 use third-party offerings to address gaps in its native capabilities. These third-party features include those that fill these gaps for legal hold management, eDiscovery, DLP, ransomware recovery, advanced threat protection, encryption, and business continuity. While Office 365 includes a number of these capabilities, the platform cannot be all things to all organizations, so it contains some deficiencies that purpose-built, third-party offerings can more adequately address. Often times, these capabilities can come with a better price-point than Microsoft can offer.

> *"We have become painfully aware that Microsoft doesn't backup Office 365 well. Thinking Microsoft would be able to recover it was not the case. Microsoft response was, 'it's not in our service level agreement'. So we have some levels of weakness that we need to address with MS around protecting O365 data."*
>
> *— Microsoft Office 365 Customer*

Here are few key reasons why having a third-party data availability and governance offering in conjunction with Office 365 is critical, and provides a major benefit (capabilities and price-point) to any organization.

Data Recovery

Leading online service providers such as Microsoft offer cloud-based information solutions that are essential to businesses and operations around the globe. But do these major SaaS providers protect their customer's data with backup and recovery? Why would anyone want additional protection for data that's already in the cloud? It turns out that cloud providers do indeed offer different levels of recovery, largely to ensure data accessibility and save themselves and their clients from data loss. But here's the catch: such backups are not intended to make all data available to customers. In fact, cloud solutions are not natively designed for data restoration, and the cloud providers that do have backup capabilities may charge customers a sizeable fee for retrieval. Generally speaking, in most online services, the only backup you have for your organization's data is via the recycle bin, which is automatically purged after a fixed period of time. After that, your data is gone forever.

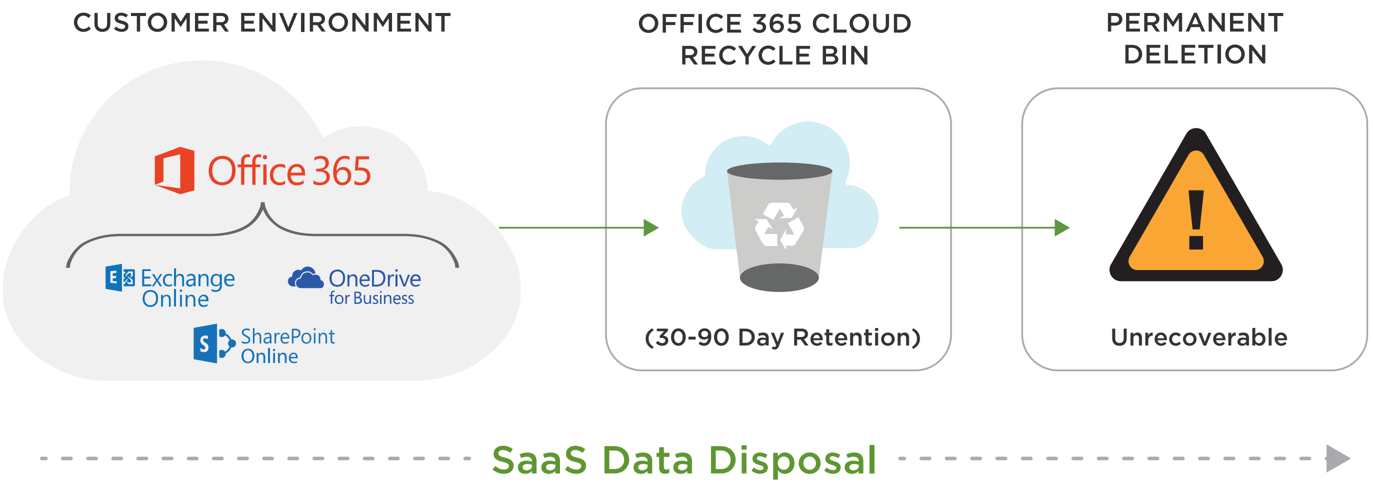
The truth is that once your data is deleted, altered, or corrupted—whether accidentally or intentionally—there is very little an admin can do to recover it.

File Sharing is not Data Protection

People often assume that because they're using a cloud-based file sync and share solution like OneDrive for Business, that their data is protected, as if it was backed up. It's quite the old argument: "We already have OneDrive for Business, can't you just store your files on OneDrive and call it a day?". The short answer is there are significant and important differences between these types of online services. While file sharing and data protection technologies have some overlapping features, they are fundamentally different in their approach. Here's what you need to know.

It's important to understand why Microsoft's file sync and share solution, OneDrive, is not backed up. File sharing is built for real-time collaboration with user content, but it is not designed for data recovery in the case of user error, data corruption, or ransomware. Nor does it address archiving or a completely new set of compliance and eDiscovery challenges.

Enterprise backup software differs from file sync and sharing in that the software automatically makes a copy of every user's data available for recovery. Endpoint and cloud application data is protected in its entirety and if a device is lost or stolen, additional features such as remote wipe and geo-tracking help organizations trace the device and/or remotely delete corporate data. In addition, backup of a user's system and application settings ensures that new or replacement devices can be set up quickly, while preserving a user's familiar working environment.



The Many Causes of Data Loss

While it's extremely unlikely that a major online service provider will lose all your data or suffer a complete service outage, there are a number of other causes of data loss that are very real and occur all too frequently, including:

- **Accidental Deletion and User Error —** More often than not, data is deleted only for the user or organization to later realize that it is still needed. For instance, you might delete a scrapped project and then later learn it is starting up again. Or a collaborator may delete a shared project by accident. Information can also unknowingly be overwritten or corrupted by users and third-party apps.
- **Malicious Actions —** People often delete data before they quit if they suspect they are going to be fired, or to spite a boss or co-worker. Hackers can also be the culprit, surpassing security systems to delete or corrupt data. Whether internal or external, these scenarios are a reality.
- **Data Corruption —** Applications hold large amounts of an organization's most mission-critical data that is constantly updated. Over-writing data is a common problem that occurs when large data sets are imported into the application via bulk uploads or when integrated, third-party applications are used to manage the data inside the SaaS application. For example, what if your project management app purges all your calendar events or overloads your inbox with redundant, malformed messages? What if your expense report app paves over your tax records spreadsheets with garbage data? What if your marketing analytics tool corrupts your CMS database, destroying all your carefully coded web designs?
- **Service Provider —** Loss of data due to an e-service provider revoking access to your account can be catastrophic, with no options available until the services are back online. Imagine your primary file-sharing application going offline with reports, presentations, and client deliverables on hold until the issue is resolved. What would the cost be to your organization?

Ransomware in the Cloud

A few years ago, no one had even heard of ransomware. Today, ransomware is not only commonplace, it's on the rise. What most organizations don't realize though, is that SaaS applications are equally at risk, with hackers constantly employing new strategies and turning this once rare form of intrusion into its own mature industry. The ransomware threat is no longer limited to a handful of business in a couple of verticals, but now affects all organizations and industries. At the same time, the threat is no longer limited to physical devices, but is a major concern now for users of cloud applications as well. Companies are quickly finding themselves struggling to understand this unsettling new threat and how to adequately plan their response to an attack.

Ransomware is on track to become a

$1B

industry

Downtime from ransomware costs small businesses around $8,500 an hour. In the US, this adds up to a loss of $75B+ per year. And since these criminals continue to operate with zero consequences, it's likely these crimes will not only increase in frequency and severity but also become a standard part of a company's daily threat landscape. According to the Federal Bureau of Investigation's Internet Crime Complaint Center, there were nearly 2,500 complaints registered in 2015 representing $1.6M+ in damages. But the true numbers are far higher, as less than 1-in-4 incidents are actually reported.

What's at Stake?

Many organizations fail to understand that the cloud is just an extension of a user's operating environment. Data in the cloud is just as susceptible to loss, theft, or malicious attack as anywhere else. Enterprises are still responsible for managing data in the cloud and failure to comply with rules and regulations can result in hefty fines and, worse yet, loss of reputation.

> ***"By 2020, over 50% of all corporate data will reside outside of the corporate data center."***
>
> *— Gartner, Plan Your Data Exit Strategy Before You Sign a SaaS Contract, Published March 2016*

Organizations need to take into account three new challenges and considerations around data availability, compliance, and security in order to adequately address the data protection and governance gaps brought about by the rise of cloud apps:

- **Ensuring Always-On Data Availability —** A common misconception among IT leaders and end users alike is that SaaS or cloud data does not need to be protected because the SaaS vendor is already backing up your sensitive enterprise information under their Service Level Agreement (SLA). However, what many people are not aware of is the fact that the SLA provided by their SaaS vendor only covers data loss if the SaaS provider is at fault—e.g., a service outage. The SLA typically does not cover data lost due to accidental deletion, migration errors, data corruption, or malicious attacks. SaaS vendors may not be able to help you recover deleted data older than 30 days, because their service, as a part of their standard, permanently purges the deleted information after that period. Even if the SaaS provider is willing to work with you, and the data still exists, they may charge you a sizeable fee and recommend you use a cloud backup solution. Still, in the event that the data is actually recovered, there are countless hours of productivity lost while trying to get it back.
- **Meeting Legal Hold Obligations —** Today, businesses can face very serious consequences if they fail to produce data stored on SaaS platforms during litigation following a discovery request made by the courts. This requires legal teams within an organization to have immediate access to user data that may be critical for the defense of their case or to avoid serious penalties. In many cases, some or all of this data resides in cloud services like Office 365 or Box, which may not be recoverable or continues to remain completely unprotected throughout the litigation process and susceptible to deletion or mishandling by the users.

  The core of legal discovery is the process of mining through the data to identify and isolate information that is relevant to the litigation. To do so assumes that information is properly indexed and that the search functionality is sufficiently flexible. In addition, during early case assessment, the ability to see results in real-time and refine the search based upon the results becomes essential.

  Not having timely and easy access to current and historical data for collection and review purposes could cost an organization millions of dollars in legal fees or even the outcome of a lawsuit. Collecting data residing on cloud applications, while preserving and handing it in a way that can be defensibly presented in court (no data spoliation), is key for every organization and their legal team to address with an effective solution.
- **Addressing Security and Compliance in the Cloud —** A top concern for any Information Security (InfoSec) team is the risk associated with the leakage of sensitive and confidential data. A recent study performed by Dimensional Research indicates that close to 95% of businesses have some form of sensitive data in the cloud. The cost of not protecting this data can be staggering, not just in the form of regulatory fines, but also measured by the effects it would have on a business' reputation and the significant loss of trust as a result.

  With privacy laws changing constantly, the regulatory environment is becoming even more complex. The General Data Protection Regulation (GDPR) and Privacy Shield, adopted by the European Union (EU), demonstrates data visibility mandates that go beyond what most organizations have in place today. Sarbanes-Oxley, HIPAA, and new data privacy regulations have likewise forced businesses to drastically change how they capture, store, and secure data.

Business Case for Third-party Apps

Office 365 includes an entire suite of SaaS applications that offer a range of valuable capabilities which organizations rely on everyday to help them be more productive in achieving business goals. However, these powerful tools are not the purpose-built products that are needed to address the key concerns highlighted above. An increasing number of organizations have taken action to address the gaps in end-user data protection, data recovery, legal hold & eDiscovery, as well as third-party managing of Office 365 archival data.

> *"SaaS is growing at three-times the rate of on-premises software."*
>
> *— Boston Consulting Group*

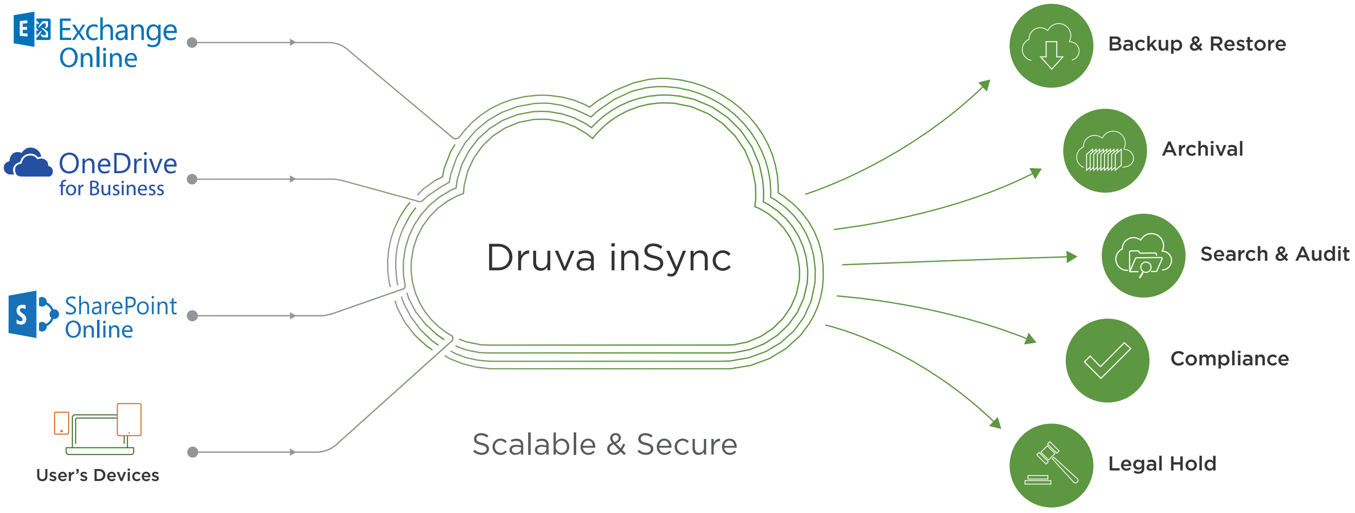
While Office 365 includes some of these capabilities, the platform cannot be all things to all organizations, and so it contains some deficiencies that third-party offerings can more adequately address and often at a better price-point than Microsoft. The chart below helps provide a clear picture of the key value that an effective third-party data protection solution should provide across all of these critical business issues.

Microsoft Office 365	Third-party Offering Benefits
Protection of All End-user's Data	Choosing a third-party data protection service that guards end-user's data, irrespective of where it resides—laptops, smartphones, tablets, or cloud applications—will aid in overcoming two key gaps in Office 365's data protection functionality: • Limited Functionality — Microsoft's services do not cover the full breadth of a user's digital footprint, since laptops and mobile devices are excluded, and provides limited backup, recovery, and archival for Office 365 data only.
Better Data Recovery	By using a third-party service in conjunction with Office 365, data can be easily and immediately recovered by an end-user or admin and can be downloaded or restored to any device or original location. This is in stark contrast to recovery services offered in Office 365: • Microsoft will recover your data, as per their SLAs, only if it loses your data • If you lose your data, then Microsoft's recovery capabilities are limited and expire within a short period of time (30-90 days depending on the service they have been paid for), beyond which, you cannot recover any additional data. • Microsoft cannot recover data in the event of a ransomware intrusion. A true backup service is required for this in order to provide the necessary time-indexed snapshot capability.

Better Basic Litigation Hold Capabilities	Supplementing your Office 365 environment with a third-party service to address the compliance, regulatory, and eDiscovery challenges of your enterprise will save your organization significant time, hassle, and money. • The litigation hold capabilities deal only with content in Office 365, but not content stored elsewhere. • Existing legal holds created in Exchange or SharePoint were workload specific and cannot be migrated into Office 365's new unified Security & Compliance Center. As a result they cannot be pulled across for a unified view of current and outstanding legal holds. • Exports from Office 365 are not protected and so are at risk of alteration and spoliation. Moreover, there are no additional encryption options provided by Microsoft to encrypt the export.
Third-Party Managing Archival	Just like offsite replication like within your data center, you'll want to have a separate copy of all your cloud application data stored securely in a different cloud structure in case of outages or in the event that your service provider revokes access to your account.

How Druva Fits In

Druva helps some of the world's largest organizations protect their investment in Microsoft Office 365 from data loss and compliance violations. Druva's industry-leading solutions, inSync, gives users a single pane of glass to monitor and protect data no matter where it resides.



Druva inSync is the essential layer of data protection functionality companies need to defensibly archive and discover business-critical information, adding to the core of Office 365 without sacrificing security or compliance across four crucial areas of exposure:

- Protection of All End-user's Data
- Data Recovery
- Data Governance
- Third-Party Managing Archival

Where the Value is Added

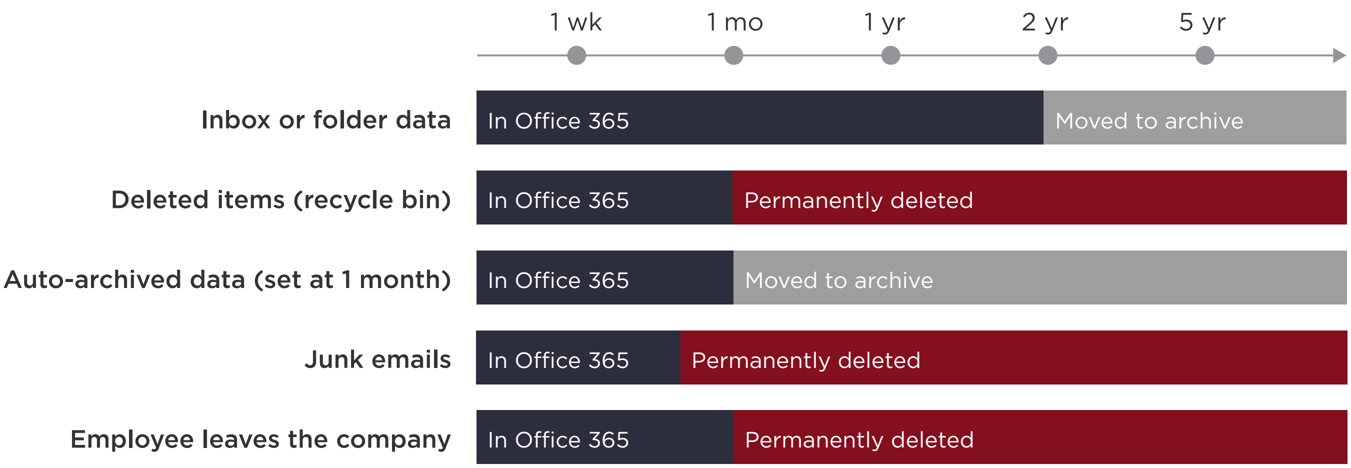
The following sections provide a comparison of the capabilities provided by the Office 365 and the inSync services.

Backup and Recovery Options

Office 365 does not offer traditional backup and recovery capabilities in the same way as organizations have deployed in on-premises environments in the past because it is a live production system that offers recovery of messages and documents within a rolling time window.

Microsoft Office 365	Druva inSync
Office 365 Exchange: Deleted items are moved to the Deleted Items folder where they will remain until either manually deleted or automatically deleted based on the retention policies (default is 30 days). Once deleted from the Deleted Items folder, items will remain in the Recovered Items folder for a minimum of 14 days.	**Office 365 Exchange:** inSync provides unlimited retention for emails, calendar, & contacts. Emails backed up by inSync can be recovered at any point in time. inSync provides the ability to restore emails directly to a user's mailbox and also to another user to support recovering emails of a departed employee.
Exchange Online Archiving: Microsoft offers Exchange Online Archiving as part of E3 and E5 plans, or as a separate add-on at an additional cost per user (currently $3 per user /month). This is an email-only archive that must be setup for each individual mailbox, and does not include archiving of calendar, contacts, or tasks. Although individual emails can be recovered, this does not provide the ability to restore a mailbox from a specific point in time.	**Exchange Online Archiving:** inSync can also backup a user's Exchange Online 'In-Place' Archive mailbox with unlimited retention. Emails backed by inSync can be recovered at any point in time. inSync provides the ability to restore emails directly to a user's mailbox and supports recovering emails of a departed employee.
OneDrive for Business: Deleted items are placed in a recycle bin and remain for 30 days before being completely purged. Users can restore items from the recycle bin before they are purged completely.	**OneDrive for Business:** inSync can backup user OneDrive for Business with options for unlimited retention.
SharePoint Online: Deleted items are placed in first the Site recycle bin and then the Site Collection recycle bin for a total of 90 days, at which point the item is completely purged from SharePoint Online. Data backup occurs every 12 hours. Individual files are not backed up directly; restoring an individual file will require restoring the entire Site. Data can only be restored to the original URL, overwriting the original data.	**SharePoint Online:** inSync can backup Sharepoint Online with options for unlimited retention. Backup occurs every four hours or manually as needed. Granular object-level backup allows individual files, libraries, or other SharePoint Online components to be restored. Data can be restored to the original location, a different location or can be downloaded.

Office 365 Retention Policies



Legal Discovery & Compliance Requirements

Legal Hold

When it comes to meeting information, governance, and legal reviews, cloud data is no different than data that would be located on endpoints or on-premises in email, CRM, or file services. Today, businesses can get into hot water if they fail to produce data stored on SaaS platforms. Legal or HR teams within an organization need access to user data to either support an investigative search or an active litigation. In many cases, some or all of this data (which could be key forensic evidence) resides in cloud services like Office 365 and may not have been archived.

Not having timely and easy access to current and historic data for collection and review purposes could cost an organization millions of dollars in legal fees or even the outcome of a lawsuit. Collecting data in cloud applications while preserving and handing it in a way that it can be defensibly presented in court (no data spoliation) is something that every organization and their legal team should be thinking about.

Microsoft Office 365	Druva inSync
Current legal holds created in Exchange or SharePoint cannot be migrated into the new experience in the Security & Compliance Center. They are separate objects that must run their course and then expire, rather than being something that can be pulled across for a unified view of current and outstanding legal holds.	All legal holds created in inSync can are compatible with older version of the inSync clients for a unified view of current and outstanding legal holds.
The litigation hold capabilities deal only with content in Office 365, but not content stored elsewhere. Organizations with significant data repositories outside of Office 365—on-premises and in other cloud services—will require multiple, disparate systems for setting and apply legal holds, creating a complex legal compliance minefield subsequent review.	The litigation hold capabilities, with inSync, seamlessly and proactively collect end-user data across endpoints and cloud applications via time-indexed backups.

No workflow support for coordinating with data custodians across the organization who may have content that is responsive to the legal hold parameters. While these could be manually created and sent, no audit trail reporting would be created for.	Seamless workflow support for coordinating with data custodians across the organization, with complete audit trails for all activities.

Export

The ultimate output of any archiving solution is data that is fed into another legal review system or passed directly to opposing counsel. Export performance and workflows are key attributes of an effective solution.

Microsoft Office 365	Druva inSync
Search results for Exchange Online, SharePoint Online and OneDrive must be exported from Office 365 to facilitate the review process—the Exchange content as one or more PST files, and the SharePoint and OneDrive content as individual files—creating a duplicate set of content outside of Office 365 which must be protected. Moreover, Exports from Office 365 are not protected and so are at risk of alteration and spoliation, and there is no reporting on actions taken on the exported content in the eDiscovery case in Office 365 because Office 365 is blind to post-export actions.	Once data has been collected in the cloud and placed on legal hold, processing can immediately take place by directly connecting well-known, third-party eDiscovery tools using direct-to-cloud connectors. The direct-access method removes the need for transferring information across insecure networks, using separate storage media, performing additional shipping or other cumbersome and costly methods. inSync provides a chain of custody report to ensure data is fingerprinted for authenticity and collected with extended metadata (as outlined by the Department of Justice and EDRM) to meet defensibility requirements.
A client-side app is used to export search results from Office 365 to Azure and then a local computer. For large exports, this could mean several hours of processing time, creating unhelpful delays in an urgent process for compliance officers.	Exporting is not required as 3rd party eDiscovery products can direct-connect to Druva's native cloud infrastructure—not discovery users' machines. As such, they do not depend on the user's computer resources being available. As well, data access can be easily achieved by mounting the legal hold as a device on a local machine. In the case of an explicit export request, auto-stop and resume occurs depending on device availability.
Results must be downloaded from the eDiscovery Center to the user's local machine, then uploaded to legal service providers.	inSync provides legal administrator access to review held data and expose it for ingestion directly to a 3rd party eDiscovery platform, without needing exporting first. In a few quick steps, the downstream legal process of review and tagging can begin.

Search and Investigation

The core of legal discovery is the process of mining through data to identify/isolate information that is relevant to the matter. To do so assumes that information is properly indexed and that the search functionality is sufficiently flexible. In addition, during early case assessment or investigative tasks, the ability to see results in real-time, combined with the power to refine the search based upon the results, becomes critical.

Microsoft Office 365	Druva inSync
Exchange Online maintains separate indexes for each mailbox. This is the optimum model to allow end-users to search within their mailbox, but it creates performance challenges for searching across mailboxes. In addition, because Exchange's indexing is a background process and a "best efforts" model, not everything that exists in mailboxes may be fully indexed at any given time. Depending upon your retention strategy, if a user deletes their copy of a message, yet it exists in other mailboxes, focusing on searching only their mailbox might miss relevant items that you still possess.	inSync maintains a unified index structure for the entire archive. A single-instance copy of each message exists in the archive, with metadata about which mailboxes each message belongs to. This allows for searching within specific mailboxes, or across the entire repository—all in near real-time. inSync indexes the content before it is added to the archive. This ensures that every item within the archive is fully searchable.
Due to the mailbox-based indexing model, Office 365 does not execute searches in real-time. Instead, you create a search job and get notified when it's complete. You can either copy the results to another "discovery mailbox" (in which case your search results are limited to the 50 GB maximum mailbox size) or you can create an Export job directly to PST files. While this model may work if you are extracting a whole mailbox, it does not allow for investigation or search refinement. The end result is that downstream discovery costs may be higher as more data needs to be processed. Due to batch processing, searches using the native Office 365 functionality are fairly slow. It can take several minutes to run a single search and search time increases based on the number of mailboxes in question.	inSync's real-time search experience allows you to easily scan through search results to identify opportunities for refinement. Not only is this critical for investigational activity, where you are trying to understand what was going on, but it also allows you to narrow the scope of data exported to third-party tools/vendors to reduce the next steps in legal discovery.
Office 365 executes searches on a mailbox-by-mailbox basis. As a result, the more mailboxes you search within, the longer it will take for the batch search to be completed. And since you can't preview results or initiate an export task until the search is finished, this can lead to significant amounts of wasted time during key discovery phases if you don't initiate follow-up steps immediately upon completion.	By default, discovery searches are performed across the entire archive. This allows you to use the archive as part of the identification phase to determine who might be potential custodians for a matter.

Data Integrity

To be useful for legal discovery, the data must be of evidentiary quality. It must maintain all of the metadata of the original message. In addition, the processes around data management need to ensure that data is never lost or corrupted.

Microsoft Office 365	Druva inSync
Office 365 is designed, first and foremost, to meet the business needs of communication and collaboration. To that end, data is replicated in near real-time between data centers to ensure very high availability. No snapshots or backups are performed. The drawback of this approach is that any corruption is also replicated, with no rollback possible. For legal discovery, this means that messages can be lost—including those that are on legal hold.	Druva's cloud uses object storage service and guarantees seven 9s (99.99999%) of reliability, thereby giving matching data resilience for inSync device data backups. inSync separates the data and metadata streams. For inSync cloud, data, and metadata are replicated across three data centers within the specified region. inSync cloud runs stateless compute nodes as backup servers. Due to the stateless nature of the backup servers, inSync can handle compute node failures without affecting the service.
The design of the Office 365 tenant architecture was designed so that each organization used one and only one tenant, homed in one geographical region, and to which all out-of-region traffic would route for access to the organization's data. What this means, therefore, is that under the original design, an organization with significant operations in multiple geographies cannot geo-ring fence content into local Office 365 data centers, which has implications for legal cases, government access, and compliance with data protection regulations.	Druva provides 30+ customer-selectable regions so that users can address regional variations in privacy rules and meet the needs of their data residency laws and regulations.
There is the potential problem of Office 365 (or any other single cloud provider) being the sole source of data. If there is not an independent store of the data for validation purposes, data corruption or deletion can result in deletion of the single source of "truth" for key business records. Best practice for a comprehensive information governance is to have an independent source of these records in a separate archive/data store.	Druva provides customers a secondary source of data should your relationship with the vendor deteriorate, or if their system somehow becomes unavailable.

inSync's Approach to File Sync & Share

- File sync and share is interactive—you select, copy, or move files and folders you choose to sync. **Backup is invisible and comprehensive.**
- With File Sync & Share, when files are synced across devices, all devices are impacted if a version is deleted or corrupted. **Backup is designed to create redundancy in case one version is lost, deleted, or corrupted.**
- File sync and share makes a subset of your files available to other devices or people. **Securely backs up all of your files and keeps them safe so you can access and restore files when needed.**

Microsoft OneDrive	Druva inSync
Lack of Automation: OneDrive stores only files that a user places in their "sync folder," requiring end-user training and severely limiting the scope of what data is captured. Files left open will not sync until closed, leaving data at risk. OneDrive's sync and share lacks automated deployment and reporting, requiring hands-on management by IT.	**Continuous Protection:** inSync provides continuous protection for all data (including .pst files); file exclusion optional, without user intervention, to ensure access and recoverability of existing files at all times.
File Size and Sync Limitations: OneDrive has a file size upload limit of 10GB per file, and restricts the amount of items that can be stored: 20,000 files for business library and 5,000 for the site library. OneDrive does not support large directories, and path size is limited to 250 characters, limiting usability.	**Unlimited:** inSync imposes no limits on either the largest file size or the maximum file counts and versions that can be backed up. Admins can configure inSync to enforce limits for their unique environments, but inSync inherently does not impose any of these limitations.
No Support for Locked Files: OneDrive does not backup files which are already open by other applications like Adobe PDF viewer, Outlook, etc.	**Support for Locked Files:** inSync uses Windows Volume Shadow Service (VSS) to backup open files. Linux and Mac actually don't enforce mandatory locks like Windows, enabling backup of such files.
Lack of Bandwidth Management: OneDrive's lack of deduplication and resource throttling (bandwidth and CPU) increases the risk of a poor end-user experience, particularly for users on WAN or networks of varying quality.	**Improved Network Performance:** inSync's WAN optimization, smart resource (bandwidth and CPU) throttling, and auto-resume ensure that backups and restores are non-disruptive and complete efficiently for end-users.
Limited Cross-Platform Support: OneDrive does not currently offer support for Linux operating systems.	**Cross-Platform Support:** inSync currently supports Windows, Mac, Linux operating systems. inSync strives to maintain functional parity between OSs where applicable and feasible (OS migration, email backup, exclusion policies).
Limited Data Archival & Compliance: In the event of a profile being deleted because a user leaves the company or otherwise, the administrator has only 30 days to access and download the data. Any documents that were owned by that user will be permanently deleted after that 30-day period.	**Complete Data Archival & Compliance:** inSync enables organizations to maintain a user's data indefinitely after they leave the company. Users are placed in a preserved state, freeing up licenses for new active users, while preventing the departing user data from being deleted.

Incomplete Legal Hold: Office 365 only offers in-place eDiscovery and legal hold capabilities for Exchange and OneDrive/SharePoint content, ignoring the information on end-users devices as well as other cloud services.	**Legal Hold and eDiscovery Across Endpoints and Cloud:** inSync supports legal hold and eDiscovery across all services being backed up (endpoints and cloud). inSync offers an in-place legal hold without requiring customers to restore or move data to a different storage repository. The inSync legal hold and eDiscovery enablement capabilities are developed natively and offer an out-of-the-box HTTPS connector for eDiscovery vendors (e.g., Recommind, AccessData, Guidance) to collect, analyze and process this data. The eDiscovery integration does not require a restore. The custom connectors can be used to access information from within the eDiscovery tools without any additional effort.
Privacy: OneDrive's encryption key model is a simple key stored in the cloud. This model does not ensure data privacy because Microsoft can be subpoenaed, court ordered, or have a warrant served for the data.	**Digital Envelope Encryption and Authentication:** Key management in inSync is modeled after a bank lockbox system, in which both parties hold part of the key. The encryption is based on the concept of digital envelope encryption. This mechanism of encryption results in the customer key never being stored or accessible from outside a user's active session. It also means that Druva cannot produce customer data under warrant, court order, or subpoena.
Support: Office 365 support is only available during business hours and has no stated response time commitments for high or non-critical events.	**Enterprise-class Support:** Druva's Customer Success team provides enterprise-class, 24/7/365 support.

Determining What Plan Makes Sense

Microsoft Office 365 is available in a variety of plans to best meet the needs of any organization, with services and pricing varying dramatically between plans.

Service Family: Enterprise		Office 365 E1	Office 365 E3	Office 365 E5
Target Customers	User/Monthly	$8.00	$20.00	$35.00
	User Max	Unlimited	Unlimited	Unlimited
Office Apps	Office Online	●	●	●
	Full, installed Office Applications		●	●
	Office on tablets and phones		●	●
Standard Service	Business class email, calendar, and contacts	◒ 50 GB inbox per user	● Unlimited inbox	● Unlimited inbox
	HD video conferencing	●	●	●
	Team sites	●	●	●
Advanced Services	Self-service Business Intelligence of Office 365 docs		●	●
	In-Place Hold and Litigation Hold of Office 365 docs		●	●
	Advanced eDiscovery with ability export Office 365 docs to third-party review apps			●
	Protect against unknown malware and viruses			●
	Analytics tools			●

Data Protection and Recovery With Office 365 E3 + inSync

Given the vast price differences between E1 and the E3 and E5, opting for a lower priced E3 plan subsidized with a third-party app for data governance and availability can make a lot of sense for companies looking for the right combination of data protection and governance at the right price point.

Key Features	Office 365 E1	Office 365 E3	Office 365 E5	Druva inSync + E3
Cost per user				
Licensing	$8	$20	$35	$35
Availability				
Backup and recovery of Office 365 documents	◒ Limited	◒ Limited	◒ Limited	●
Backup and recovery of files from third-party cloud apps				● Office 365, Box, Google Apps, Salesforce
System & application settings backup for device refresh				●
Data backup for smartphones & tablets				●
Data Governance				
Cloud-based archival of Office 365	● 50 GB mailbox	●	●	●
Federated search across all users in Office 365	●	●	●	●
Federated seach across all users, endpoints, and cloud applications				●
In-place litigation readiness & in-place legal hold across all users within Office 365		●	●	●
In-place litigation readiness & in-place legal hold across all users, endpoints, and cloud applications				●

Ability export data on legal hold to third-party review apps			◒ Office 365 docs only	●
Advanced eDiscovery			◒ Office 365 docs only	●
Proactive Compliance across endpoints and cloud applications				●
Continuously monitor for anomalies, to trigger ransomware alerts				●

To learn more about how to fill the critical gaps in your Office 365 service, visit druva.com/solutions/cloud-application-backup/ and experience the advantages for yourself.

About Druva

Druva is the global leader in Cloud Data Protection and Management, delivering the industry's first data management-as-a-service solution that aggregates data from endpoints, servers and cloud applications and leverages the public cloud to offer a single pane of glass to enable data protection, governance and intelligence—dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations, and protects over 100 petabytes of data. Learn more at www.druva.com and join the conversation at twitter.com/druvainc.

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44 (0) 203-7509440
India: +91 (0) 20 6726-3300
Japan: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729
sales@druva.com
www.druva.com