



COMPUTER



SECURITY



MOBILE



PROTECTION



SEARCH

HOW DRUVA CLOSES THE GAPS IN OFFICE 365 DATA PROTECTION



www.druva.com

“Some IT organizations wrongly assume that high-availability and disaster recovery capabilities offered by SaaS providers can recover data loss by users errors or malicious attacks.” —Gartner

When migrating to Microsoft Office 365, some organizations fail to guard against data protection gaps in the Software as a Service (SaaS) model.

The advantage of SaaS is that the providers take over responsibility for IT infrastructure and applications, which now reside in the cloud. However, as a SaaS customer you are still responsible for your data both in the cloud and on end user endpoints ranging from desktop PCs to notebooks, tablets and smartphones. While Microsoft does not have a history of losing Office 365 data, it does not provide comprehensive data protection with a repository for all your data regardless of its location. If you suffer a data loss due to human error or malware, or if you have legal or regulatory requirements for data retention, Microsoft and other SaaS providers may not be able to help you.



Fortunately, an increasing number of organizations are taking action to address the gaps in end-user data protection, data recovery, legal hold and eDiscovery, as well as third-party managing of Office 365 archival data. Organizations beginning the migration process to Office 365 would be wise to join them.

You need to have the same data protection with SaaS as you did when all your data was onsite behind your firewall on your servers. This includes offsite replication so you 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. You will also need to have access to all data both in the cloud and on endpoints in case a legal action requires you to produce emails and other documents. Also state, national and international as well as industry regulations may require you to follow set data retention policies. In all these cases, your SaaS provider is unlikely to be able to help you.

For example, documents deleted by an employee are likely to be purged from the Windows Recycle Bin after

approximately 90 days. Where will you find that document then if your legal team or a regulatory agency requests it? There's a saying in the data security business: "The Recycle Bin is not a backup and recovery application." Collaboration applications like SharePoint also are not built for data security.

Druva, a leader in cloud data protection and management, 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 give users a single pane of glass to monitor and protect data no matter where it resides.

THERE'S A SAYING IN THE DATA SECURITY BUSINESS: "THE RECYCLE BIN IS NOT A BACKUP AND RECOVERY APPLICATION."

So how are you going to manage the data in the cloud with the same due-diligence that you had for your data in the data center? What do you do if a user needs to retrieve their accidentally deleted files? How will you handle legal holds if there is litigation? Can you quickly recover from ransomware?

PROTECTION FROM ENDPOINTS TO CLOUD

For comprehensive data protection, you need a solution that will take all your data from end users endpoints to SaaS applications. That's where Druva can help. Druva helps organizations go to the cloud for the benefits of collaboration but still provides a way for IT to manage the data for which they are ultimately responsible. Organizations moving to the SaaS model need to ensure that their data is available and protected, so IT can meet their organization's compliance regulations and e-discovery obligations.

Druva is the essential layer of data protection functionality companies need to defensibly archive and discover business-critical information, making full use of Office 365 without sacrificing security or compliance across crucial areas of exposure.

BORN IN THE CLOUD

Founded in 2008, Druva was born in the cloud. The company has approximately 4,000 enterprise customers. It is one of Amazon's top five storage partners. In the end user data protection space, Druva has been rated number one by Gartner every year they have rated the space. The company focuses on helping very large organizations manage their data whether the data is in Office 365, desktops and laptops back in the office, or mobile devices in the field. Druva is helping IT regain control over that data.

Unlike on-premises or hosted backup and recovery systems that bottleneck uptime

and hamper cost efficiency, Druva was built from the ground up in the cloud to afford businesses scalable, secure, and unified data protection. Druva collects end user data throughout your enterprise: from remote offices, from mobile workers, and from applications everywhere in between. A highly optimized backup engine leveraging patented deduplication technology stores a single centralized, and highly durable copy of all your data. This allows you to meet your data protection, retention and archival needs without additional systems or copies of data. It provides IT departments with anytime, anywhere instant data access and recovery. It also gives IT pros a straightforward path to disaster recovery right from cloud-based backups.

PROTECT, PRESERVE AND DISCOVER

For the end-user, Druva's inSync product enhances productivity through self-restore capabilities and anywhere, anytime, any device access to their data.

**FOR THE END-USER,
INSYNC ENHANCES
PRODUCTIVITY THROUGH
SELF-RESTORE
CAPABILITIES AND
ANYWHERE, ANYTIME,
ANY DEVICE ACCESS TO
THEIR DATA.**

inSync provides IT departments with a single pane of glass for protecting, preserving and discovering information across endpoints and cloud applications—helping customers dramatically increase the availability and visibility of business-critical data while reducing costs, risk and complexity:

- **Endpoint Data Protection**
High performance backup, remote wipe and geo-location of laptops and smart devices
- **Cloud Application Backup and Archival**
Protection and governance for Microsoft Office 365, G Suite, Box and Salesforce
- **Data Compliance Monitoring**
Identification and remediation of at-rest sensitive data risks (PHI, PII, PCI)
- **Federated Search**
Quick location of files across endpoints and cloud applications
- **Legal Hold Management & eDiscovery Enablement**
Instantly preserve custodian data for investigative and litigation needs

BEYOND BACKUP AND RECOVERY

When it comes to governance, Druva's industry-leading information management capabilities elevate your ability to seamlessly address legal requests, search across the data landscape and provide deep analytics for compliance purposes, simplifying the overall process and reducing the need for maintaining multiple data silos. As a 100 percent cloud-native solution, Druva is transparent to your daily operations. There is no need

for additional hardware. Druva inSync requires no de-duplicate appliances and no additional software. Druva stores data far more efficiently than traditional methods, saving up to 76 percent in operating costs. True elastic performance means Druva effortlessly scales to the need and you pay only for what you use. Unified, simple, affordable: That's a higher vision of data protection and management.

Druva provides:

- **Tamper-Proof audit trails**
 - > Ensure a chronological view of data activities by users and administrators
 - > Identify and maintain a clear chain-of-custody of files
 - > Ability to download audit trails for offline analysis
- **Data Loss Prevention**
 - > Remote wipe corporate data
 - > Locate lost/stolen endpoint

Through policy enforcement, the IT admin can also mandate encryption on devices and set rules for auto deleting data when the endpoint does not connect within a set amount of time.

With Druva you can easily monitor and track lost or stolen endpoints, remotely wipe any sensitive information and enforce encryption to protect against any data leaks or breach.

For example, if an employee loses an iPad with corporate data on it, an IT admin can pinpoint the location of the missing iPad on Google maps, so the employee can go get it. But if the iPad

has fallen into the wrong hands, the admin can remotely wipe out the corporate data so it can't be used for nefarious purposes.

FOCUSING ON KEY OFFICE 365 COMPONENTS

Druva inSync focuses on three components of Office 365:

- Exchange Online
- OneDrive for Business
- SharePoint

It also can be used to back up data in Google, Box and Salesforce.com.

Covering endpoints, inSync gives IT visibility into data on end user devices in a consolidated form. In a scenario where you have some data off in the cloud, including AWS and Azure, some of it in Office 365 and some of it is with other vendors such as Box, inSync gathers all of that data together and then makes it available for different workflows.

For those components inSync does:

- Backup and restore
- Archival
- Search & Audit
- Compliance
- Legal Hold

INSYNC DOES NOT BURDEN YOUR NETWORK

inSync uses Microsoft native APIs to back up directly from the OneDrive cloud, for example, into Druva's cloud data repository. Users can choose whether that repository is in AWS or Azure.

THIS BACKUP SOLUTION MEANS YOU'VE GOT A SECONDARY COPY OF ALL YOUR DATA SOMEWHERE OTHER THAN ONEDRIVE.

Regardless, the data does not traverse your network. It goes from cloud to cloud. So there is no burden on your network.

This backup solution means you've got a secondary copy of all your data somewhere other than OneDrive. So if there's a ransomware attack or some other kind of malware that moves from a PC in your office to OneDrive in the cloud, your data is safely backed up in Druva's cloud repository. So if malware were to lock up the data in your OneDrive repository, which Microsoft is not going to be able to help you with, you've got a time-index snapshot of your data to roll back to. You can also archive data as long as you need to, so there is no need to go searching in Recycle Bin and hoping the document your legal team needs is still there. You can keep data based on your retention policies from any point in time and then roll back to it for a true snapshot not just file versions.

MEETING LEGAL AND REGULATORY REQUIREMENTS

Druva focuses on helping organizations by giving IT the ability to look at all their data whether it's in cloud applications or any endpoint devices. All of that user data regardless of data source is organized by user and resides in the scalable and secure Druva data repository. It can then be made available to IT for use cases

including backup and recovery, e-discovery and compliance. IT can also search across all that data as opposed to having to search an Outlook mailbox or OneDrive or SharePoint.

Beyond backup and recovery, inSync gives you the ability to handle legal requests. Organizations are dealing with an estimated 250 percent increase in the number of regulations that require compliance. Lawsuits often require discovery of email content. How are you going to be able to provide that content from OneDrive? But if you've got that data backed up in Druva's cloud repository, you've got a single view into all of that data. That gives you the ability to go in and put legal holds in place. You can specify the users and specify the period of time. All of that data is now held. It doesn't matter if a user goes in and deletes something on their end. Data is still held permanently in the inSync repository. This allows you to have more of a proactive response and you are not at risk because of user behavior.

THE WORKFORCE SOFTWARE USER STORY

“Druva's ability to work with various cloud services and the expected growth of those services was enticing ... we didn't really have a way to do that.”

— Workforce Software

“DRUVA'S ABILITY TO WORK WITH VARIOUS CLOUD SERVICES AND THE EXPECTED GROWTH OF THOSE SERVICES WAS ENTICING ... WE DIDN'T REALLY HAVE A WAY TO DO THAT.” –WORKFORCE SOFTWARE

Workforce Software is a Michigan-based technology company that provides software for human resources including contracting and resource management. They were moving to Office 365 for their users' endpoints. They were aware that they still needed full control of their data in Office 365. But they didn't want to enter yet another solution in their IT portfolio.

They came to Druva looking for that single way of looking at all their data regardless of where it resided. They also needed the ability to manage that data for backup and recovery. An additional

issue was that they had some executives who were using Google Gmail for their email. With Druva they could cover Gmail as well as Outlook and OneDrive and all their endpoints.

Druva helped them create a single repository for all their data and allowed IT to do all of their management from that single location.

Find out more

www.druva.com

