



 Tip Sheet

# THE TOP 6 MYTHS ABOUT SaaS APPS AND DATA RECOVERY

## Unforeseen Risks

Cloud-based applications have become critical to businesses and operations around the globe. But do leading SaaS solutions such as Office 365, Box, G Suite, and Salesforce protect their customer's data with equally critical backup options? Here are the top six myths about SaaS apps that might lead you to believe your company's cloud data is secure—when in fact it is at serious risk of being permanently lost without a third-party data protection solution.

*IT organizations wrongly assume that capabilities offered by SaaS providers can recover data loss by user errors or malicious attacks.*

*Gartner - Data Backup/Recovery Factors to Consider When Adopting SaaS*



### 1. Myth: You Can Always Recover Your Cloud Data

Cloud providers do indeed offer different levels of recovery, but there's a 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 providers that do have backup capabilities may charge customers a sizeable fee for retrieval. With 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.



### 2. Myth: File Sharing is the Same As Data Protection

Many companies have said “we already have cloud file sharing, can't you just store your files there and call it a day?” Here's the uncomfortable truth: File sharing is NOT data protection. While the two technologies do have some overlapping features, they are fundamentally different in their approach:

- File sync and 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.
- Unlike file sharing, enterprise backup software automatically makes a copy of every user's data available for recovery. Data is protected in its entirety, including files stored by SaaS applications, and if a device is lost or stolen, additional features help organizations trace the device and/or remotely delete corporate data.



### 3. Myth: Your People Don't Make Mistakes

Let's face it: even the smartest people at your company are only human; mistakes can (and will) happen. It is not uncommon for data to be deleted by an employee, only for that same person or others in the organization to realize later that it is still needed. A collaborator might accidentally delete a shared project, or you might remove a scrapped project only to discover afterwards it is starting up again. If you don't identify the issue within a very short period of time (anywhere from 30 days to as little as two hours), your critical data may be lost for good.



### 4. Myth: You Can Stop Malicious Employees Before They Do Damage

Why is it standard practice for your HR department to escort terminated employees from the building? Because angry people often react in destructive ways. Disgruntled employees may delete data before they quit a job, if they suspect they are going to be fired, or simply to spite a boss or coworker they are angry at. All it takes is one press of a delete key to potentially erase weeks, months, or even years worth of valuable data. And the danger isn't just confined to the insides of your office: hackers are circumventing even the most robust security systems to delete, corrupt, or lock up your data with ransomware. Whether internal or external, untrustworthy people are a reality.



### 5. Myth: Ransomware Isn't That Big a Deal

Downtime from ransomware costs small businesses around \$8,500 an hour—in the U.S., this adds up to a loss of \$75B+ per year. Today, ransomware is not only commonplace, but it's on the rise. Many organizations fail to understand that the cloud is just an extension of a user's operating environment—data is just as susceptible to loss, theft, or malicious attack in the cloud as it is anywhere else. Enterprises are still responsible for managing sensitive, cloud-based data, and failure to comply with rules and regulations can result in hefty fines and, worse yet, loss of reputation.



### 6. Myth: A Legal Hold Just Means "Don't Delete Anything"

Businesses risk very serious consequences if they fail to produce SaaS data during litigation following a discovery request made by the courts.

In many cases, this data—residing in cloud services like Office 365 or Box—may not be recoverable or is susceptible to deletion or mishandling by the users. By ignoring the data retention gaps within these products, you are relinquishing control of your organization’s business-critical information and putting it entirely in the hands of the end users. This places the burden of compliance solely on the shoulders of those who may have no understanding of how to manage company data correctly.

*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*

## Summary

While the rapid adoption of SaaS-based applications has been fueled by the unique advantages of the cloud, the core capabilities of Office 365, G Suite, Box, and Salesforce are not necessarily built to be comprehensive solutions for companies’ data availability and governance needs. In fact, they do little to address concerns around backup and archival of critical data. This is why it is imperative that businesses supplement the native capabilities of these applications with third-party backup tools to establish a strong data protection solution in the cloud.

## 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 40 petabytes of data. Learn more at [www.druva.com](http://www.druva.com) and join the conversation at [twitter.com/druvainc](https://twitter.com/druvainc).



### **Druva, Inc.**

Americas: +1 888-248-4976  
Europe: +44 (0) 203-7509440  
APJ: +919886120215  
[sales@druva.com](mailto:sales@druva.com)  
[www.druva.com](http://www.druva.com)