eBook

Why SaaS isn't Backup

Yes, You need to backup your cloud data

Introduction

One of the most business–friendly innovations in recent years has been the proliferation of cloud apps like Google Apps, Office 365, and Salesforce. These SaaS apps have fundamentally changed the way we do business, enabling companies to take advantage of economies of scale, reduce infrastructure costs, and expand the boundaries of a cubicle.

Storing data in cloud applications is far safer than storing data on most on-premise storage systems — but "safe" does not equal "invulnerable." **In fact, one third of SaaS users report losing data in the cloud.** Yes, the cloud is safe, but it's not infallible and today's cloud vendors lack the incentive to point out their vulnerabilities. So we're stepping in!

In this eBook, we compare three of the world's premier SaaS applications (Google Apps, Office 365, Salesforce) to highlight how they are (and aren't) protecting your data. Get the facts straight and start backing up before it's too late.

The single leading (and unpreventable) cause of data loss in the cloud is end user error.

1. How is data being protected

Google Apps

Google offers infrastructure high availability (HA) with erasure code and multiple replicas in multiple geographies, so data will still be accessible in incidents of hardware failure. Google does not offer native backup capabilities for Google Groups or Sites data.

Office 365

The infrastructure of O365 is not unified, which means the backup capabilities for the components differ depending on the application. Backup measures include: local flash copies, encrypted, offline remote backup, and near real-time replication to a data center.

Salesforce

Customer data is automatically backed up to a tape library on a nightly basis. Backup tapes are cloned to an offsite facility to verify their integrity. Clones are stored in a secure, fire-resistant location at the same offsite facility.

Takeaways

The cloud, when left alone, is very safe. Google, Microsoft and Salesforce do a great job of ensuring the data is protected. And yet, data loss happens every day. So who's at fault? The single leading (and unpreventable) cause of data loss in the cloud is end user error. This will always be an achilles heel of the cloud until software can discern between an intentional and unintentional command. Other common culprits? Intentional deletion by disgruntled employee, hackers and external app errors (data corruption via syncing/over-writing).

Businesses can safely and securely restore any historical data without relying on the service provider.

When data loss occurs, it's likely not the fault of Google, Microsoft, or Salesforce. With a cloud-to-cloud backup solution, businesses own the data from the moment a backup begins without limits around point-in-time.

2. How Data is recovered

Google Apps:

Once admin or end user deletes any data, the files stay in the Trash folder for 30 days, after which point the data is deleted permanently and only recoverable by an admin. Data is irretrievable once an admin deletes a user account.

Office 365

Microsoft backs up data daily multiple times. End users may recover deleted files from the Recycle folder. Admins can restore data, such as collections, as well as deleted users.

Salesforce

Salesforce support can recover customer data at a specific point in time, in the case that it has been permanently deleted or corrupted. The price for this service is a minimum of $10K and it could take weeks.

Takeaways

If data is lost due to human error, malicious attacks, or other reasons, there are some options to restore said data, but they mainly involve relying on Google, Microsoft, and Salesforce, not to mention, potentially paying thousands of dollars. It could take a while, which isn't helpful when the data is critical to day-to-day business operations. Also, mirror image replications means ransomware, such as CryptoLocker, can potentially access replicated Google data, which is not something anyone wants to recover.

Recovering data through the native apps is limiting – not only in how far back you can restore data from, but in what you have control over.

With a cloud-to-cloud backup solution, cloud data is available whenever it's needed. Businesses can safely and securely restore any historical data without relying on the service provider. It means users can restore any lost or corrupted data while maintaining the integrity. So if malware strikes a system, users can restore data from a point-in-time before the data was hacked without compromise.

3. Recovery limitations

Google Apps:

Any data deleted from Trash folder requires admin assistance to recover, but only for 25 days. All or nothing restore - cannot select specific files.

Office 365

Data deleted from the Recycle folder goes to the Recoverable items folder for 14 days (30 days if reconfigured), and requires admin assistance to recover.

Salesforce

Only 3 months of data recoverable. Deleted data goes to the Recycle Bin and is queried in an “isDeleted” API. Data deleted beyond this requires SFDC assistance. Any recoverable data must be manually imported back into Salesforce.

Takeaways

Recovering data through the native apps is limiting – not only in how far back you can restore data from, but in what you have control over. It may also be a long, tedious process with a lot of manual workloads.

Recovering data can take anywhere from minutes to weeks to longer (if at all).

With a cloud-to-cloud backup solution, businesses are no longer limited to just a few weeks or months of data. With Datto SaaS Protection, for example, companies backup all data without having to delete previous versions. So whether the data is from last week, last month, or last year, it can easily be recovered.

4. Recovery Time

Google Apps:

Up to 1 hour.

Office 365

Minutes.

Salesforce

A 15 business day minimum.

Takeaways

The time it takes to recover data from the cloud varies app to app. For Google Apps, O365 and Salesforce, it can take anywhere from minutes to weeks to longer (if at all).

With a cloud-to-cloud backup solution like Datto SaaS Protection, the data is restored directly into the app in minutes without overwriting any previous versions, making it easily identifiable as a restored item.

Conclusion

While cloud applications are more resistant to data loss than conventional, on-premise solutions, they are far from immune to irreparable loss of data. Today's companies back up their on-prem data to ensure they don't have a single point of failure for their irreplaceable information. This doesn't stop being a great idea just because the data is now in the cloud. If you're leveraging SaaS applications, make sure you are treating the data just as you do your on-prem data: by backing up. It's a standard practice that needs to be implemented wherever your business data lives. After all, the more you do business in the cloud, the more you have to lose.

For more information please contact:

John Schick
Phone: 647.956.6081
Email: john@1computerservices.com