eFolder White Paper: How to Choose the Best Cloud Backup Service

February 2015

Introduction

This paper is a resource for IT professionals working in corporations that use a number of cloud services, including Office 365, Google Apps, Salesforce, and Box. Over the past several years, productivity has moved to the cloud, enabling users to get more work done on different devices and in different locations. For all cloud-based services, data is stored off-premises and is not included in the backup protocols your company has established for on-premises data.

Many IT managers falsely believe that since cloud providers' infrastructure is designed to ensure service continuity and safeguard data from hardware failure, a backup strategy for the cloud is not necessary. However, no cloud provider can prevent errors that originate on the user's end. That is why nearly every Software-as-a-Service (SaaS) provider recommends using a third party backup solution.

This paper will help users of Office 365, Google Apps, Salesforce, and Box determine if third party cloud backup services makes sense for their organizations and, if so, how to differentiate between the various vendors providing this type of service. The paper begins with a brief survey of research focused on the risk of data loss in the cloud and its impact on an organization. This is followed by a discussion of third party backup options available to mitigate the risk of data loss. Focusing on cloud-based SaaS solutions, this paper provides a checklist of relevant questions to ask in order to help differentiate between the top providers of third party cloud backup solutions. The objective is to help readers determine the best fit for their individual organizations.

1. How common is data loss in cloud-based services?

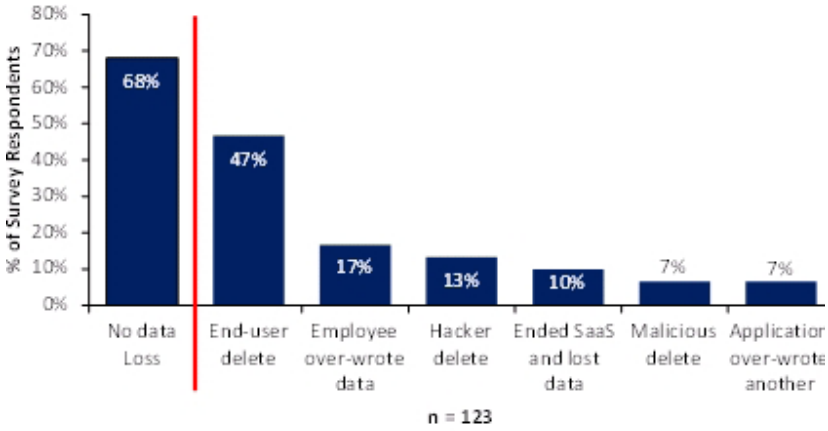
Data loss on cloud platforms is more common than you might think. A January 2013 SaaS report from the Aberdeen Group provided a clear picture of data loss in the cloud. The survey showed that 32% of the companies that are using SaaS services have reported losing data.

Top 5 ways data is lost in the cloud

1. User Error - 64%
   Registered users who accidentally delete or overwrite data.
2. Hackers - 13%
   Outsiders who get into the system with nefarious intent.
3. Closing account - 10%
   Registered user or provider who closes an account without regard for the data left behind.
4. Malicious Delete - 7%
   A registered user who purposely deletes data.
5. Third Party Software - 7%
   Unintentional data overwrite by third party software on the user's system.

Reasons for SaaS Data Loss

Source: Aberdeen Group January 2013

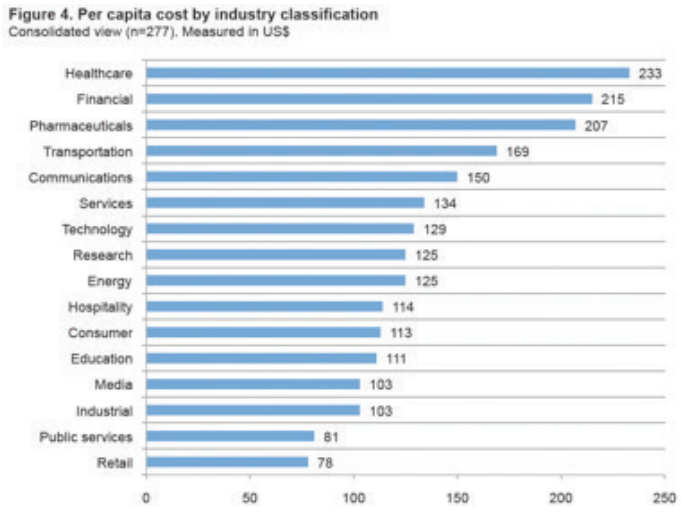


However, this is less of a reflection on the platforms than it is on the people using them. Mature cloud platforms rarely lose customer data. In almost every case, data loss in the cloud is the result of external forces. In the Aberdeen study, user error accounted for 64% of data loss. This is consistent with the findings of a study done by the IT Policy Compliance Group that showed human error, in one form or another, accounts for 75% of all data loss, whether cloud-based or on-premises.

According to the Aberdeen Group's report, hackers, along with malicious, purposeful deletion of data, were responsible for 20% of data loss. Software compatibility and corruption issues accounted for the remaining 17% of data loss.

The point here is that data loss in cloud-based services is a real threat. In almost every case, data loss is not the result of hardware failure on the SaaS provider's end, but is caused by simple errors by your own well-intentioned users. Even your most experienced users are not immune; Apple's co-founder, Steve Wozniak, posted on Gizmodo to explain how a third party app accidentally overwrote his Google Calendar during a routine system update. In order to protect your data, you need to understand how data can be lost on cloud-based platforms and the degree of these threats.

2. What impact does lost data have on an organization?



Corrupt, missing, or deleted data is disruptive to a company on many levels, not the least of which is financial. A 2013 report from the Ponemon Institute, 2013 Cost of Data Breach Study: Global Analysis, showed that the consequences of data loss can be financially significant. A report citing this survey from IT World stated:

"Data losses cost companies big. In fact, on average, it costs $136 for every record lost. And that financial disincentive is what spurs many of them to be better stewards of our data (or at least try harder)."

The cost can even be higher depending on your industry. The Ponemon study found that the cost of data loss could be as high as $233 per record lost for a healthcare company, compared to $111 for an educational institution. The average cost of data loss can also vary by geography, with the US and Germany in the top spots for absorbing the greatest financial impact for lost data.

Data loss can seriously disrupt business. As an IT professional, you know how disruptive data loss can be to an organization. Quantifying the cost of that disruption helps clarify the importance of protecting cloud data. The more reliant an organization is on cloud-based services, the more relevant this point becomes.

3. What are the options for reducing the risk of data loss?

Cloud-to-Cloud Backup Basics

All the leading cloud-to-cloud backup services are characterized by these main backup features:

- Automation - Backups occur automatically on a predetermined schedule.
- Frequency - Backups are run at least every 24 hours.
- Security - Server Side Encryption (SSE) and 256-bit Advanced Encryption Standard (AES-256)
- Reliability - Durability and availability of service ratings in excess of 99%.
- SaaS - Requiring no purchase or maintenance of software.
- Pricing - A free trial period with monthly fees charged per user account thereafter.
- Autonomy - Service works independent of source application.
- SLA - Reasonable service level agreements ensuring high level of functionality and uptime.

One of the challenges companies face with cloud computing is the decentralization of their business data. IT professionals, who once controlled data management from their on-premises servers, now experience a sense of "data scatter." In this new scenario, the responsibility of managing and safeguarding the organization's data still falls on the IT department; however, much of that data is now beyond their control, spread across several cloud servers. This new, decentralized data landscape is one of the main reasons why fresh thinking is required to mitigate the risk of data loss.

First and foremost, regular backup of your cloud data is essential. A prevalent misconception among cloud users is that cloud services back up their users' data as a general rule. In fact, 33% of respondents in one study believe the cloud service provider is responsible for backing up their company's data. Unfortunately, this is not often the case. While some services does provide limited backup coverage, most cloud-based services are primarily focused on business continuity, not on data backup. They want to ensure that their service is available to users, so they create secure, redundant systems. That's why most SaaS providers recommend the use of a third party backup provider.

There are several different options for safeguarding your data in the cloud. These range from creating your own custom application to back up data from your SaaS providers Application Programming Interface (API) to mirroring your cloud data in real time on your own servers to manually extracting the data yourself on a regular basis.

The backup approach recommended by many SaaS providers is a fully automated cloud-to-cloud backup. This paper will focus on this category of backup. As the number of companies using cloud-based services to store critical data has grown in recent years, so has the popularity of cloud-to-cloud backup services as a first line of defense against data loss.

The popularity of cloud-to-cloud backup is driven by many of the same factors that made organizations turn to the cloud in the first place. Compared to purchasing a software program or developing your own custom application, cloud-to-cloud backup offers several advantages:

- The upfront cost is zero.
- You can test drive the product before investing any money.
- Implementation can be done in a matter of days compared to months.
- The costs and hassle of developing software or managing software licenses, maintenance, and hardware compatibility are eliminated.
- Upgrading to new software releases is effortless.
- Data can be accessed and managed from virtually anywhere.
- SaaS offers ease of scalability to growing organizations.
- There is always an entire team of developers and specialized IT professionals working every day with a single-minded focus – making that one application the best it can be.

Once an organization has decided that a SaaS backup solution is right for them, the next challenge is to decide which one is the best fit.

4. How can I assess the differences between various cloud-to-cloud backup services?

If you take a look at the top three cloud-to-cloud backup solutions, you'll find they share many common features. All provide reliable automated backup with robust data security and a free trial period. Furthermore, all have similar pricing plans and terms of use.

However, beyond that, the services can vary considerably in terms of ease of use, data management features, and the product vision that guides development moving forward. These differences can be quite difficult to spot and time-consuming to assess. For that reason we have included a concise list of questions (below) to help you differentiate between offers as well as determine which may best suit your organization's needs.

Before committing to an online backup service for your data, it is recommended you take advantage of that service's free trial period. During that period, be sure to compare services in terms of these core features of cloud-based backup service:

- Adding/deleting accounts
- Scheduling backups
- Performing unscheduled, manual backups
- Customizing error notifications
- Searching backed-up data
- Restoring data
- Data overview
- Reporting
- Support

These are the nine areas where you are likely to find the most variability from service to service. Beyond these functional comparisons, explore the following areas in more depth to ensure a cloud-to-cloud backup provider is best suited for your organization today and well into the future. These topics have been separated into service-related issues and service provider-related issues.

Assessing the service

How often can data be backed up?
Services vary in terms of how often they back up your data before extra charges are incurred. These additional charges are often the result of exceeding the API call limits set by each SaaS provider.

How easy is it to search backed-up data?
Each service takes a slightly different approach to search. The result is that the providers have different search interfaces which can affect both the ease and speed of the search.

How easy is it to restore backed-up data?
When data is lost, you need to be able to perform a restore swiftly and easily. Will the data be restored exactly as it was before the loss or will formatting be lost in the process? How much control do you have over what is restored? For example, can you specify between individual records or entire user accounts?

What type of data overview is provided?
There is an added benefit to cloud backup: it provides IT managers with the opportunity to analyze the backed-up data. Check to see what type of data overview tools the service provides and how easy they are to use.

How is the backup protected from user error?
We know that the biggest cause of lost data in the cloud is due to user error or malicious activity. Logically, this would also apply to your backup service. Is it possible for a user to delete backed-up data through the online interface?

Assessing the provider

How future-proof is your cloud-to-cloud backup solution?

When these services were initially offered, the only concern was the reliability of the basic backup functionality and the security of the data. As the category has matured and the challenges of reliability and security have been addressed, many users are seeking more refined and future-proof features from their online backup. Specifically, business users are concerned with the ability of a backup service to handle multiple data sources (e.g. Salesforce, Google Apps, Office 365, Box, on-premises data, etc.) and how well it allows them to manage this data once it is aggregated in a central backup. There is a clear trend today for companies to adopt cloud-based software solutions. As companies find more and more of their important data stored with various cloud services, the centralized management of that data is likely to be of increasing importance.

Does the provider specialize in serving the needs of businesses?
The needs of individual users and small companies can vary considerably from those of the enterprise. Is the service designed for individuals and small businesses? Does it focus exclusively on the needs of medium to large organizations? Is it a generalist that serves all types of users? Obviously, the best choice is a service that specializes in your organization's specific needs. Make sure that the service you select focuses on organizations of your size.

Can on-premises data be backed up as well?
It's difficult to manage data that is housed on different servers. For that reason, some providers will also back up on-premises data as well as your organization's data. Having specific types of data in one place can make search, information overview, and reporting tasks a lot easier. This will be of increasing relevance as organizations rely more on cloud-based services.

Does this provider back up other cloud-based services?
A recent study by Forbes Magazine concluded that the uptake of cloud computing will increase by 36% over the next three years. If your company uses, say, Box today, there is a good chance you are either using additional cloud-based services or will do so in the near future. Using one vendor to backup multiple cloud services makes sense. But only if the vendor you choose provides one interface with seamless, integrated search, oversight, and reporting across these different cloud services. So look for a cloud-to-cloud backup provider that, at least, plans to cover multiple cloud services and check how seamless their search, overview, and reporting functions are cross-platform.

What is the provider's development plan for the platform?
Cloud-to-cloud backup is a relatively new category, so you can expect the various offers to be evolving at a steady clip over the next few years. The beauty of SaaS is that upgrades are automatic, so the product keeps improving. At least that's true in theory. Make sure your provider's plans for the platform are in line with your projected needs. Will it be able to back up multiple cloud services? Can it incorporate on-premises data? Will the basic functionality work as well across platforms as it does for one platform? How future-proof is the solution?

5. Summary

Cloud platforms are becoming increasingly integrated into the day-to-day operations of many organizations. This is a trend that will likely increase over the next five years. This paper has specified the ways in which cloud-based data is vulnerable despite the reliability of the platform. Most of the risk to the data comes from user error, which, in many cases, is difficult to prevent. The cost to organizations that experience data loss varies depending on geography and industry, but in all cases it is significant.

As with any technological advancement, the cloud requires measures to be in place to ensure that important data remains safe, secure, and reliable. Eliminating user error and other causes of data loss is unlikely. However, it is possible for IT managers to minimize the cost and disruption of data loss to an organization by utilizing a cloud-to-cloud backup service.

SaaS is rapidly growing in popularity as the backup method of choice for cloud-based platforms. While the leading providers of these services offer very similar basic features and pricing, significant differences exist between them. These differences can affect how well the service will perform for a particular business. For that reason, these differences should be explored before committing to any one service.

Ultimately, the best cloud-to-cloud backup service for an organization will be the one that best suits its needs today and can develop in line with its future requirements. This document has outlined several of the variables that can distinguish one provider from the others. These differences are included in an assessment worksheet. Using these tools can save time and will increase the likelihood of selecting the service best suited for your particular organization's needs.

About eFolder Cloudfinder

eFolder Cloudfinder provides secure, reliable, and integrated backup and data management for Google Apps, Salesforce, Office 365, and Box. eFolder's mission with Cloudfinder is to combine absolute data security across all cloud platforms with the market's most intuitive information overview, search, and retrieval capabilities. Cloudfinder has been adopted by major companies, including game studio Rovio, advertising agency DDB, and convenience store chain 7-11.

Evaluation Worksheet

Company A:

Company B:

Company C:

Rank each option on a scale of 1-5 with one being poor or least favorable and 5 being excellent or most favorable. Additional spaces are provided to add your own criteria.

Criteria	Company A	Company B	Company C
Ease of adding accounts			
Ease of deleting accounts			
Ease of scheduling backups			
Frequency of scheduled backups			
Ease of performing unscheduled, manual backups			
Flexibility for customizing error notifications			
Ease of searching backed-up data			
Range of search criteria			
Speed of searching backed-up data			
Ease of data restore			
Speed of data restore			
Protection from deletion of backup data due to user error or malice			
Data overview capabilities			
Reporting capabilities			
Customer support experience			
Can back up multiple cloud-based platforms			
Can back up on-premises data			
Ease of cross-platform search, data overview and reporting			
Specialized in addressing organizations of your size			
Future-proof qualities of the solution in line with your projected needs			
TOTAL:			

Corporate Headquarters
2340 Perimeter Park Drive, Suite 100, Atlanta, GA 30341 ▪ 678-888-0700 ▪ www.efolder.net