

THE BUSINESS CASE FOR **Cloud-to-Cloud Backup**

An illustration on the left side of the page shows a blue cloud at the bottom left with several grey document icons flying upwards and to the right towards another blue cloud at the top right. The background of the entire page is a light blue with a fine, diagonal hatched pattern.

Introduction

As we move into the information era, data becomes a foundational element of business. Data is collected, stored, and analyzed allowing businesses to gain a new depth of insight into their customers and their habits with an endless amount of possibilities to grow their business in a smarter, more agile way. This data needs to be available around the clock to ensure the operational success of the business.

Data that once lived in basements and backrooms is being moved to cloud-based servers and SaaS applications. Historically, data backup has always been a key component of any IT strategy – whether it was stored on floppy disks, duplicate servers, or in custom built applications. With this shift to the cloud, backup shouldn't be taken out of the strategy; rather, it should be re-thought to be more adaptable and cost-effective – the same reason you moved to the cloud in the first place. ▶

But isn't the Cloud Already Backed Up?

There is a common misconception that the cloud is backed up. However, while Amazon, Google, and Salesforce all have disaster recovery plans for the data they store on their servers, but is that the only way you think you'll be affected by data loss? It's more likely that an employee is going to delete something they end up needing two weeks later than the possibility of all of Google's servers being destroyed by a tornado. Google and Salesforce both have limited functionality when it comes to getting your data back if it is lost for reasons other than hardware failure or disasters. In fact, Salesforce has a high cost associated with recovering your data and it can take up to 15 days. These applications usually aren't the responsible party for your data loss, but they aren't built to protect you against accidental or malicious actions either.

The Cloud Security Alliance listed data loss as #2 in the Top 9 Cloud Security Threats in 2013, up from #5 in 2010.

How Can I Lose Data?

Data loss has serious implications for businesses affected. The Cloud Security Alliance listed the [Top 9 Cloud Security Threats](#) in 2013 and rated Loss of Data as the #2 most severe threat, up from #5 in 2010. For businesses that sustain data loss, statistics show that 60% of those companies will be out of business within 6 months of the disaster.

Accidental Deletion and User Mistakes.

More often than not, data is deleted then later realized that it is actually still needed. A collaborator might accidentally delete a shared project, or you might delete a scrapped project and then later learn it is starting up again. Information can also unknowingly be overwritten or corrupted by users and third party apps.

Over-Writing Data

SaaS applications hold large amounts of data that are constantly added to and 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 base SaaS application.

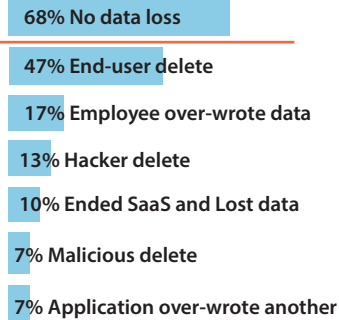
Malicious Actions.

People often delete data before they quit, if they suspect they are going to be fired, or to spite a boss or coworker they are angry at. Hackers can also be the culprit, surpassing security systems to delete or corrupt data. Whether internal or external, untrustworthy people are a reality. ▶

More than one in every three companies lose data in the cloud.

Reasons for SaaS Data Loss

% of Survey Respondents



n=123 Source: Aberdeen Group January 2013

All of these measures help to minimize the instances when data is lost, however, none replace your data once it's gone.

How Common is Data Loss?

In their report entitled “SaaS Data Loss: The Problem You Didn’t Know You Had,” the Aberdeen Group sites that 32% of companies surveyed lost data from in a SaaS application. That means more than one in every three companies lose data in the cloud.

Within their report, Aberdeen breaks data loss into how frequently each type of instance it occurs, with the most common instance being end-user deletion 47% of the time. The second most frequent is the overwriting of data (17%) followed by hackers deleting information (13%).

How Do I Prevent Data Loss from Causing Business Disruption?

At Backupify, we suggest a layered approach to protecting your company’s data, which involves all or a combination of the following measures:

- Good Data Management Processes
- SaaS Application Training
- Robust Password Policies
- Automated Backup with Easy Recover and Restore

Good data management processes means putting procedures, policies and checklists in place specific to SaaS applications. They could be focused on instances such as times of high-volume data or when users come and go. Users should be thoroughly trained in order to understand the purpose of the application and the role the data plays in the success of the organization. Passwords should always be robust and changed frequently.

All of these measures help to minimize the instances when data is lost, however, none replace your data once it’s gone. That is why having an automated daily backup like Backupify that you can “set and forget” is critical to your cloud strategy. This makes your information readily available when you need it, including an instance of user error and deletion, allowing you to easily restore data with minimal business interruption.

About Backupify

Backupify is the leading provider of backup and recovery solutions for Software as a Service (SaaS) applications, offering an all-in-one archiving, search and restore solution for the most popular online services including Salesforce, Google Apps, Facebook, Twitter and more. Backupify ensures that companies can access and control the data they entrust to these systems and prevents data loss from external threats, user error or service failure. Backupify was founded in 2008 and is based in Cambridge, Massachusetts. For more information, please visit www.backupify.com or follow @Backupify on Twitter. ■