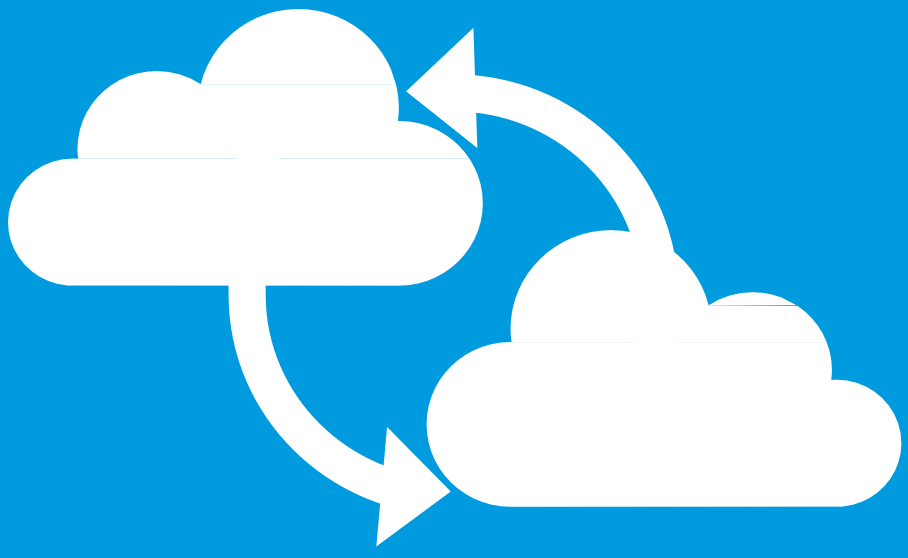
MAKING THE CASE FOR CLOUD-TO-CLOUD BACKUP



EZ WORKNET
"Your Technology Source"

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.

EZ WORKNET

"Your Technology Source"

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, 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. In other words, if the data loss is your fault, you're out of luck in most cases unless you have your own backup solution.

How Can I Lose Data?

Data loss has serious implications for businesses affected. The Cloud Security Alliance listed the Top 9 Cloud Security Threats 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.

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.

Accidental Deletion and User Mistakes

More often than not, data is deleted only for the user or organization to later realize 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.

How Common is Data Loss?

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

In a similar report by Forrester titled, “Back Up Your Critical Cloud Data Before It’s Too Late” it was stated that companies were steadily increasing their use of SaaS applications. According to Rachel Dines, the analyst who wrote the report: “As more critical data is deployed in the cloud, it’s time for I&O leaders to be proactive and invest in mitigating these risks instead of waiting for data loss to occur.”

If there is one thing that the above statements have in common, it’s that the use of SaaS applications is growing but data loss within those apps is also increasing at a steady pace. Companies are investing more and more of their data in SaaS applications, and protecting those investments should be a priority.

“We live in the era of ‘now’: Your customers expect data and services - both on-premises and in the cloud - to be available immediately whenever and wherever they require them. Waiting for days or weeks for the recovery of lost data or being informed that data is unrecoverable is unacceptable for most end users,” said Dines.

The use of SaaS applications is growing but data loss within those apps is also increasing at a steady pace.

How Do I Prevent Data Loss from Causing Business Disruption?

At **EZworknet,** 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 join and leave a company. 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 solution can help businesses “set it and forget it” - and having some type of backup should be critical to your overall cloud strategy. The result is that your information is readily available when you need it, including in an instance of user error and deletion, allowing you to easily restore data with minimal business interruption.

www.ezworknet.com