eFolder White Paper: Top 5 Sources of Cloud Data Loss and Prevention

June 2015

Introduction

Businesses are rapidly adopting SaaS applications. According to the Aberdeen Group, 80% of businesses reported at least one SaaS application in their organization. Beyond adoption, usage has also increased: 2014 was the first year in which the majority of workloads took place in the cloud, versus a traditional on-premises space, 51% to 49%, according to Silicon Angle. And there is solid business logic for doing so; moving to the cloud has increased productivity, enabled mobility, and promoted collaboration.

One major issue that moving to the cloud has not eliminated for organizations is the reality of data loss. While SaaS applications such as Salesforce, Office 365, Google Apps, and Box are inherently secure and resilient, the biggest threat is not hardware or software malfunctioning – the biggest threat is the result of human intervention. As an indicator, 32% of companies in 2013 using cloud services reported losing data. This data loss reality is especially pertinent when we consider that more than 50% of organizations are transferring sensitive or confidential data to the cloud.[1]

This white paper serves to educate IT administrators and business owners on the top five sources of cloud data loss. In addition, this white paper surveys different backup methodologies and makes an assessment as to which is most appropriate for a business environment.

Top 5 Sources of Cloud Data Loss

1. User Error

Accounting for a whopping 64%, user error checks in as the primary source of cloud data loss. Examples of user error include accidentally overwriting data or deleting files. Accidental deletion accounts for 47% of all lost cloud data, which goes to show that even the most earnest of humans are prone to making mistakes. Accidents are inevitable at any company, but it is critical for businesses to clean them up before they interrupt business continuity and productivity.

2. Hackers

At 13%, the second largest source of data loss comes from hackers, outsiders who get into the system with nefarious intent. Hackers are increasingly willing to attack companies of any size, not just mega corporations such as Sony, Target, or Home Depot. In fact, now 50% of data breaches occur at companies with fewer than 1,000 employees. Common types of hacker attacks consist of the hacker breaking into an organization's database or acquiring administrator and user credentials. Often, this type of activity results in sensitive data being compromised, jeopardizing both the business and its customers.[2]

3. Closing Account

10% of cloud data loss is the result of closed accounts. This type of data loss is the result of a registered user or provider who closes an account without regard for the data left behind. A common example of this kind of data loss is an organization that switches their CRM application from one platform to another without a comprehensive transition of data. According to the 2011 Pacific Crest "Private SaaS Company Survey," the average churn rate for a SaaS application is 5%. When organizations make these software switches, cloud data is lost, costing the business time and money.

4. Malicious Delete

"Jim would never do that" – unfortunately, Jim would. Malicious deletions account for 7% of lost cloud data. Malicious deletion happens when a registered user purposely deletes data. This type of activity may be initiated by a disgruntled employee or a recently terminated employee who still has access to cloud applications and data. At all levels, there are examples of employees not valuing company data nearly as much as the IT department or executives do, especially when these employees view their job as a stop-gap or temporary. Consider that the average turnover rate for a B2B sales representatives is 13.9%, and those individuals are responsible for working with potentially important leads and accounts. Malicious deletion is a difficult and dangerous form of data loss to control because the culprit is a member of the organization and knows where the most vital data resides.

5. Third-Party Software

Finally, third-party software comes in fifth, responsible for 7% of cloud data loss. This kind of data loss is defined as an unintentional data overwrite by third-party software on the user's system. A common example of third-party software causing data loss is a Salesforce Admin using third-party tools, such as Demand Tools, who inaccurately identifies a prospect as a duplicate account and ends up deleting that prospect's record completely. Cloud data loss from third-party software is repairable, but can be time-consuming and costly. The Salesforce data recovery process, as an example, can cost upwards of $10,000 and can take an entire week to complete.[3]

Protecting Yourself from Data Loss

This white paper has now covered the top five ways organizations lose cloud application data. This section of the white paper will explore different backup methodologies that can help mitigate cloud data loss.

Data Export

Many SaaS applications offer a native export tool. Using your application's export tool, you can download SaaS application data in a raw format. That raw data can be manually imported back into the application of choice, however, depending on the application and the way the raw data is tagged, re-importation is not guaranteed to be a seamless process.

Not all SaaS applications allow users to export data on their own schedule, either. For example, Salesforce Data Export allows for manually generation of backup files once every six or 28 days. If the queue is large enough at the time an export is planned, it is possible a user will have to wait as many as seven days for that export to be made. For Salesforce users backing up on a weekly basis, this is an unacceptable amount of time to wait for copies of their records.[4]

In either case, performing backups on only a monthly or weekly basis is unacceptable. Users are making changes to files consistently throughout the day, each day of the week. The more time that is left between backups the greater the likelihood that the organization is missing a piece of data in the interim period.

Manual Backup

Manual backups are time-consuming and take IT professionals away from the jobs and tasks that rank higher on the hierarchy of business needs. When networks go down or employee computers need to be fixed or updated, it is common for backups to be pushed aside while those high-priority tasks are completed. The fact that manual backups have the potential to be inconsistently performed makes this backup methodology an inherently unreliable method. On top of being time-consuming, having humans perform SaaS backups is costly. The organization is spending an inordinate amount of time and money to have staff members perform a relatively menial, tedious task.

Finally, the cost of storage is something that any company must consider when adopting a backup strategy. As more and more manual backups pile on, the organization must consider how much it costs to retain these backups. Manual backups are not incremental. In other words, each backup will take more time than the last, and since the organization is taking on the storage itself, storage costs will rise because more data is being retained each time.

Automated Backup

Automated backups are scheduled backups of SaaS application data. Backup automation frees IT staff members and resources to be available for other proactive IT measures, as well as addressing fixes or disasters that have occurred in the IT environment.

Automated backup is not a native function of commonly used business SaaS applications, as they're not incentivized to store client data longer than the application's standard retention policy. Automated backup is a function largely fulfilled by third-party applications at pre-scheduled times and varying increments on a daily basis. Solutions that back up data multiple times a day at frequent intervals are more accurate than applications that back up less frequently. Additionally, automated backup applications ensure that data is backed up to a second, secure location.

Off-site Backup

The safest measure of backup is backing up to an alternate location. The primary benefit of off-site backup services is that if an attack on your data, or an on-site backup is made and the data is compromised, all is not lost because a second version of the same data exists elsewhere. Malicious users or hackers may very well delete a large portion of sensitive business data from the

SaaS application of choice, but a secure second backup location will negate the attacker's efforts once a restore is performed. Ideally, the cloud-to-cloud backup solution employed by proactive organizations combines both backup automation and a secure second backup location.

Introducing eFolder Cloudfinder

eFolder Cloudfinder ensures that the data used in an organization's instance of commonly used business applications is backed up, restorable, and protected. Cloudfinder can be used to perform backups on:

- Google Apps emails, files, folders, attachments, and metadata.
- Salesforce records, standard objects, custom objects, emails, and files.
- Office 365 emails, files, folders, attachments, and metadata.
- Box files and folders.

Organizations that deploy Cloudfinder can rest assured that all of their critical application data is backed up three times a day to an encrypted, tamper-proof SafeHaven®. Cloudfinder utilizes military-grade encryption, ensuring that user data is protected from the most powerful of attacks.

Administrators can instantly search data with rich filtering and select the data to restore. Search filters include title, owner, created date, modified date, and folder so that it is simple to find any record that needs to be restored. For emails, administrators can even search send date, received date, label, sender, subject line, keyword, and attachment names. In addition, detailed dashboards, reports, and monitoring of all backup activities demonstrate how Cloudfinder is working to protect organizational data. These features benefit businesses by allowing easy access any file that may have been lost, while giving IT staff insight greater insight on how the applications are being used.

Cloudfinder's ability to perform granular, point-in-time restores helps it stand out from other backup solutions. Organizations that have experienced data loss are able to restore to a specific point in time before loss occurred. Because application data is backed up three times a day, Cloudfinder ensures minimal data loss in a restoration, and because data is restored directly into the application of choice, organizations face minimal downtime.

When choosing a backup solution, the two most important factors are backup accuracy and how quickly a SaaS environment can return to normalcy after a loss of data. Cloudfinder excels at both factors, making it the most powerful solution on the market.

To learn more about the Cloudfinder solution, and how cost-effective and powerful it can be for your organization, visit www.cloudfinder.com to request a free trial or demo today.

[1] Woods, Jack. "20 Cloud Computing Statistics Every CIO Should Know." Silicon Angle 23 Jan. 2013.

[2] Kavilanz, Parija. "Cybercrime's Easiest Prey: Small Businesses." CNNMoney. Cable News Network, 22 Apr. 2013. Web. 28 Mar. 2015.

[3] Csaplar, DIck. "SaaS Data Loss: The Problem You Didn't Know You Had - See More At:
Http://www.aberdeen.com/research/8323/ai-cloud-data-loss/content.aspx#sthash.wEUyJEJe.dpuf."
Http://www.aberdeen.com/research/8323/ai-cloud-data-loss/content.aspx. 25 Jan. 2013. Web. 13 Feb. 2015.x

[4] "Exporting Backup Data." Exporting Backup Data. 1 Jan. 2015. Web. 28 Mar. 2015.
<https://help.salesforce.com/apex/HTViewHelpDoc?id=admin_exportdata.htm>.

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

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