eFolder White Paper: 3 Little-Known Risks Associated with Leading Cloud Services

May 2015

Introduction

In the last few years, an increasing amount of corporate information has moved to the cloud. Office 365 and Google Apps moved productivity online; Salesforce paved the way for an entirely cloud-based CRM solution; and Box created a compelling cloud-based file sync and share solution. Rightfully so: cloud services and SaaS applications have unlocked numerous benefits, including affordability, collaboration, accessibility, and mobility. Unfortunately, these inroads have not reduced the potential for data loss.

Misconceptions abound about cloud data; the most prevalent myth is that there is no risk of data loss in the cloud. This belief has led many small- and medium-sized business to eschew standard business continuity practices, such as regular backup and auditing of data, when it comes to the cloud. Unfortunately, the statistics are sobering: a study commissioned by Symantec and published in 2013 reports that more than 40% of companies have lost data in the cloud.[1]

This white paper aims to address several aspects of the cloud that businesses overlook. It highlights the issues of accidental and malicious data deletion, subpar data retention policies applied by leading SaaS providers, and common mishaps with data migration, export, and integration. This white paper also discusses why it is imperative that businesses employ a cloud-to-cloud backup, search, and restore solution that will minimize the risk and cost of data loss.

Risk #1: Accidental or malicious data deletion

The primary threat to cloud data is user error. Accidental or malicious deletion poses a constant threat to corporate data, and the open and collaborative nature of cloud applications increases this risk. A recent study by the Aberdeen Group revealed that user error was the number one source of cloud data loss, accounting for 64% of data loss events.[2]

Data, including records, emails, contacts, and documents are all susceptible to user error or accidental deletion. As an example, an employee may delete an old electronic receipt she believes she no longer has a need for, only to discover that the accounting department needed access to her copy. On a daily basis, system administrators are burdened by these types of data recovery procedures.

Malicious or deliberate data deletion is also all too common. There are several instances of ex-employees or disgruntled employees with proper credentials logging into their cloud account and deleting critical emails, documents, customer data, and more. If the cloud service being used does not have adequate retention policies in place, a timed, automatic deletion could result in permanent deletion of the data.

When data is stored in a cloud application with an inadequate or non-existent backup strategy, accidental or malicious deletion is a time-consuming and costly experience.

Risk #2: Subpar data retention policies

Organizations using cloud services wrongly assume that once their data is stored in the cloud, it is always accessible at a moment's notice. In reality, most major cloud services only retain data for a limited amount of time; this often only becomes apparent when a system administrator tries to retrieve deleted information only to discover that it has been automatically purged.

It is important to note that data retention does not just come into play when files are accidentally or purposefully deleted. When an employee leaves an organization, his or her user accounts are usually closed, taking the corresponding data with them. Besides the inconvenience of lost data, there can be serious legal and financial implications if data is not retained long enough. Here is a look at the retention policies of four major cloud services:

Microsoft Office 365
Microsoft's Office 365 has been a major hit in the business world, but its retention policy deserves a second look. SharePoint Online retains deleted data for a maximum of 216 days, after which it is purged and unrecoverable. For Exchange Online, once a user deletes an item from his or her Deleted Items folder, the item is retained in a secondary folder accessible to admins for only 30 days unless Exchange Online Archiving is added on for an additional cost (included with Enterprise E3 plans). With OneDrive for Business, deleted items are retained for a maximum of 186 days, after which they are purged and unrecoverable. More concerning is the lax retention surrounding deleted user profiles; OneDrive only retains data for 14 days once an admin deletes a user profile. Since Office 365 drives so much productivity within organizations, losing any data from this service could result in significant downtime and costs.

Google Apps

Much like Office 365, Google Apps is the hub of emails, calendars, contacts, and other important documents for businesses that have fully embraced the cloud. Unfortunately, Google Apps' retention policy is rather onerous. With Gmail, deleted emails stay in the Trash for only 30 days before they are purged. Google offers an archiving solution, called Vault, for an additional $5/user/month. However, Google Vault does not protect items that have been deleted from Google Drive's Trash; these files are purged and unrecoverable once deleted from the Trash. From a data security standpoint, Google Apps is not much better than an ordinary computer that doesn't have a backup system in place. Especially since storing and backing up most Google Apps data locally is not an option, losing data from Google Apps could result in permanent loss.

Box

Box, used by many businesses as a cloud file sync service, features configurable retention for its Business and Enterprise plans. Additionally, Box's Retention Management feature, released in 2015 and available only for Enterprise plans, allows administrators to set "formal retention periods to protect selected files from deletion for a number of days, months, or even years." Box does note that "at the expiration of a retention period, [Retention Management] ensures proper disposition."[5] This means that administrators who improperly set retention policies for critical data could see that data deleted permanently sooner than expected.

Salesforce

Salesforce helps over one hundred thousand organizations keep track of their contacts, opportunities, and other CRM data in the cloud. For such a comprehensive solution, Salesforce's minimal retention policy is alarming. Once a user deletes an item (such as a record), it goes into Salesforce's Recycle Bin. Unfortunately, just 15 days after an item enters the Recycle Bin, Salesforce purges the item. Though Salesforce offers the option to recover purged data, this process — called Data Recovery — is limited, expensive, and time-consuming. Salesforce says it "can go back no more than 90 days for production and 30 days for Sandbox from the date of deletion" and charges $10,000 at minimum for the service.[6] Moreover, Data Recovery takes about 4 business weeks. Companies whose Salesforce data goes missing can suffer immensely if their sales and marketing teams are unable to access any customer information when they need it the most.

Risk #3: Mishaps with data migration, export, and integration mishaps

Every cloud platform is vulnerable to mishaps when it comes to data migration, export, and integration. Whether it is customer records in Salesforce, information in a shared document, or contact lists, it is easy for anyone to overwrite previously existing data, either purposefully or inadvertently.

Issues related to third party software and account migration can result in cloud data loss. Moving to a new email client, for example, could result in a user's inbox being lost, especially if multiple email accounts are being configured at once. A record management application, such as Salesforce Data Loader, could import duplicate contact information from multiple services and overwrite information at the source when syncing new data. An outgoing employee may delete her calendars without realizing her incoming replacement needs that data. Regardless of the case, undoing the damage caused by data overwrites or data loss requires a separate backup repository linked to individual recovery points.

Conclusion

There is no doubt that using cloud services presents companies with numerous advantages. Data, including files, emails, contacts, and documents, can be shared and accessed by multiple people across multiple devices, and businesses can save money and enjoy greater collaboration by moving productivity to the cloud.

Unfortunately, the risks of inadequate data retention policies, data deletion, and data corruption need to be carefully considered by administrators looking to utilize the cloud. Administrators looking to transition to cloud services need to consider the risks of inadequate data retention policies, data deletion, and data corruption. The sources of data loss and the limited retention policies of cloud applications make it imperative for businesses to implement a robust backup, search, and restore solution when transitioning business applications to the cloud.

Though little can be done to prevent files from being accidentally or maliciously deleted, eFolder Cloudfinder backs up the critical data stored in Office 365, Google Apps, Salesforce, and Box to ensure these deleted files can always be found and recovered. Commonly used cloud services often lack customizable retention policies in line with corporate requirements, but Cloudfinder provides an encrypted, tamper-proof SafeHaven™ with unlimited retention for all cloud data. Finally, Cloudfinder ensures that mishaps with migrations, exports, and integrations do not cause important data to be overwritten.

Cloudfinder adds value to leading SaaS applications, empowering businesses to work in the cloud without worrying about their data being permanently deleted. Learn more at www.cloudfinder.com.

[1] Symantec. "Avoiding the Hidden Costs of the Cloud." Mountain View, 2013

[2] Aberdeen Group. "Who are the Heavy Users of SaaS Applications?" Boston, 2013

[3] Microsoft. "Configure Deleted Item retention and Recoverable Items quotas" https://technet.microsoft.com/en-us/library/ee364752%28v=exchg.150%29.aspx

[4] Google. "How retention works" https://support.google.com/vault/answer/2990828?hl=en&ref_topic=3209998

[5] Wacker, Rand. "The Products That Power Box for Financial Services." Web log post. Box Blog. Box, 26 Feb. 2015. Web. 26 Mar. 2015.

[6] Salesforce.com. "Data Recovery Service and Cost" https://help.salesforce.com/apex/HTViewSolution?id=000003594

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