eFolder White Paper: 5 Best Practices for Backing Up Salesforce Data

July 2015

Copyright © 2015, eFolder, Inc.

Introduction

Over the last decade, Salesforce has become the market-leading CRM solution. For organizations focused on managing customers and moving leads efficiently through the sales cycle, Salesforce data is the lifeblood of their business. When this data is lost, deleted, or compromised, sales operations are interrupted or ceased, resulting in significant costs to the business. This reality makes it imperative that IT administrators design a backup strategy for Salesforce data.

But Salesforce data resides on secure servers. Why is a backup strategy necessary?

Many IT administrators are quick to point out that Salesforce data is stored on secure and resilient servers, and recognize that Salesforce has taken measures to ensure continuity of service. While all of these assertions are correct, IT administrators often overlook the primary causes of Salesforce data loss: human intervention and user error.

Implementing a backup strategy for Salesforce is not intended to protect against architectural, hardware failure, or service interruptions. Backing up Salesforce data protects against the primary causes of cloud data loss: human intervention and user error.

No matter how resilient cloud services are, Salesforce cannot prevent errors that originate from human intervention and user error. According to a 2013 study by the Aberdeen Group, 32% of companies using SaaS services, such as Salesforce, have reported losing data, with 64% of that data loss coming as the direct result of user error. In fact, the top five sources of data loss are the result of human intervention: user error (64%), hackers (13%), closing account (10%), malicious deletion (7%), and third-party software (7%).

How much does Salesforce charge to recover lost data?

Besides the costs absorbed by a business when sales operations are interrupted, Salesforce charges a significant amount of money to recover lost data. Salesforce offers a "last resort" Data Recovery that costs $10,000, takes 20 days to complete, and is only able restore three months of data from the day the Data Recovery is performed[1]. When the Data Recovery is completed, the client receives the data in a raw .csv format and must clean up and import the data back into Salesforce on their own. This "last resort" option is not an ideal data recovery scenario, which is why many IT and Salesforce administrators are in the market for a comprehensive and cost-effective Salesforce backup solution.

This white paper outlines five best practices for backing up Salesforce data to help IT administrators and business owners design a Salesforce backup strategy for their own organization.

Copyright © 2015, eFolder, Inc.

Best Practice 1: Backup Salesforce Data

The first best practice for backing up Salesforce data is to design a backup strategy. As we previously discussed, this preventative measure can prevent businesses from incurring significant costs when Salesforce data is lost. IT administrators can design their backup strategy in multiple ways.

Currently, the native Salesforce application offers a tool called "Salesforce Data Export," which allows users to make regularly scheduled manual or automatic backups once every 6 or 28 days. When the export is initiated, the export is placed in a queue and performed when other activity has cleared.

There are several downsides to the Salesforce Data Export tool. The first being that it must be initiated by a Salesforce administrator, making it an easily forgotten process. Also, because the Salesforce Data Export is placed in a queue, it is at the whim of other requests and activity and may actually be performed at a much later date than when it was initiated, making the date unreliable. Finally, the Data Export produces data in a raw CSV format, creating additional steps for IT administrators that want to restore data directly back into the application.

Performing a Salesforce Data Export is a step in the right direction – but it is clearly a rudimentary process for backing up and restoring Salesforce data. Instead, many IT administrators are designing their backup strategy with a cloud-to-cloud backup solution that offers automated backup; in the next best practice, we discuss the importance of automating backups.

Best Practice 2: Automate Salesforce Backups

Relying on manual backup is not an acceptable business practice. A manual backup strategy drains an IT professional's most valuable asset: their time. If IT professionals are occupied working on menial, time-consuming efforts such as performing backups – a task that can easily be done by machine – other important IT initiatives are delayed.

Copyright © 2015, eFolder, Inc.

Even Salesforce's native Data Export automation does not qualify as a completely automated solution. With Data Export, a user is still required to download the data manually within 48 business hours of receiving their data export confirmation email before that data is deleted by Salesforce.

Besides being time-consuming, manual backups allow for user errors to affect the quality of a backup. When a machine can automate the process, users can be sure that their Salesforce data is most accurately backed up on a regular basis. Further, performing a manual backup can be easily forgotten or put off in lieu of more pressing issues and tickets..

Backup is often inappropriately thought of as a "nice to have," so when an organization's IT staff has a pressing initiative or mission-critical task at hand, backup unfortunately is one of the first tasks to be overlooked. With backup automation, a business is assured that important data is consistently backed up without fail, regardless of any other IT tasks at hand.

Best Practice 3: Back Up to a Second Location

Backing up data in the same instance where the active files live is not enough. In the event of a malicious or innocuous deletion of Salesforce data, without a backed up version in a second secure location, the organization is not entirely protected. For instance, if a malicious user or hacker were able to get into a user's Salesforce application, it is highly likely that they could access the backup if it is in the same instance and destroy that data just as easily. Similarly, in the event of an accidental deletion of Salesforce data, a user could cause harm to a backup if it is not stored away in a location that is inaccessible to standard-provisioned local users.

For this reason, leading cloud application backup services back up and copy organizational Salesforce data to a secure second location, utilizing military-grade encryption to store client data safely away from compromise. This setup allows for an organization's Salesforce admin to call down data if a restore is necessary and assures that the quality and accuracy of the backed-up data is optimal.

The second location should be secure enough that even if an organization's Salesforce data were the target of an attack, it would result in a failed attempt to destroy that data.

Copyright © 2015, eFolder, Inc.

Best Practice 4: Unify SaaS Backups

Adopting a cloud backup solution for organizational Salesforce data is a positive start, but deploying a comprehensive backup solution for all company cloud applications is necessary for optimal security and productivity.

The cloud-to-cloud backup solution an organization chooses should serve as a complete backup, search, and restore service for the common business applications used by the company. The rapid rise of cloud adoption, and especially CRM adoption, means that companies are more reliant on the cloud than ever before.

The likelihood that an organization is making every day use of two or more common cloud applications, such as Office 365, Google Apps for Work, or Box, in addition to Salesforce, is high. As such, those organizations benefit from a cloud-to-cloud backup solution that connects those applications in an environment that consolidates backups.

A solution that allows for instant full-text search and rich search filtering across multiple applications gives organizations the ability to quickly find files related to the search query regardless of which application they're stored in. Users can search for names, projects, folders, files, and instantly find anything related to the query, whether it is an email, contact info, contract, lead, or opportunity. In the event the searched data has been deleted from the application it refers to, the user can also quickly restore it so the sales team can resume work immediately.

A complete cloud application backup, search, and restore solution goes beyond making sure an organization's sensitive data is protected, it makes that data more useful through connectivity.

Copyright © 2015, eFolder, Inc.

Best Practice 5: Leverage Backups

Given that an organization is following the first four best practices, the final best practice for backing up Salesforce data is to leverage the cloud application backups being created. With a system in place that allows for easy search and restore, it is practical to use the solution as an internal search engine in which IT admins can quickly track down any SaaS file, regardless of which application it lives in.

Three of the most important things to consider in a cloud backup solution are:

- How soon can data be restored in a useable format?
- How accurate is the restore going to be?
- How long is backed up data retained?

Is the recovered data going to be pushed back down into the application of choice and be immediately restorable, or will it be sent to the user in a raw format that must be meticulously formatted and re-imported into the cloud application before employees can access and utilize that data? Organizations should choose a solution that boasts the former restoration to truly leverage backups.

This solution should also allow for accurate and flexible data restores. What this means is that in the event a restore is necessary, the data can be restored to exact point in time the user desires. If an accidental deletion occurred on February 19 at 4pm, and the closest time the user's backup solution can restore to is February 16 at 9am, there is still a significant amount of time and data that will not be accounted for, which is simply unacceptable in a backup solution.

The third consideration, retention, is also key. Several verticals, such as financial, insurance, medical, and law, operate under regulations that require them to keep data on file for long periods of time. If an organization's backup solution does not allow the organization to fulfill those obligations, the organization should look elsewhere for a more comprehensive backup.

Fully leveraging cloud backups is an important piece of the security and productivity puzzle, a piece that cannot be overlooked when choosing a cloud-to-cloud backup solution.

Copyright © 2015, eFolder, Inc.

Introducing eFolder Cloudfinder

eFolder Cloudfinder is a cloud-to-cloud backup, search, and restore service that automatically backs up cloud application data to a secure off-site SafeHaven®, with zero possibility of accidental deletion, three times per day. Cloudfinder backs up the most important data used in common business applications, including Office 365, Google Apps, Salesforce, and Box from a single interface.

Cloudfinder backs up the following files:

- Salesforce – Records, standard objects, custom objects, emails, files, and metadata
- Office 365 – Emails, files, folders, attachments, and metadata
- Box – Files and folders
- Google Apps – Emails, files, folders, attachments, and metadata

A key strength of the Cloudfinder solution is its ability to perform point-in-time restores, so users can pinpoint the time right before an accidental deletion or disaster occurred, and restore data to that time. Cloudfinder enables instant full-text search across all four previously mentioned cloud applications, as well as rich document search filtering, including title, owner, created date, modified date, and folder make it simple to find any record that needs to be restored. And with rich filtering that includes send date, received date, label, sender, subject line, keyword, attachment names, and within attachments, a lost document is never further than a quick search away.

The fact that Cloudfinder automatically performs backups three times a day means that when a restore is performed, the admin is guaranteed to have an accurate representation of the data they wish to restore at any given time, instantly. Manual backup solutions require the user to re-import compromised data on their own, costing businesses time and money while waiting for that data to become usable again. With Cloudfinder, restores are made directly into the cloud application of choice, resulting in the least amount of possible downtime.

To learn more about the Cloudfinder solution, and how this solution can be used to protect cloud application data, visit www.cloudfinder.com to request a free trial or demo today.

Copyright © 2015, eFolder, Inc.

[1]"Exporting Backup Data." *Exporting Backup Data*. 7 Jan. 2015. Web. 17 Apr. 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

©2015 eFolder, Inc. All rights reserved. eFolder™ is a trademark of eFolder, Inc. 06/15 EF363