Outlook Report

Backing up Software-as-a-Service Applications

An Outlook Report from Storage Strategies NOW

December 1, 2014

By Deni Connor and Earl Follis
Client Relations: Phylis Bockelman

Storage Strategies NOW
8815 Mountain Path Circle
Austin, Texas 78759
(512) 345-3850

SSG-NOW.COM

Note: The information and recommendations made by Storage Strategies NOW, Inc. are based upon public information and sources and may also include personal opinions both of Storage Strategies NOW and others, all of which we believe are accurate and reliable. As market conditions change however and not within our control, the information and recommendations are made without warranty of any kind. All product names used and mentioned herein are the trademarks of their respective owners. Storage Strategies NOW, Inc. assumes no responsibility or liability for any damages whatsoever (including incidental, consequential or otherwise), caused by your use of, or reliance upon, the information and recommendations presented herein, nor for any inadvertent errors which may appear in this document.

This report is purchased by Spanning Cloud Apps, who understands and agrees that the report is furnished solely for its distribution to customers and prospects, without the prior written consent of Storage Strategies NOW.

Copyright 2014 All rights reserved. Storage Strategies NOW, Inc.

StorageStrategies NOW

Outlook Report

Sponsor

Dear Reader,

SSG-NOW takes a look at technologies and products when confusion exists in a specific market. In this case, we looked at the software-as-a-service market (SaaS) and some of the applications that reside in the cloud. We asked users and vendors a lot of questions and received a variety of responses. Perhaps the most common responses we received were actually questions: Why do you need to back up software-as-a-service applications, such as Salesforce or Google Apps, when the cloud service provider or vendor managing the service backs them up automatically or as part of the service? Why when you use a cloud application, such as Google Sheets, do you need to back it up when you could simply export the file to your local drive and consider it done?

If your company uses SaaS applications, such as Google Apps, Salesforce or Microsoft Office 365, your company may be at considerable risk for data loss even as you read this report. Ironically, many companies are flocking to SaaS applications precisely because they assume that, a) their SaaS provider will diligently perform periodic backups of all company data, and b) their SaaS provider will happily and quickly restore any data that turns up missing, whether due to nefarious deeds, user error, replication errors, malware infections or other data-loss causes. That is not always – in fact, it is rarely – the case.

While all SaaS providers do perform regular backups, those backups may not include all of the business-critical data on which your company depends. And, even for the data that is backed-up by SaaS providers, restoration of your business-critical data after a data-loss event may be expensive, time-consuming, impractical or even impossible in some cases. The purpose of this report is to identify the risk of data loss when using SaaS applications and recommend best practices that can mitigate -- or even eliminate -- that risk. If your company relies on SaaS applications to support critical business functions and activities, the information provides an eye-opening look into the unseen dangers of putting all of your IT eggs in the SaaS basket without a viable plan to restore data, when necessary.

This report is aimed at IT professionals, companies and organizations who want to learn more about SaaS applications and the inherent risks of betting that your SaaS provider will be there for you in case of a data-loss event.

SSG-NOW is pleased to present this report on backing-up and restoring SaaS applications. Read it with interest and if you have any questions or comments, please feel free to contact us at the addresses below.

Deni Connor
Principal Analyst
dconnor@ssg-now.com

Earl Follis
Senior Analyst
efollis@ssg-now.com

Executive Summary

Cloud-based applications and software-as-a-service (SaaS) are quickly revolutionizing the way companies deploy and manage their business-critical computing resources. The impetus for moving to SaaS applications include lower costs, ease of administration and deployment, automatic scaling of resources, ubiquitous access, resiliency and data security. The cloud certainly delivers all of these benefits to varying degrees. Of these benefits, data security and resiliency are probably the most often cited yet least understood aspects of SaaS applications, because most companies assume cloud-based application providers will fully protect their data with complete backup and recovery services. Though various SaaS providers do perform regular backups of customer data, those backups are not configurable or accessible in any way from the customer perspective.

For example, though salesforce.com backs up their customer data nightly, the only option for recovery is to engage Salesforce directly, pay a minimum of $10,000, then wait a few weeks for their data to be restored. salesforce.com does offer customers the opportunity to automatically export all customer data and attachments to a downloadable comma-separated values (CSV) file, though the most frequently that task can be scheduled is once a week.

The other area of concern for companies who depend on SaaS applications is the process of performing restores of deleted, missing or corrupt files.

Just because your SaaS provider performs regular backups does not mean that you can easily access those backups, because SaaS providers do not open their backups to customers, nor do they make restoring critical data easy or intuitive. Horror stories abound of companies that bet their business and IT operational plans on the safety and security of SaaS applications, only to discover that there are many situations where your SaaS provider is either not backing up all of your critical data, or else the process to restore said data can take weeks and thousands of dollars just to recover needed files. There must be a better way to reap the myriad benefits of SaaS-based computing without simultaneously exposing your company to the risk intrinsic in loss of business-critical data and files.

Enter a group of intrepid engineers and entrepreneurs who decided that one huge missing piece of the SaaS puzzle is the lack of a clear and cogent backup and restore strategy for companies who rely on SaaS applications to generate revenue and conduct day-to-day operations. The resulting company, Spanning Cloud Apps, has an elegant solution for companies who signed up for SaaS applications before realizing the implications of making such a move without a strategy to ensure the security of their data. The more a company relies on SaaS applications to run their business, the clearer their need for a tool that backs-up and restores SaaS application data. The editors of this

report have been followers of Spanning Backup almost since the inception of the company. The company management team includes a virtual who's-who of high-performing tech companies such as Vignette, SailPoint, IBM, Symantec, Microsoft and Oracle. The seasoned software pros at Spanning have developed an easy-to-use, comprehensive software solution for protecting company data that resides in SaaS applications.

This report will delve into more detail about the problems of backing-up and restoring SaaS applications, while also providing an in-depth look at the Spanning backup and restore solution. Remember, that modern data security is not just a matter of being able to retrieve data from SaaS applications; most companies operate under corporate compliance and governance requirements for data retention of certain types of information. A comprehensive business continuity and data retention plan is a requirement for most corporate compliance and governance guidelines and regulations. Spanning helps companies meet these requirements by providing a customer-controlled method to backup and restore SaaS application data on an as-needed basis, including as part of a business continuity plan. Beyond those regulatory requirements, Spanning also provides data protection for SaaS application data by allowing for ad hoc restoration of data, either by an administrator or by the end-user. Spanning protects from accidental or malicious deletion of SaaS data by providing a quick and easy way to restore deleted or corrupt data.

Hence, the loss of data from SaaS applications can directly affect not just the bottom line of a company, but SaaS data loss can also expose a company to sanctions and fines for not retaining corporate records according to applicable laws, both here in the U.S. and abroad. Your company cannot afford to ignore these risks. Implementing a comprehensive data protection plan using Spanning Backup is not just a good idea, it is truly a must-have capability for companies who rely on SaaS applications. Fortunately, Spanning offers just what the doctor ordered at a reasonable cost and with minimal administrative overhead required to fully protect company assets. Spanning helps companies cover the business continuity and data protection gaps that are intrinsic in most SaaS applications. Spanning provides peace of mind for SaaS data, knowing that any data loss can be addressed quickly and easily to restore critical company data.

StorageStrategies NOW
Outlook Report

Business Drivers for Backing up SaaS Applications

The practical use of SaaS applications began 15 years ago with the founding of the senior statesman of SaaS applications, salesforce.com. Salesforce was the first commercially available SaaS application that met with considerable success in the marketplace. At first, Salesforce was dogged by the perception that the service was prone to outages and the importance of resiliency of the network link to the Internet was under-appreciated. According to Forbes.com, by 2004, Salesforce had more than 200,000 users from more than 13,000 companies. By 2014, according to salesforce.com, Salesforce now boasts more than 100,000 customers and a market capitalization of more than $4 billion.

Buoyed by the success of Salesforce and the increased acceptance by mainstream businesses of cloud-based applications, millions of users now use Microsoft Office 365, Google Apps and many other SaaS offerings on a daily basis. The perception of many SaaS users is that because SaaS applications are cloud-based, regular backups and easy-to-perform restores are included in the SaaS paradigm. This widespread assumption is not only inaccurate; it can be a catastrophic assumption for companies who assume that their cloud-based data is secure and easily restorable in case of a data loss event.

The costs of data loss and downtime can be significant, with some industry analyst firms estimating that downtime costs a company an average of $5,600 per minute, or more than $300,000 per hour. Of course, these are just average figures. Companies that have embraced SaaS applications can easily lose much more than $300,000 per hour if they have thousands of employees who cannot access the cloud-based applications required to perform their jobs. SaaS outages and accompanying data loss can not only leave employees in a non-productive state for hours at a time, but can also cause a direct hit on revenue as orders cannot be placed or processed. Even when a SaaS application is back online after an outage, the time and expense required to restore lost data can be significant. The implications for reduced profitability, inability to generate revenue and the expense of recovering lost SaaS data can severely affect companies, who suffer a data loss with no defined disaster recovery plan.

To a casual observer, the fact that SaaS applications are cloud-based gives the impression that regular data backups occur automatically and thus, data recovery is a no-brainer. This impression could not be further from the truth. Though cloud-based applications do make disaster recovery (DR) and data protection (DP) activities easier to perform, it is a mistake to assume that DR/DP for cloud-based applications is a naturally occurring feature of SaaS applications. Every company who leverages SaaS applications must also devise an effective DR/DP strategy to deal with data loss events. Many SaaS providers tell their customers that all SaaS data is backed-up on a regular basis, and thus data loss events should be non-existent. Yet the dirty little secret of the SaaS industry is that companies lose company SaaS data on a regular basis and most SaaS providers do not offer on-demand data restore capabilities that can be initiated by their customer companies. That perception gap between what many companies *think* that their SaaS provider offers for a DR/DP strategy, versus the

true DR/DP capabilities of SaaS providers, is a much-needed market niche for companies that offer a SaaS backup and restore software solution.

Cloud-based SaaS applications provide the perfect mechanism to make the backup and restore of SaaS data a reality. Now that applications are located on a public cloud, companies, such as Spanning, can access the underlying data structure of SaaS applications via application programming interface (API) calls and other methods to backup and restore SaaS data. Whereas your SaaS provider sets their backup frequency and may offer data export only weekly or monthly, SaaS backup and restore applications offer configurable backup schedules and self-service restore capabilities that put control of SaaS data back in the hands of the data owners, not the SaaS providers.

SaaS application backup and restore software faces numerous challenges to backing-up and restoring SaaS data, including getting access to SaaS data, utilizing undocumented or ever-changing SaaS APIs and the "hidden" nature of SaaS details, at least from the customer's perspective. Though most SaaS providers profess that their backup and restore processes are all any customer should need, most SaaS providers will also acknowledge that providing transparent backup and restore capabilities are not priorities. In this way, SaaS providers recognize the need for backup and restore applications, such as Spanning, while not necessarily making life easy for these companies. As a result, SaaS backup and restore companies must constantly be vigilant that their software is compatible with new releases of SaaS applications.

Backing up SaaS Apps Essentials

Now that the problem of SaaS application data protection is better understood by the technology media and many SaaS customer companies, the question is: How does SaaS data backup and restore software work and how do I use it to protect my SaaS data? SaaS backup and restore companies map out the various publicly visible and hidden components of SaaS applications and figure out effective strategies to back-up every available data set. Most of the mapping and gathering of data is performed via published APIs from the SaaS provider. Spanning and other SaaS backup and restore vendors also work closely with SaaS providers, such as Google and Salesforce, to ensure that all publicly accessible data is fully protected.

Though the idea that every SaaS data set be regularly backed-up is considered a universal truth in the technology arena, to ensure that your SaaS data is protected, it's important to first understand the specific situations that might lead to a data loss event for SaaS applications:

- Accidental deletion of data by an authorized user;
- Malware or other cyber threats, including cyber-attacks;
- Disgruntled current or former employees, who trigger a data loss event in an attempt to delete or corrupt company SaaS data;
- Application and data migrations performed under the covers by your SaaS provider resulting in significant loss of data; and,
- For Salesforce users, deploying a misbehaving Salesforce application -- whether developed in-house or purchased from the Salesforce AppExchange -- can cause data loss in your Salesforce workspace.

These risks are all-too-common in the modern IT landscape and most companies deal with one or more of these risks on an ongoing basis. Accidental deletions happen on a daily basis at most companies, underscoring the need for an easy-to-use, self-service restore capability in your SaaS backup solution. Malware, cyber-attacks and the actions of disgruntled employees are a common source of publicly identified data loss, including many high-profile cyber-attacks on governmental and corporate infrastructure.

The fact is that while all SaaS applications are backed up by the SaaS provider on a regular basis, those backups are not configurable and may not provide the requisite layer of protection against customer data loss. For instance, Salesforce backs-up customer data daily but only allows customers to automatically export that data to a CSV file on a weekly or monthly basis. Most companies require at least daily backups and some might require backups to be performed either more often than that or on an ad-hoc basis. Salesforce does not offer and cannot meet data protection requirements that require backups more than once a week or require ad-hoc backups and

restores. Which brings us to another common problem with data resiliency of Salesforce: The process of restoring lost Salesforce data is a slow, cumbersome and expensive process, costing a minimum of $10,000, which typically takes weeks to complete. Salesforce explicitly advises their customers to utilize a SaaS backup and restore solution for the recovery of lost Salesforce data and Salesforce only offers their restore service as a "last resort process."

The process of deploying the Spanning backup and restore solution is simplicity personified: You purchase Spanning Backup licenses based on SaaS users requiring data protection, login as an administrator to the Web-based Spanning application, enter your SaaS application details and credentials, then configure your Spanning account settings. You designate any required delegation of backup and restore rights to your users, configure notifications and auto-generated status reports, and then start using the product. That's all there is to it! Spanning performs backups of your SaaS data on a nightly basis, though Spanning users can perform an ad hoc backups at any time and as often as needed. The Spanning application homepage displays a dynamic heat chart depicting the current and historical status of your SaaS backups. You can drill-in to the status charts to identify and rectify any SaaS backup anomalies. Because one of the goals of SaaS backup and restore solutions is to provide self-service capabilities to end-users, the delegation of restore activities and ease-of-use are of paramount importance to this process. (More about Spanning Backup later.)

Can your cloud service provider restore your data?

There are a variety of questions to be asked as you evaluate whether or not your SaaS provider(s) offer backup and restore capabilities sufficient to protect your company's business-critical data assets.

- Does the SaaS provider perform regular backups? You can't restore data you didn't back up so first, be sure that your SaaS provider performs regular backups that meet your company data retention and business continuity policy.
- If your SaaS provider does provide regular backups, do they also retain past versions of customer files? If so, how many versions are kept before they are aged out of the system, leaving you once again with no data to restore.
- Does your SaaS provider have a reliable method of guaranteeing that requests to delete customer data comes from an authorized source? Most SaaS provider privacy policies require that the provider permanently delete data when a customer instructs them to do so. But most SaaS providers have no way of verifying that a data deletion request is legitimate, rather than unintentional or malicious.
- Assuming that your SaaS provider does perform regular backups of customer data, how quickly can the provider satisfy a customer request to restore data? If it takes weeks for your SaaS provider to perform a data restoration, what will you company do in the meantime? The corollary to "You can't restore data that you didn't back up" is:

Having to wait days or weeks for your SaaS provider to perform a restore of your business-critical customer data is almost as bad as not having that data backed-up to begin with.

- As with any other IT service offering, service level agreements (SLAs) on a SaaS provider's restore process are an important metric to protect customers who need data restored quickly. Unfortunately, most SaaS providers do not offer an SLA on data restores, resulting in most SaaS data restores being performed on a best-effort basis only.
- What are the costs involved in a SaaS data restore? As we've mentioned, Salesforce charges a minimum of $10,000 per data restore request. Knowing that every company needs a way to restore SaaS data on an ongoing basis, wouldn't it be better to spend a little bit of money up-front to protect your SaaS data in order to avoid that $10,000 invoice every time you have to call Salesforce for a data restore?
- Does your SaaS provider have a support or services organization with which customers can engage when a restore of SaaS data is required? Some large-scale SaaS providers, such as Google, do not provide a support mechanism for customers who need to restore their SaaS data.
- Does your SaaS provider's data restore process restore all attributes and sharing rights intact? Google's "admin restore" process will perform a blind restore of data but the data is not restored with the same sharing settings as the original data.
- If your SaaS provider does offer a restore process, who is allowed to perform the restore operation? The provider, the customer administrator, or the end-user who lost the data? Enabling end-users to find and restore their own lost data greatly decreases the time it takes to return users to productivity, while reducing the support burden on IT.

As you can see, there are a plethora of questions, decisions and ramifications that must all be fully considered when evaluating the backup and restore capabilities of a SaaS provider. Spanning provides a solution for each of the issues and possibilities listed above, but customers should ask these questions no matter which SaaS backup and restore solution they choose.

Benefits of Cloud and SaaS backup

For companies that use SaaS applications and want to mitigate the risks of data loss, the fact that there are easy-to-use, cost-effective solutions for backing-up SaaS applications makes implementing one of these solutions an easy decision. SaaS backup solution providers offer reasonably priced monthly and annual pricing models, based on either per-user or per-company licensing. See Figure 1 for a comparison of SaaS backup vendors pricing.

	Google Apps	Microsoft Office 365	Salesforce	Box	Facebook	Twitter	Yahoo
Asigra	Not sold direct*	Not sold direct*	Not sold direct*				
Backupify	$3-$4/month/user; $990/month/domain**		$199-$799/month/co.		$99-$299/month/company**	$99-$299/month/company***	
CloudAlly	$30/year/user	$30/year/user	$30/year/seat				$3/month/user
CloudFinder	$30/year/user	$30/year/user	$30/year/seat	$30/month/user			
Spanning	$40/year/user		$48/year/user				
Syscloud	$6/year/user						

*Pricing on amount of data to recover
**Priced by frequency of backups per day
***Priced by number of users and amount of storage used

Figure 1. SaaS backup vendors and typical license costs

As you can see from Figure 1, license costs average about $3 per user, per month for Google Apps, Office 365 and Salesforce. The only exception to that pricing is Salesforce backup and restore licensing from Backupify, which charges between $199 and $799 per company, per month, based on number of employees. One may also assume that companies with a large number of SaaS users can likely negotiate even better licensing terms than is shown in the chart. Compared to the difficulty of restoring SaaS data after a data loss event, these budget-friendly licensing options underscore the fact that companies that rely on SaaS to run their business simply cannot afford to ignore the exposure created by SaaS

applications. The license costs are negligible compared to a single data loss event that prevents your SaaS application from being online, up-to-date and ready for your employees to use as expected.

The customer-side administrator of SaaS backup and restore solutions is typically the Salesforce, Office 365 or Google Apps administrator. Dedicated SaaS administrators are usually very busy and don't have time to handle restore requests for every user who may accidentally delete data. That fact means that delegation of restore authority and ease-of-use of the restore process becomes even more important to a successful SaaS backup and restore strategy. If you rely on your SaaS admin to handle all data restore requests, you will have only succeeded in moving the bottleneck from your SaaS provider to an internal admin or team of admins. When evaluating SaaS backup and restore solutions, pay particular attention to the self-service portal within the software, to verify that the average SaaS user will be able to fulfill the majority of restore requests themselves.

The last consideration when evaluating SaaS backup and restore solutions is the ability for end-users to provision their own backups as needed. Your SaaS backup and restore solution must also offer end-users the ability to configure their own backup schedules, set notifications, create reports and address any routine backup or restore issues themselves. Your IT help desk will thank you and your end-users will be a much happier lot once they realize that they are empowered to manage their SaaS backups and restores without assistance from an administrator or help desk agent.

Application-specific Use Cases

Salesforce

As the granddaddy of SaaS applications, Salesforce has evolved into an entire eco-system dedicated to customer relationship management (CRM) and related services. The only aspect of the Salesforce SaaS model that has not been fully addressed is the lack of a customer-facing backup and restore portal. Considering that large amount of data being backed-up and archived by Salesforce, if Salesforce were to allow user-configurable backup schedules, it would likely cause a significant increase in the amount of customer data backed-up and archived by Salesforce. Any significant increase in the amount of customer data stored by Salesforce would likely require a significant increase in the cost of Salesforce user

licenses. Hence, the paucity of backup options offered by Salesforce and the expensive, time-consuming restore process offered to customers.

You should also note that custom applications, integrations and customer-defined workflows developed within Salesforce are backed-up during the daily backups performed by Salesforce, but that metadata is not included in the weekly or monthly automatic CSV data exports that Salesforce does offer their customers. As a result, Salesforce customers who have customized their Salesforce workspace with integrations to other software products, added third-party applications or designed workflows in Salesforce are the most at-risk for data loss. At an average cost per user per month of about $4, there is no reason for Salesforce customer data to remain at risk for want of a third-party SaaS backup and restore solution.

Google Apps

Google Apps are a veritable black hole of data resiliency. While Google does reveal that all Google Apps data is replicated across clustered servers, as well as geographically diverse data centers, Google has no apparent strategy for users to be able to configure more-frequent backups or recover lost files. And, it lacks a self-service data restoration portal. Google also does not offer a way to recover lost data when a Google Apps user account has been deleted. Once you delete a user account, the accompanying data is gone forever. As with Salesforce, for an average cost of less about $3 per user per month, there is little downside to subscribing to a SaaS backup and restore service, especially when compared to the business and compliance issues that can be created when a key user suffers a data loss.

Microsoft Office 365

Office 365 is a relative latecomer to the SaaS party, as evidenced by the lack of a cohesive backup and restore strategy for customer data. All Office 365 data is automatically replicated to multiple data centers using a feature in Exchange 2010 called Database Availability Groups. Users do have the option to manually backup Office data via a .CSV export process. Word documents and personal storage files, i.e., .PST files can also be manually exported through the export feature in Outlook. Though Microsoft does give users the ability to manually restore deleted objects from any Office 365 email folder, once a user account is deleted, their data is only recoverable for 30 days. After 30 days, all data from deleted mailboxes is gone permanently. Currently, only one SaaS backup and restore vendor offers coverage for Office 365 users and even that capability is for *email only*, but we expect that situation to change in the near future as other companies jump into the breach. And yes, the ubiquitous price point of about $3 per user per month holds true for Office 365, as well.

Best practices and recommendations

If your company currently uses SaaS applications or is planning to implement SaaS applications in the future, we strongly recommend that you protect your data via a SaaS backup and restore solution. Here is a short list of best practices and other important guidelines for selecting and implementing a SaaS data loss prevention solution:

- Always start your software evaluation with a comprehensive list of hard requirements, nice-to-haves and optional features that are important to your company.

- Research and understand the features and limitations of the SaaS application platform you want to backup. For instance, Google Docs does not allow SaaS backup solutions to backup and restore PDF attachments, passwords, and some Google native formats like scripts and forms, via the Google API.

- Be sure that the SaaS backup and restore solution you choose provides redundant infrastructure with at least three 9s of availability. The only thing worse than not having a viable backup of your SaaS data is to have a backup but not be able to access it due to an issue with your cloud-based SaaS data protection software.

- Alert notifications and reports are a frequently overlooked aspect of backup and restore software. Be sure to spend time exploring notifications and reporting via a hands-on evaluation of the SaaS backup and restore solutions under consideration. There is no better test of the suitability and applicability of software than to test it in realistic scenarios before spending any money.

- Fully test and explore the self-service and delegation capabilities of your SaaS backup software. If possible, have a small group of end-users try out the self-service portal and provide feedback about the usability, ease-of-use and the ability for your admins to delegate routine work tasks, such as data restore, are key features that should not be overlooked.

- Verify that the SaaS backup and restore software you choose has achieved relevant industry certifications. For example, Spanning has successfully completed industry-standard audit process certification.

- 256-bit encryption of data in the cloud, as well as data in transit, is the industry standard for keeping your data secure. Be sure that your software of choice offers comprehensive data encryption both in-transit and at rest.

Proper planning during the evaluation phase is critical to any successful software implementation and that is certainly the case with SaaS backup software. Keeping these best practices and recommendations in mind will help your company avoid difficulty and expenses down the line. We also recommend that you open a support case with the vendor as part of any evaluation program for SaaS backup and recovery solutions. Considering the mission-critical role of backup and recovery to customers, your SaaS backup provider must be willing and able to deliver excellent customer service because data loss events are typically an emergency situation and vendor support must be exemplary. It's important to know before you buy a SaaS backup and recovery solution that your vendor of choice will be there when you most need them.

StorageStrategies NOW

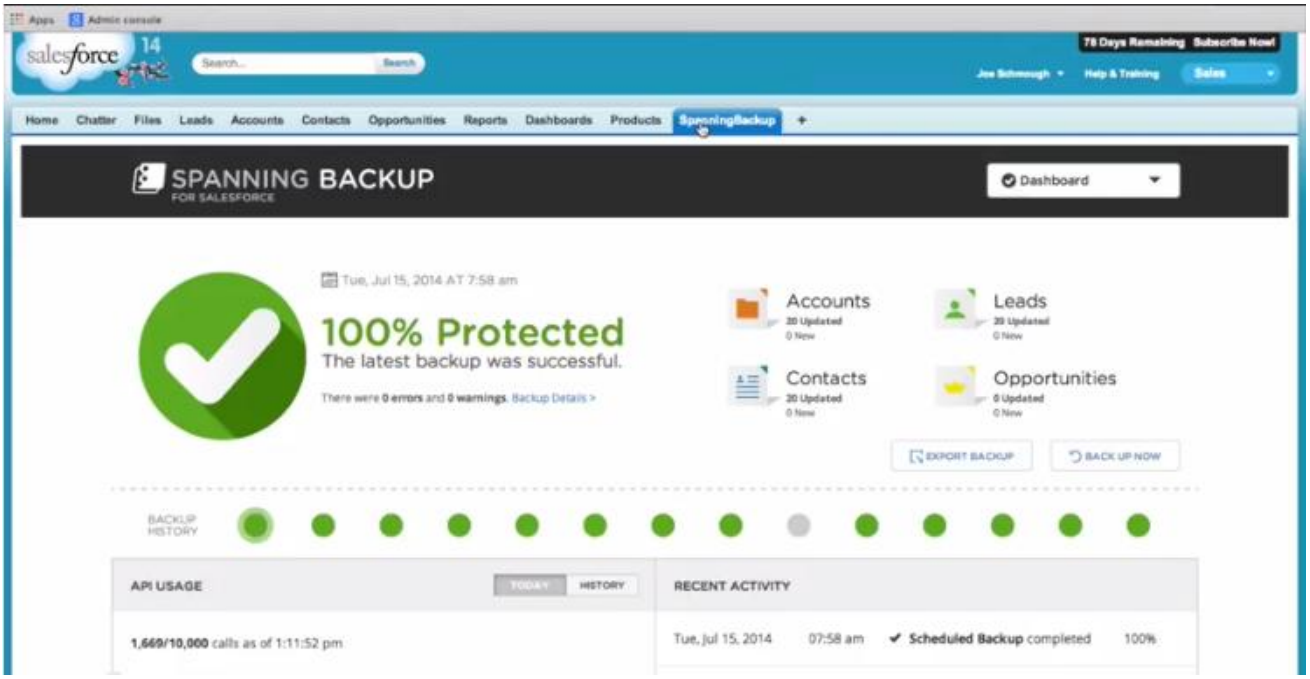
Outlook Report

Vendor/Product Profile

Company name: Spanning Cloud Apps
Product Name: Spanning Backup for Salesforce and Spanning Backup for Google Apps
Product Type(s): Software-as-a-service backup software
Link to website: www.spanning.com
Link to Data Sheet: Spanning Backup Product Line Overview

Description of Product/Technology: Spanning is a software-as-a-service company that provides backup and recovery tools for Salesforce and Google Apps. The company has two products, Spanning Backup for Salesforce and Spanning Backup for Google Apps, as well as a few free tools for Google Apps. The next product, Spanning Backup for Microsoft Office 365 will be available in Q1 2015.

Spanning Backup for Salesforce: This software, delivered to the customer as a service, automatically backs up all critical customer data and configurations in Salesforce, including standard and custom objects, files, attachments and the "metadata" (configurations), such as dashboards, reports, custom views and email templates. The service also backs up applications built on the Force.com platform, both custom applications and 3rd party applications installed from the Salesforce AppExchange marketplace.



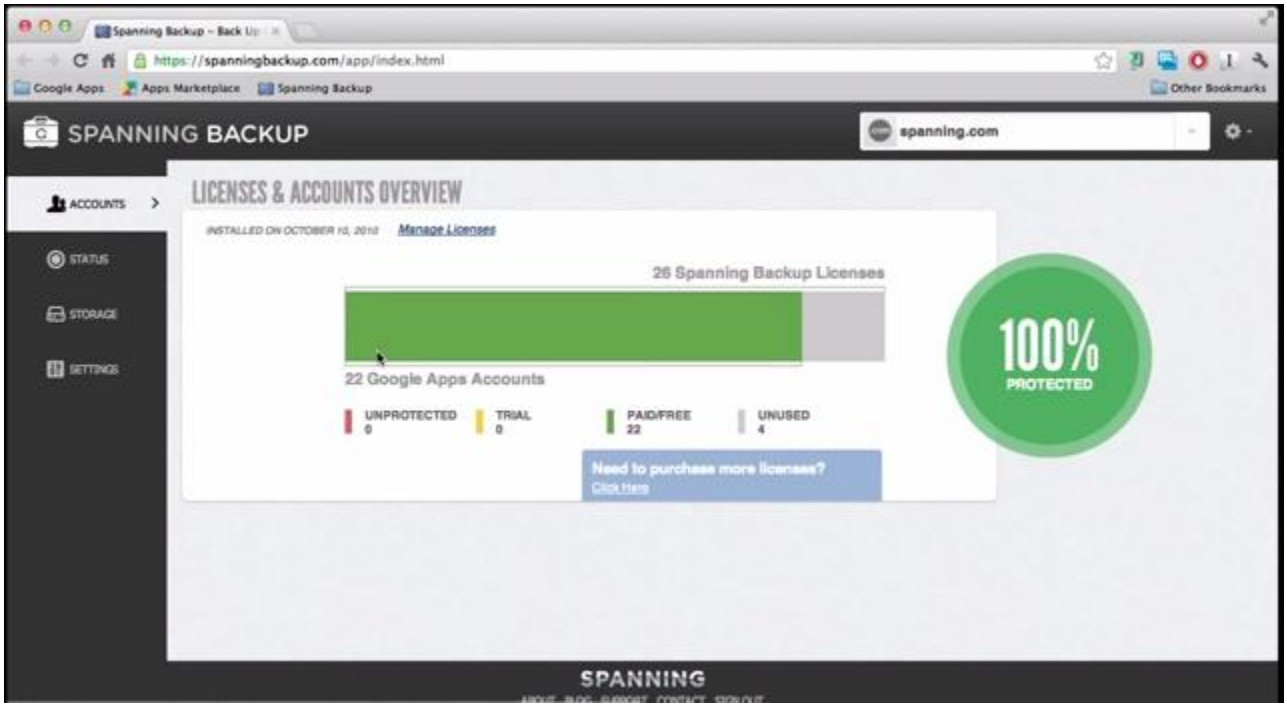
Backups include on-demand and daily, automated backups. Admins have full visibility into the status of the backup processes and are kept informed through interactive Chatter posts and a Salesforce1 mobile application. Admins can also monitor all activity and the number of API calls made each day.

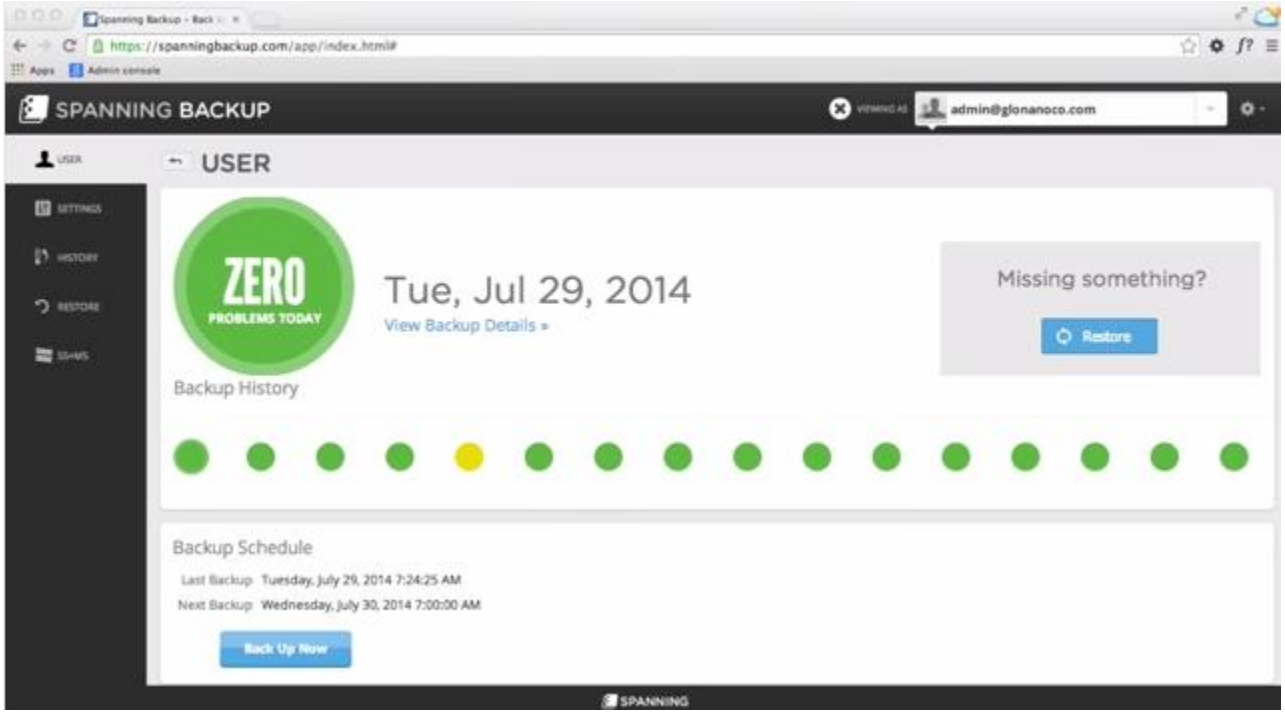
Administrators and optionally end-users can perform on-page restores of Salesforce records from any previous point-in-time. The granular field-level restores allow the user to select and compare individual fields, such as phone number or opportunity amount and also to restore attachments that were previously part of the record. Since all restores are performed as the user who is logged in, field-level security is maintained, allowing them to only restore data they can normally edit.

Backup for Google Apps: This software, delivered to the customer as a service, automatically backs up Google Apps, such as Gmail, Drive, Calendar, Contacts and Sites. Data, including previous versions, document directory structure, nested folders, site structure and sharing and permissions settings, can be backed up and recovered in or to its original state.

Emails can be searched for date, label, sender or subject line, and restored. All backed up data, such as files, email, calendar entries, etc., can be exported into standard file formats and downloaded. Finally, admins can restore emails, files and folders into other accounts to transfer former employee emails to new or existing users.

Data backups run automatically on a daily basis and can also be initiated on-demand at any time. On-demand backups can also be initiated at any time. From the dashboard, the Google Apps Administrator can also select the contents of the backup -- specific applications, mail labels, calendars and contact groups. From the Spanning Backup application, the Google Apps administrator can prevent or allow user modifications to backup settings.


Spanning Backup - Back Up
https://spanningbackup.com/app/index.html
Google Apps
Apps Marketplace
Spanning Backup
Other Bookmarks
SPANNING BACKUP
spanning.com
ACCOUNTS
STATUS
STORAGE
SETTINGS
LICENSES & ACCOUNTS OVERVIEW
INSTALLED ON OCTOBER 10, 2013
Manage Licenses
26 Spanning Backup Licenses
22 Google Apps Accounts
UNPROTECTED 0
TRIAL 0
PAID/FREE 22
UNUSED 4
100% PROTECTED
Need to purchase more licenses?
Click Here
SPANNING


https://spanningbackup.com/app/index.html#
Apps
Admin console
SPANNING BACKUP
admin@glonanoco.com
USER
USER
SETTINGS
HISTORY
RESTORE
SLAMS
ZERO
PROBLEMS TODAY
Tue, Jul 29, 2014
View Backup Details »
Missing something?
Restore
Backup History
Backup Schedule
Last Backup Tuesday, July 29, 2014 7:24:25 AM
Next Backup Wednesday, July 30, 2014 7:00:00 AM
Back Up Now
SPANNING

The admin can also manage software licenses at the organization or individual user level. In addition, the Spanning admin can set email retention policies for entire domains, monitor and resolve backup errors and maintain a detailed record of all admin actions for compliance purposes. The admin can also automatically assign Spanning Backup licenses to new users and set email notification frequency preferences for backup status. Finally, Spanning Backup for Google Apps can be integrated into onboarding and provisioning processes by leveraging user management and export APIs.

Spanning Backup for Google Apps is sold through a network of resellers or direct from the Google Apps Marketplace. The company gives all its customers a 100% Restore Guarantee, that gives the 10x their money back for one year on the individual account for which Spanning lost data or was not able to restore data.

Security: Spanning uses the Amazon Web Services (AWS) cloud to host their service. Data that is backed up to AWS is protected there by 256-bit AES encryption with unique keys for every object and a master key that protects the unique keys. Data is protected in transit to or from the applications and AWS is protected with Secure Socket Layer (SSL) encryption.

Free Google Apps Admin Tools:

In addition to the subscriber offerings, Spanning also offers several tools that are free for user use. The applications are:

- Mobile Audit Log for Google Apps, which is a mobile version of the Admin Audit Log Viewer, and allows monitoring of domains by enabling push notifications of changes;
- Undelete for Google Calendar, which contrary to popular opinion, lets users restore their Google Calendars, with full details;
- Stats for Google Drive, which notifies the admin of how users and companies are using Google Drive; and,
- Admin Audit Log Viewer for Google Apps, which allows admins to monitor changes to domain settings, review a history of admin dashboard actions and audit other admin action with specific you domain.

These free apps are available on the Google Apps Marketplace, Apple App Store and the Google Play Store.

Corporate: Spanning Cloud Apps was founded in 2010 and was recently acquired by EMC Corporation. The company will continue to operate under the Spanning Cloud Apps brand and will be the foundation of EMC's "born-in-the-cloud" data protection strategy in its Core Technologies Division. The company has 50 employees and is located in Austin, TX. At present, Spanning is led by Jeff Erramouspe, serving as CEO and president. He was formerly the CEO and founder of DeepFile (now StoredIQ, an IBM Company).

StorageStrategies NOW

Outlook Report

Use Case Profile

VIF international education

Company Name: VIF International Education

Company Type: A teaching exchange program

Location: Chapel Hill, North Carolina

Products/Services: Global education programs including professional development and curriculum, language acquisition and cultural exchange programs

Contact name: Arne Plum, Data Applications Specialist

Challenge:

- 85 employees use Salesforce and Google Apps to store private and sensitive information on the 600 teachers and 20,000 applicants in the program.
- Replaced custom database with Salesforce. Salesforce doesn't have a daily backup or built-in restore feature.
- Security of data an issue because the information in Salesforce is private and sensitive personal information.
- Migration from Microsoft Exchange to Google Apps. Use Google Drive for file sharing. Manual exports of data from Google Apps for backup are hard to keep track of.
- Concerned about privacy of data in the cloud.

Solution:

- Deployed Spanning Backup for Salesforce and Spanning Backup for Google Apps.

ROI/Benefits:

- "With Spanning Backup in place, we have complete visibility into any data quality issues and can quickly resolve them, allowing us to be completely confident that our data is being backed up and available should we ever experience a data loss event. Spanning gives the executive team the peace of mind that our data is safe and secure."

- “Spanning also has much tighter integration with Salesforce. We love being able to review the status of our backups straight from Salesforce, the Chatter functionality, and especially the individual record restore feature.”

- “Having a backup solution in the cloud is important for us because we handle a large amount of information for our teachers. We really can’t afford to lose that information.”

- “In the past, we spent so much time tracking backups, checking file statuses, having to track down backups, check status, file support capability. We haven’t had a surprise since we started using Spanning Backup for Salesforce.”

- Spanning Backup for Salesforce and Google Apps stores data in SSAE 16 Type II-certified datacenters. Data is encrypted during transit and at rest.

Our Take

The compelling value offered by SaaS applications continues to attract companies of all sizes to the world of cloud-based hosted applications. Unfortunately, many companies currently using SaaS applications in production—or considering such use—are not aware of the limitations of the backup and restore capabilities of SaaS providers. Shockingly, some SaaS providers provide no customer-facing backup configuration options and restore capabilities, while some provide limited configuration and restore options, yet the cost and time required to recover deleted data remains untenable and impractical.

Fortunately, the ubiquitous natures of access to SaaS applications lends itself perfectly to a cloud-based backup and restore architecture, allowing your employees to focus on generating revenue instead of the tedious tasks of managing backups and restores of SaaS data. SaaS backups are also an important part of any corporate disaster recovery plan. Considering existing Sarbanes-Oxley requirements, as well as other corporate compliance and governance regulations, the ability to back up, retrieve and archive SaaS data is not just a good idea, in many cases such capabilities are required by law if your SaaS applications contain compliance-related data. We feel strongly enough about the importance and value proposition of SaaS backup and restore software that we cannot imagine that any responsible company would implement SaaS applications without a comprehensive backup and restore strategy in place.

Appendix 1: SaaS Provider backup and recovery policies

	SaaS Provider Backup policy	SaaS Provider Recovery policy	User-initiated backup process	User-initiated recovery process
Google Apps	Data is replicated multiple times across active clustered servers. It is also replicated to a secondary data center.	Data is unrecoverable once an administrator or user deletes an account.	Users can export .CSV files and other files manually, but admins cannot	
Microsoft Office 365	Microsoft maintains multiple copies of your data, across data centers, for redundancy. Exchange Online uses the Exchange 2010 feature known as Database Availability Groups to replicate Exchange Online mailboxes to multiple databases in separate Microsoft data centers.	Not disclosed.	Users can export .CSV, .PST and Word files manually.	Users can restore items that have been deleted from any email folder. When an Exchange Online mailbox is deleted, its contents are recoverable for 30 days using the Exchange Control Panel. The mailbox contains all of the data stored in it at the time it was deleted. After 30 days, it is not recoverable.
Salesforce	Data is backed up nightly to a tape library. Tapes are then cloned to a secondary location to verify their integrity and stored in a fire-proof off-site location.	Salesforce will recover data for customers at a minimum of $10,000 per instance. The recovery takes 15 business days.	User can manually export .CSV files every 6 or 28 days. Automatic generation of .CSV files occurs weekly or monthly.	Manual process via Data Loader function in Salesforce. Integrations are difficult to restore.
Facebook	Facebook is based on a MySQL database. Data in the form of binary logs is backed up in real-time to rack backup servers. Facebook also does traditional (mysqldump) backups. After backup, data is copied to a Hadoop cluster and distributed to a separate region.	Data is continually restored from the Hadoop cluster, verified for integrity and alarms are generated if there are any repeatable problems.		
Twitter	Not disclosed.	After a user deletes their Twitter account, recovery is impossible.	Each individual user needs to manually download their Twitter archive through the Settings function.	