backupify™

# HOW TO SELECT A BACKUP SERVICE FOR CLOUD APPLICATION DATA

JUNE 2012

## INTRODUCTION

The use of cloud application providers or Software-as-a-Service (SaaS) applications is growing rapidly. Many organizations are finding that the low capital and support requirements make SaaS an attractive alternative to on-premise systems, but few are willing to give up the IT “best practices” they have developed over the years, including the need for backing up critical data. As a result many organizations are evaluating backup services to future protect their SaaS applications.

The goal of this document is to assist your organization in evaluating potential solutions for backing up your Software-as-a-Service (SaaS) applications. It provides a suggested methodology as well as an example evaluation matrix.

## WHY BACKUP CLOUD DATA?

If you are reviewing this document you may have already decided to backup your cloud application data. However if you are still considering whether a backup service is necessary, a quick summary is provided below. A more complete analysis is provided in Backupify's "The Business Case for Google Apps Backup", available at www.backupify.com.

Data loss is generally caused by one of five factors:

1. Hardware failure
2. Natural disaster
3. User error
4. Software corruption
5. Malware & viruses

SaaS providers are able to protect very well against hardware failure and natural disasters through data center provisioning and management. However, user error, software corruption and malware & viruses are largely outside of the control of SaaS solutions. For example, the IT Policy Compliance Group suggests that 75 percent of all data loss is due to user error while Gartner surveys (cited by the SANS Institute) put 32 percent of data losses down to user error.

All five of the risk factors above can be mitigated through the use of a backup service.

## EVALUATION OVERVIEW

Most organizations follow a simple process for selecting an IT solution:

1. Align the organization and stakeholders around the need for a solution.
2. Identify the organization's key requirements.
3. Identify vendors to be screened.
4. Rate each solution based on screening criteria and identify candidates for Proof of Concept.
5. Take one or more vendors through an in-depth Proof of Concept and score each solution.
6. Select a vendor and roll out the solution.

This process can take from days to years depending on the needs of the organization, the complexity of the solution, and the urgency of the requirements. The timeframe for selecting a SaaS backup provider generally ranges from two weeks to two months.

## ALIGNING THE ORGANIZATION

Before beginning any IT solution selection, it is important to ensure that all the key stakeholders in the organization are aligned on why the solution is important. The "why" will drive the type of requirements, the timeline, and the types of vendors selected for evaluation.

For a SaaS backup solution the stakeholders typically include:

| Stakeholder | Key Concerns |
|---|---|
| CIO | • Ensure that organization's IT strategy (cloud, on-premise, hybrid) supports the enterprise business objectives.<br>• Minimize risk to organization while maximizing value IT systems provide. |
| IT organization | • Ensure that the level of support that end-users receive is not compromised by move to SaaS provider.<br>• Ensure that the risk of data loss is minimized.<br>• Provide service in cost-effective and efficient manner.<br>• Ensure the organization's Restore Point Objectives and Restore Time Objectives can be met. |
| Finance organization | • Comply with relevant document retention and archiving requirements. |
| End-users | • Enjoy the same level of data protection and convenience that they had in an on-premise environment. |

Before evaluating any IT solution, it is helpful to confirm that all of these stakeholders are consulted to ensure their needs are included in the evaluation process.

## IDENTIFY KEY REQUIREMENTS

After consulting the stakeholders listed above, the evaluator should draw up a list of requirements. Typically these requirements fall into several categories.

1. Vendor qualifications – Size, financial resources, technical expertise, experience with similar customers.
2. Technical requirements – Specific features the organization has identified as critical to a solution.
3. Use cases – Evaluation of the solution against specific use cases.
4. Affordability – The cost of the system, as well as the cost of any training or associated services.

Most organizations will divide these requirements into a screening set and a Proof of Concept (POC) set. The screening criteria can be applied without in-depth evaluation of the product; for example, by reviewing vendor websites and online reviews. The POC requirements demand engagement with the vendor and detailed examination of the solution.

## IDENTIFY VENDORS

Given that SaaS solutions are relatively new to the market, the number of SaaS backup providers is not vast. There are several ways to identify potential vendors.

- Ask a colleague – Other IT professionals may have experience with moving key data to the cloud and may have had similar needs around data backup.
- Look in an "app marketplace" – Some SaaS solutions, like Google Apps and Salesforce, sponsor app marketplaces where vendors of complementary product can list their wares.
- Ask the SaaS provider – your SaaS sales rep may be aware of backup solutions and may be able to recommend a provider they have worked with before.
- Consult online blogs / magazines – Online resources like *CIO Magazine*, *eWeek*, *Computerworld*, and *CSO Online* have written reviews of SaaS backup providers.

## SCREEN VENDORS

Depending on the number of vendors you have identified and the time you plan to invest in the evaluation process, you may wish to screen the vendor list down to one or two candidates before you start a POC. Many organizations will screen on criteria such as:

- Does the vendor support the SaaS applications you depend on? Obviously if a vendor doesn't support any of your SaaS apps you won't be evaluating them.
- Does the vendor have a proven track record? Given that reliability is a key attribute of a backup provider, you may choose to screen out vendors who are relatively new. You may be able to use public metrics on their number of

customers, amount of data stored and so on to evaluate a vendor's track record. If a vendor has a history of data losses, this should be considered.

- Does the vendor offer the basic features you need? You should be able to determine from the vendor's website what basic features they offer. If you need the ability to export a file and it isn't available, you may choose to eliminate that vendor without a full evaluation. Bear in mind, though, that most vendors do not attempt to list all features on their website. When in doubt, reach out to a sales representative. A list of suggested features can be found in Attachment A.
- Does the vendor offer acceptable support? When you have a problem with backup, you will likely need an answer quickly. You may choose to screen out vendors who don't offer access to a support representative, or whose support is based overseas. One way to evaluate the quality of support is to look for a written Service Level Agreement (SLA).

Once you have established your screening criteria you can use it to narrow the list of providers down to one or two for the Proof of Concept.

## EXECUTE PROOF OF CONCEPT

Now that you have narrowed the list to a few vendors you're ready to start a Proof of Concept. During this phase you'll get "hands on" with the product and ensure that it meets the needs of your organization.

### SELECT YOUR EVALUATORS

You may decide to have only one person evaluate the product or you may decide to enlist several evaluators to guarantee all stakeholder needs are met. If you will be working with a team, it's a good idea to have a kickoff meeting to confirm that everyone has the same expectations and will use the same framework, then a wrap up to discuss the results. If only one person will be doing the evaluation you won't need these meetings.

### CONDUCT THE PROOF OF CONCEPT

Most SaaS backup providers offer a trial of about two weeks, during which you can evaluate the product on your production system with no commitment. Because backup tends to be a "set it and forget it" product, it's important to go in with a specific evaluation plan so you can ensure that the product meets your needs for all the use cases you can think of. The criteria fall into three areas:

- Commercial – Does the vendor's business meet your requirements in terms of customer support and service commitments? Although you don't need a POC to gather this information, this is typically the phase when it makes sense to dive into the company's qualifications.
- Technical – How does the product rate on key features?
- Use Cases – How well does the product support your key use cases?

A list of common evaluation criteria is provided in Attachment A. Each criterion is evaluated on a 0-3 scale.

## SELECT A VENDOR

After you've completed the POC you'll be able to rate each provider on their business strength, technical features, and support for your use cases. If you have found that one vendor scores substantially above the others, you are ready to move forward and finalize your selection. In some cases, there may be two additional steps to take before selection.

### TALK TO A REFERENCE

Depending on your organization's process, you may want to speak to a reference customer. Bear in mind that for smaller organizations it may not be feasible for the vendor to provide a live reference – you may be able to depend on case studies and references posted on the vendor's website. For large organizations, a solutions provider should be able to put you in contact with a relevant customer. Ask that customer:

- Has the vendor delivered on their SLA and promises?
- Has the product worked as promised?
- Would they recommend the vendor to others?

### UNDERSTAND THE ROADMAP

If you've found that no single vendor meets all of your needs, you may need to engage with the solution provider to understand their plans for the future. Again, this is more feasible for large organizations than smaller ones. If you have hundreds or thousands of users, it's reasonable to ask the vendor to help you understand how their organization plans to grow in the future. Ask to speak to someone in the product management or product marketing organizations and find out:

- What features do they plan to add over the next six months?
- What features have they added recently?
- Do they plan to support other SaaS applications?

This may help you understand how the organization intends to expand. Bear in mind that the vendor may not be able to commit to releasing specific features at specific times, but they should be able to articulate the process by which they evaluate and implement new features.

### FINALIZE THE DECISION

Once you've evaluated the product and had all your questions answered, you're ready to make a decision. Make sure your stakeholders have "come along on the journey" – validate that their concerns have been addressed and that they support the decision. This will make the implementation go more smoothly.

## CONCLUSION

A SaaS backup solution ensures that your organization maintains best practices for data protection and control even as you move data to the cloud. Selecting the right vendor will protect your SaaS data from user error, malicious attacks and data corruption. Following a clear evaluation process will ensure that your organization makes the right decision in a timely and inclusive manner.

## ABOUT BACKUPIFY

Backupify is the leading backup provider for cloud application data, offering an all-in-one archiving, search and restore solution for the most popular online services including Google Apps, Salesforce, Facebook, Twitter and more. Backupify ensures that companies can access and control the data they entrust to these systems and prevents data loss from external threats, user error or service failure. Backupify was founded in 2008 and is based in Cambridge, Massachusetts.

### FIND OUT MORE

If you're interested in the peace of mind you get from an automated Google Apps backup solution, feel free to contact us directly at info@backupify.com.

- Web http://www.backupify.com
- Phone 1.800.571.4984
- Twitter http://twitter.com/backupify



backupify™

# ATTACHMENT A – SAMPLE EVALUATION MATRIX

Instructions: Score each attribute 0-3 for each vendor.

0 = Not present or not acceptable
1 = Partially present or planned
2 = Satisfies most of requirement
3 = Satisfies all of requirement

| Area | Topic | Description | Score (0-3) |
|---|---|---|---|
| Business | Experience | The company should have experience backing up the type of data you are protecting. | |
| Business | Documented Security Procedures | A backup provider should offer documented security procedures for the transfer and protection of your data. It's not enough to claim to be "secure;" your SaaS backup provider should be prepared to give reasonable specifics – such as the level of encryption of data at rest, and which data transactions occur over SSL -- to assure the safety of your data. | |
| Business | Documented Support Options | A cloud application is only as good as its technical support, and this goes doubly so for SaaS backup services, as you'll be relying on your backups to function during times of need. Your SaaS backup solution should have a clear method for contacting technical support *and* self-service support options (like FAQs and help forums) so you can work towards solving problems on your own, without waiting on a response from the service provider. It's not either-or, it's both. | |
| Business | Documented Service Level Agreement | Just as you wouldn't purchase a SaaS product or cloud application without a documented Service Level Agreement, the system backing up your cloud apps should also have an SLA. Specifically, the SLA should spell out explicit guarantees around the level of backup provided and the compensation provided if those guarantees aren't met. This is very different from simply promising website uptime. | |
| Business | Flexible Billing | Your SaaS backup solution should offer as much contract flexibility as the service it's backing up. It should fit into your existing buying and budget cycle, not force another one on you. | |

| Area | Topic | Description | Score (0-3) |
|---|---|---|---|
| Business | Viability of Vendor | The provider should be able to present a convincing case of financial health, including size and revenues, as well as either being profitable or having the support of significant investors. | |
| Business | Cost of Solution | Is the cost of the solution competitive with other providers, taking into account the value of the product? | |
| Feature | Applications Supported | The vendor should support the applications you wish to protect - some providers only support certain Google Apps services for example. | |
| Feature | Comprehensive Data Backup (AKA "Complete Suite" Backup) | Many SaaS backup products only backup a portion of the data in your cloud application, often leaving out certain feature sets (backing up text but not images, documents but not emails) or ignoring key metadata (emails but not attachments; documents but not their tags and access control lists, etc.). Your cloud application backup should protect every data type necessary to keep your SaaS solution running with full data integrity. | |
| Feature | Prevention of Backup Deletion | A user should not be able to disable the backup process, exclude items or folders from backup, or delete backups. The provider's support team should have a defined process for validating any admin request for deletion. | |
| Feature | Backup Historical and Progressive Data | A backup solution should protect all the data in your system, not just the data that's added after you install the backup. | |
| Feature | Data Versioning (Incremental Backups) | Backing up just the most recent version of SaaS data means that -- if you don't catch an error before your backup archive updates -- you have two copies of *corrupted* data. Data versioning means you have multiple copies of the same data elements, each captured at regular intervals, allowing you to roll back to whichever state has the most accurate or necessary data. | |
| Feature | Local Export Options | Data trapped in your cloud application should not be equally trapped in your cloud application backup. Your SaaS backup provider should offer local download and export options so you can keep local copies of any items (or even accounts) you deem fit. | |

| Area | Topic | Description | Score (0-3) |
|---|---|---|---|
| Feature | Scheduled *and* User-Initiated Backups | Regular, scheduled, automated backups ensure that no critical data is omitted from your archives simply because an administrator forgot to trigger a backup. Conversely, user-initiated backups ensure that, following a critical update to live SaaS data, the backup archive can be immediately updated to ensure this data is protected. A competent backup system should offer both features, rather than simply one or the other. | |
| Feature | Proactive Status Updates and Error Notification | Backup administrators shouldn't have to log into a backup system -- let alone individual backup accounts -- to learn whether a backup process has been successful. The backup application should proactively alert admins to backup failures and, ideally, allow an admin to diagnose and correct the problem as soon as possible from a central interface. | |
| Feature | Support for Your Recovery-Time Objectives (RTOs) | It's not enough for a cloud application backup to restore data; it must restore data fast enough that your business isn't significantly harmed by data loss. How long does it take to restore one item, one account, or the complete data archive? Know the answer before you deploy your SaaS backup solution. | |
| Feature | Restore for Individual Items | Rarely is all the data corrupted or erased from a cloud application; a typical data loss scenario involves only a handful of missing or damaged items. Your SaaS backup solution should allow you to restore just those items -- the mail your user accidentally erased, or the single table your database dropped -- rather than deal with reinserting a complete copy of your entire account (or archive) back into your cloud application. | |
| Feature | System-Wide Search | Most restoration tasks involve single items, so your SaaS backup solution should make it easy to find those individual items within your archives -- and that requires system-wide search. Manually browsing chronological archives can significantly slow down restore efforts, and search is a must-have shortcut to ensure your Restore-Time Objectives are met. | |
| Feature | Centralized Account Management | Administrators should be able to view backups and archives for all accounts through a single interface, so that as your business grows and you add new employees, account administration stays fast and efficient. | |

| Area | Topic | Description | Score (0-3) |
|---|---|---|---|
| Feature | Robust Permission Controls | Administrators should be able to monitor and control what features their users can enable, disable or configure. Backups do you no good if end users can prevent or delete them without administrator knowledge or consent. | |
| Feature | Streamlined, Versatile Onboarding | A backup solution should allow administrators to quickly opt-in which user accounts to include in the backup archives. Mandatory backups for all accounts are unacceptable, as is a tedious, manual selection process. The SaaS backup solution should also allow for new SaaS application users to automatically be backed up. | |
| Feature | Configurable Retention Period | Some organizations may require documents to only be retained for certain periods of time. The backup provider should enable these retention policies. | |
| Use case | Admin Restore | User loses a specific known document, admin restores to original location. | |
| Use case | User Restore | User loses a specific known document, able to restore to original location without admin help. | |
| Use case | Search and Restore | User loses a file, name roughly known and last edit date known. Admin restores to original location. | |
| Use case | Employee Departure | User departing company, admin exports all data so account can be shut down. | |
| Use case | Service Offline | SaaS service is offline, user needs a document. Admin exports document in alternative format and emails to user. User opens document using alternative application. | |
| Use case | Restore Deleted Account | Employee leaves under unpleasant circumstances and deletes entire account, entire account needs to be restored or downloaded for another employee. | |
| Use case | Restore Shared Document | Group of employees are working on a project together and one of them no longer believes a shared document is useful, it is deleted and the other members of the project need to restore it. | |
| Use case | Transfer Data To New Employee | User is leaving organization and replacement needs access to contacts and documents. Data must be exported and uploaded to new account. | |
| Use case | Restore Calendar | Calendar gets corrupted, admin restores old version of calendar from known date. | |

| Area | Topic | Description | Score (0-3) |
|---|---|---|---|
| Use case | Restore Calendar | Calendar gets corrupted, admin restores old version of calendar from known date | |