Solution Brief

A Checklist when Choosing a Backup Solution for SaaS-based Applications

Date: January 2015 **Authors:** Jason Buffington, Senior Analyst; and Monya Keane, Research Analyst

Abstract: *What should organizations look for in a SaaS protection solution? That question is spurring new conversations between traditional backup admins and their counterpart DBAs, vAdmins, file/storage managers, and now, SaaS admins. Here are some of the realities those IT managers are discovering when it comes to SaaS application adoption as a whole … and SaaS-based data protection in particular.*

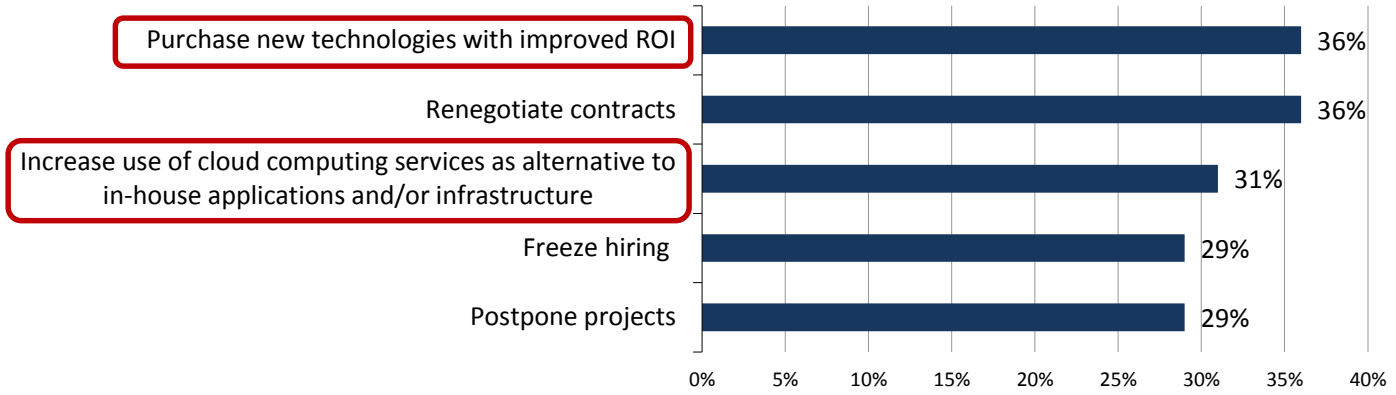
Introduction

For many information technology professionals, "IT transformation" means going to the cloud—*for better production and better protection*.

Cost control is one reason that the cloud holds great appeal: ESG research shows that cost containment is a top driver for IT strategic decisions overall,[1] and when ESG asked respondents how their IT organizations intended to reduce the costs, increased usage of cloud services was a frequently mentioned reply (see Figure 1). Even more common was the response that their organizations would invest in new technologies that deliver better ROI which, in many cases, points again to the use of cloud services.

Figure 1. Top Five Measures that Organizations Are Taking to Reduce or Contain IT Expenditures

Which of the following measures – if any – is your organization taking to reduce or otherwise contain IT expenditures? (Percent of respondents, N=562, multiple responses accepted)



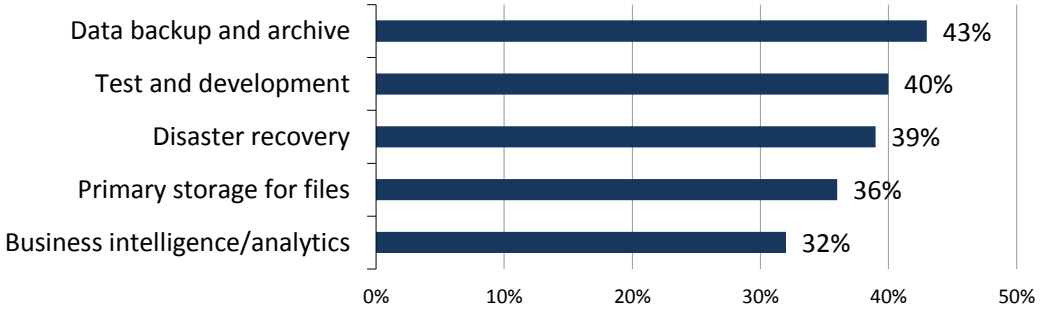
Source: Enterprise Strategy Group, 2015.

ESG also conducted research on actual intended usage scenarios among IT organizations investigating cloud infrastructure services. Data backup and archiving and disaster recovery were two of the top three responses provided by organizations surveyed (see Figure 2).[2]

[1] Source: ESG Research Report, *2014 IT Spending Intentions Survey*, February 2014.
[2] Source: ESG Research Report, *2014 Public Cloud Computing Trends*, March 2014.

Figure 2. Top Five IT Workloads Moving to the Cloud

For which of the following purposes does/did your organization use cloud infrastructure services? (Percent of respondents, N=256, multiple responses accepted)

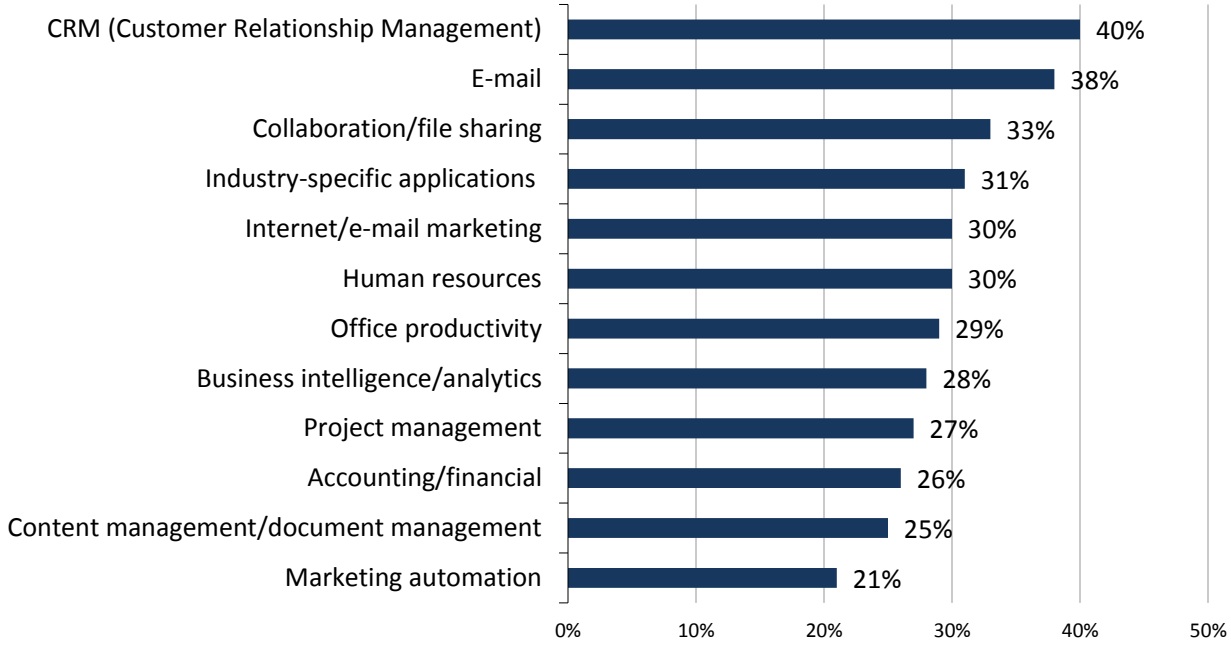


Source: Enterprise Strategy Group, 2015.

In addition to the cloud-for-backup trend, a similar transformation is occurring in regard to moving specific *production-centric* IT workloads offsite. As Figure 3 shows, many workloads that historically were data center delivered now live on software-as-a-service (SaaS) infrastructures instead.[3] Almost certainly, the shift reflects the appeal of Microsoft Office 365, Salesforce.com, Google Apps, and other mainstream SaaS-based solutions that are so popular today.

Figure 3. Specific Applications for Which Organizations Leverage Software-as-a-Service (SaaS)

You have indicated that your organization is currently using software-as-a-service (SaaS). What specific applications has your organization currently deployed via a SaaS model? (Percent of respondents, N=354, multiple responses accepted)



Source: Enterprise Strategy Group, 2015.

[3] Source: ESG Research Report, *2014 IT Spending Intentions Survey*, February 2014.

Successfully Moving to the Cloud Requires a Good Partnership

One of the nicest evolutions supporting IT productivity today is improved collaboration—particularly between workload owners (who understand the protection/recovery requirements of their own applications) and data protection specialists (who understand the overall business's mandates and policies for data protection, preservation, and availability).

The increased partnering is spurring new conversations between traditional backup admins and their counterpart DBAs, vAdmins, file/storage managers, and now, SaaS admins. Here's what they should discuss and realize.

Backup Admins Need to Understand Three Realities Related to SaaS Adoption

- **Backup reality one:** Corporate data must be protected, regardless of whether it lives onsite, in a laptop, or in a cloud. This is data that the organization relies on. Its protection must be ensured.
- **Backup reality two:** Almost *no* legacy data protection solution can back up SaaS-stored data. In much the same way that many physical-server backup solutions were late to the game in being able to protect virtual machines, most protection solutions built for data center use are now late in offering protection for SaaS workloads. You need to assess how "modern" your current data protection processes are, immediately.
- **Backup reality three:** The best place to protect most cloud-native data is to another cloud because any secondary data will be relatively unusable unless it is restored back to a cloud. Additionally, both the production SaaS provider and the backup-as-a-service (BaaS) provider likely have much better bandwidth for backups and restores than you do.

SaaS Admins Should Internalize Three Realities of Their Own as They Endeavor to Help Their Organizations Leverage The Agility of Modern SaaS Platforms

- **SaaS reality one:** Backup is almost surely *not* included with your SaaS solution. These platform vendors are focused on availability practically to the exclusion of anything else. Any protection mechanisms in use are there to ensure that the provider meets its SLA obligations. And those mechanisms won't protect you from administrator mistakes or bad/deleted data that was properly put into the system. In full disclosure, some may charge an inordinate amount for a rudimentary ad-hoc recovery mechanism (e.g. SalesForce one-time recovery starts at $10,000US and does not come with a service agreement). Call your SaaS vendor to confirm this reality.
- **SaaS reality two:** Reread reality one, then remember that Salesforce.com, GoogleApps, and Office 365 all fall in the "you must protect yourself" category, period.
- **SaaS reality three:** Your IT team's backup specialist probably already works with his or her peers who run on-premises databases, virtualization hosts, and/or storage platforms. In all cases, those other admins, like you, want some level of control and insight into the ensured recovery of the platform in question. And the backup admin needs to make sure that *all* of the organization's data is protected; so collaborate with them.

Put together, these six realities reveal two mandates and one big problem:

- The first of the two mandates is that the SaaS admin and the backup admin *must* work together.
- The second mandate is that corporate data must be protected, regardless of where it lives—including SaaS data.
- The big problem is that most mainstream data protection solutions are not able to protect SaaS workloads. So, as you evolve beyond your legacy data center servers to SaaS solutions, your legacy backup software is unlikely to follow you.

So, What Should You Be Looking For in SaaS Data Protection?

With that big problem in mind, here are several questions to ask as you evaluate SaaS data protection software:

- **Can your existing backup solution protect SaaS at all?** It seems like a simple yes-or-no question, but the answer will shrink your consideration list quite a bit. Not only do SaaS providers not offer backup or recovery services, most haven't published APIs allowing third-party backup solutions to access/acquire the data. Only very few backup software vendors (who intentionally innovated early) can gain any access to the data at all. The rest, including yours perhaps, just can't back up SaaS.

  In the bigger picture, SaaS providers need to put a higher priority of developing APIs for data protection; because until then, they risk lower adoption and reduced satisfaction with their SaaS offering due to the reduced ability to protect data stored in it. In the meantime, only those few backup innovators that go the extra mile are able to protect SaaS at all—when most legacy solutions simply can't.

- **Who will be managing the protection and the restores?** As mentioned, a working partnership must exist between the person who understands the SaaS service and administers its usage and the person who understands the organization's data protection mandates. The mix of responsibilities may not be 50/50, but both sides must be involved to ensure data is protected and preserved in such a way that user productivity-dependent SLAs are upheld, and data is restorable (for all of the same reasons that onsite backups happen).

- **How long should you keep data?** This is a conversation that the SaaS and backup admins should have. Ensure that the SaaS backup solution can retain data for typical data center retention ranges—maybe 10 years, maybe 90 days. Reasons exist to retain organizational data for long periods, and there are just as many reasons to make sure data isn't retained longer than necessary. Those reasons are well understood by the backup specialist. Meanwhile, the SaaS admin is familiar with the usage of the current data and how new data is ingested into the SaaS platform. Both sets of expertise are needed to achieve the organization's goals, and this process will further help identify which backup solutions can meet the organization's SaaS protection needs.

- **Which UI will you be using to protect SaaS?** A good rule of thumb is, "*Your pane(s) of glass will affect your pain(s) in protection*." Why add yet another lens to monitor/manage? Sometimes niche IT platforms need niche protection mechanisms. But a comprehensive protection solution that can protect the niches (like SaaS for now) can yield significant operational and budgetary benefits during acquisition and ongoing use. Also, if your legacy solution can't adequately protect SaaS, what else is it behind on? Consider revamping your broader data protection strategy to cover the protection of *all* your modern workloads and applications.

- **Where will your data be stored?** Between geo-political boundaries, governmental inquiries, industry regulations and security attacks, understanding where in "the cloud" that your data will actually be stored has never been more important to understand or self-determine. And if the data were to be exposed, as a partial result of where it was stored, is the data readable?

- **Will your data be secure?** Security is a common concern among people considering cloud-based solutions for protection (or production). But when ESG surveyed IT organizations who had already adopted cloud services, *improved security was the most-cited benefit that respondents reported*.[4] Security should improve with cloud solutions; after all, when switching from one data center tool to another, many less-secure access methods exist. But when switching to a cloud platform, all the vulnerabilities are discarded. Well-established cloud backup solutions often have far superior security features, including encryption at-rest for the on-premises copies of data center data, encryption in-flight across the internet, and (of course) encryption within the cloud repository.

- **Will your data be there when you need it?** Since you can't just walk into a SaaS provider's facility to check, are you confident in the reliability of the systems? Are you confident the provider will even be around in five years? The previous checklist questions all involved people in your organization and features of potential products/services. But at the end of the day, you are choosing a "partner" who needs the technical expertise to

[4] Source: ESG Research Report, *Data Protection-as-a-service (DPaaS) Trends*, September 2013.

understand what is necessary to facilitate recovery, the organizational commitment to help you through any calamities that might occur, and the fortitude to assure you that they (and your data) will be there when you need it. Especially when choosing a cloud-based service, the quality of the partner (and their product) is paramount.

One Option To Consider: Asigra

Asigra has been pioneering "BaaS" for more than two decades, before "the cloud" was a term and before "as a service" was understood—specifically delivering backup and recovery software as a service that is delivered by service providers around the world.

Continually broadening what its solution protects, Asigra is one of very few vendors backing up SaaS data at all—and the first "unified" solution to add SaaS platforms such as Salesforce.com, Google Apps, and Office 365 to its onsite, virtual server and endpoint protection and recovery capabilities.

- If you already use Asigra in your data center, then using Asigra v13 (or later) to protect your SaaS platforms is just "adding another workload" to the backup solution you already depend on.
- If you aren't using Asigra, then you have a new reason to look at its solution for comprehensive data protection across the myriad platforms in today's modern IT world.

And considering the question of whether your data will be both available *and* secure, know that ESG Lab validated several versions of Asigra, paying special attention to its security features such as NIST FIPS 140-2 certification. And, because Asigra has been around for many years, it's a safe bet that Asigra will be around for years to come, as well as its growing partner ecosystem. And at any point, if you want to switch to a private cloud architecture, the Asigra architecture enables the flexibility of public, hybrid, and private cloud deployments. So your data will be there for you (and only you) when you need it.

The Bigger Truth

When was the last time that you assessed your organization's retention and recovery needs for *all* of your data: the data on servers … the data on endpoints … and yes, the data in the cloud?

Your SaaS data needs to be protected, but it can't protect itself. As with any modern IT platform, the best protection and most reliable recovery will result from a solid partnership between the application (SaaS) administrator and the IT data protection specialist. Together, they can collectively understand the requirements of the platform and ensure that the data is retained and recoverable according to what the business as a whole requires.

Beyond that "rule," things simply boil down to choosing a comprehensive data protection solution that understands cloud-based SaaS applications (which most don't) and provides the flexibility, manageability, security, and longevity that ensures recoverability of the organization's data. Hopefully, the checklist of questions offered in this brief will help administrators uncover the right answers for their organizations' protection and recovery needs.