Solution Showcase

Best Practices in Cloud-powered Data Protection

Date: December 2016 **Authors:** Jason Buffington, Principal Analyst; and Monya Keane, Senior Research Analyst

Abstract: Backup and disaster recovery represent two of the most frequent uses for cloud storage today, in large part due to the operational agility and appealing cost structure that a secure offsite data repository provides. But protecting organizational data in the cloud is not a one-size-fits-all endeavor. Organizations assessing how to leverage cloud-powered data protection and cloud-enhanced availability should know not only that is cloud *not* a "tape killer," but also that three distinct types of cloud-based data protection services are prevalent today—and each has its own strengths.

Introduction: Why Cloud-powered Data Protection Makes Sense for So Many Organizations

As 2017 approaches, improving data backup and recovery remains a major issue, even a major concern, for many organizations. In fact, IT decision makers surveyed by ESG have been placing backup and recovery among their top-cited priorities year after year.[1]

But other business drivers affecting organizations' IT strategies at the moment are equally important, and those drivers frequently relate to cost control. Expanding cloud usage is the cost-reduction measure most frequently (32%) cited by IT pros, with purchasing technologies with a better return on investment being a commonly mentioned measure as well (30%). Of course, a technology offering a more appealing ROI might be using the cloud to achieve it.

ESG also finds that when it comes to leveraging the cloud in specific ways to support cost-effective IT modernization, data backup/archiving and disaster recovery top the use-case list (see Figure 1).[2]

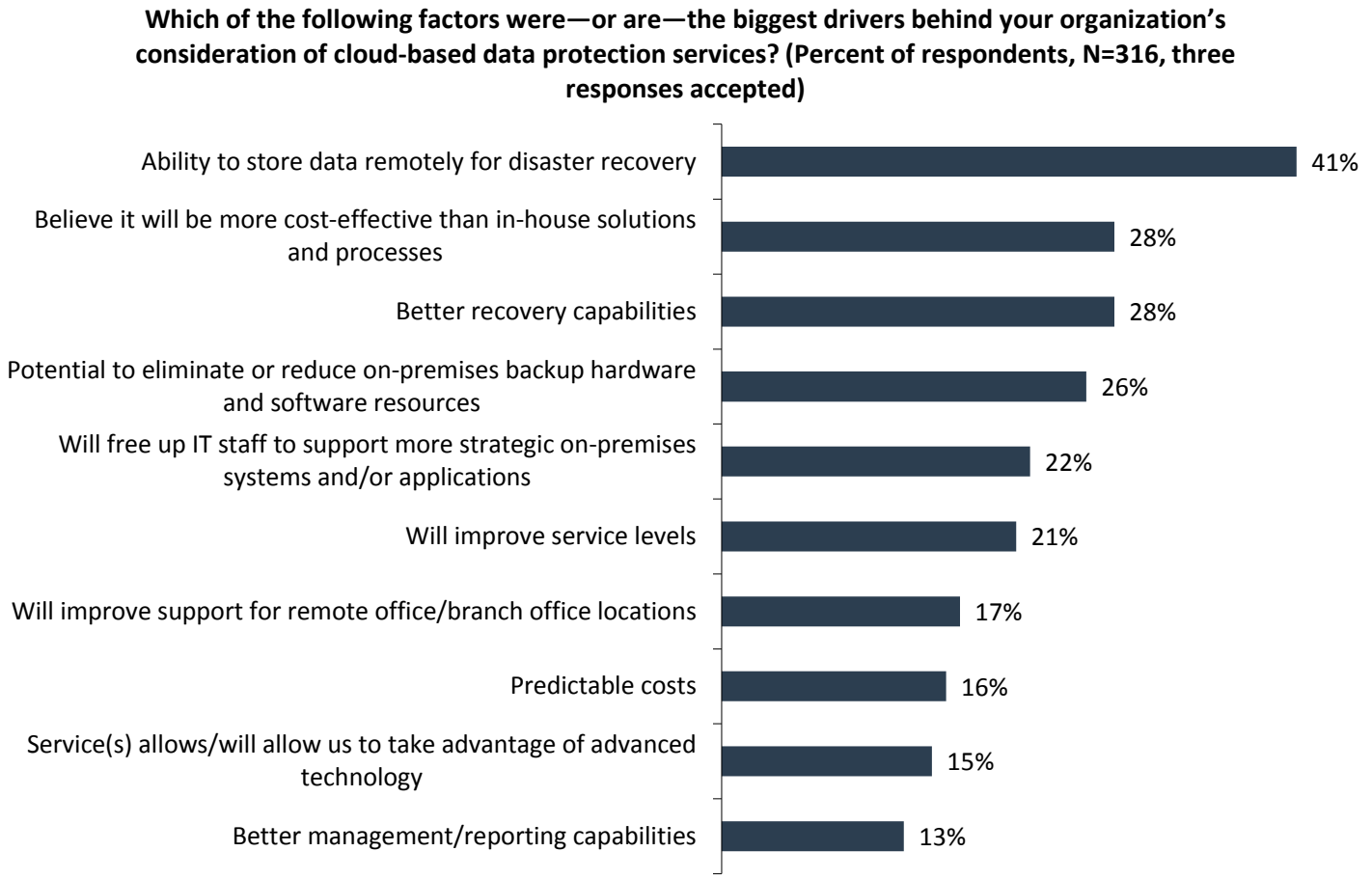
Figure 1. Top Five Cloud Infrastructure Use Cases

Source: Enterprise Strategy Group, 2016

[1] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.
[2] ibid.

Other respondents surveyed recently by ESG confirm that finding, saying their organizations are considering or already using cloud services to support remote data survivability, save money, and enhance their recovery ability (see Figure 2).[3]

Figure 2. Top Ten Drivers of Cloud-related Data Protection



Source: Enterprise Strategy Group, 2016

Is Cloud a Tape Killer?

Many organizations may be considering using cloud-based storage as *simply an alternative to tape* for long-term retention. And although some organizations (mainly small and midsized ones with limited retention requirements) may find that approach satisfactory, larger or more tightly regulated entities should really consider cloud use as a *supplement* to their current disk-plus-tape strategy.

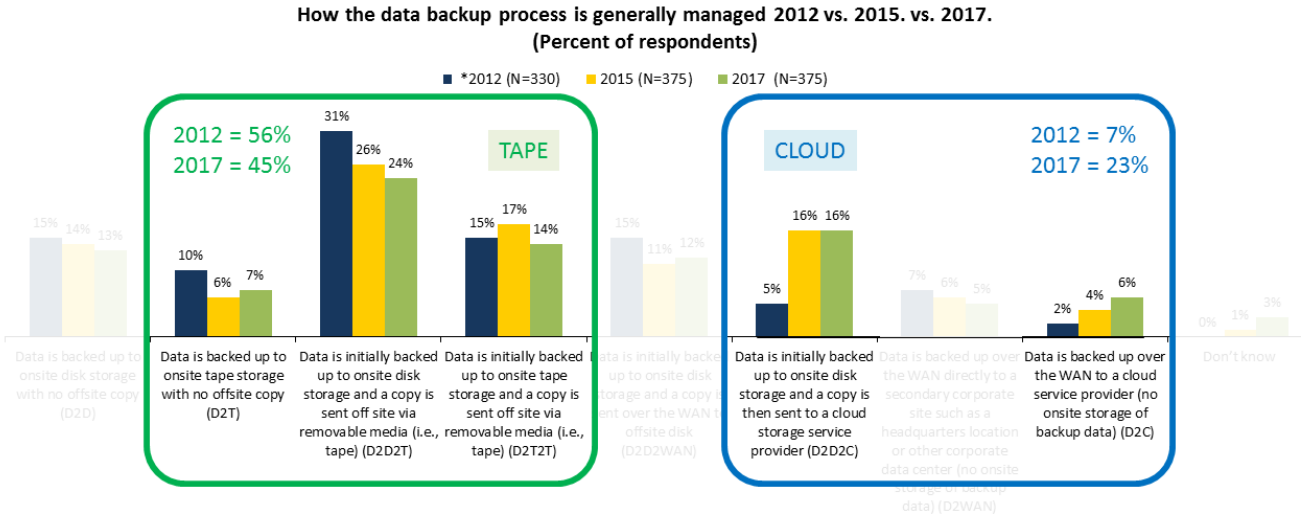
ESG regularly surveys organizations about the media they use to support their data protection efforts, including all permutations of disk, tape, and cloud. Over the five-year span from 2012 to 2017, tape use for primary backup architectures appears to have shrunk from 56% to 45%. Conversely, cloud usage increased from 7% to 23% (see Figure 3).[4]

Essentially, these findings indicate that although cloud usage for data protection is increasing significantly, tape usage is not declining at a corresponding rate.

As part of a data protection strategy, cloud usage continues to increase significantly. But tape use isn't declining at the same rate.

[3] Source: ESG Research Report, *Data Protection Cloud Strategies in 2016*, to be published.
[4] ibid.

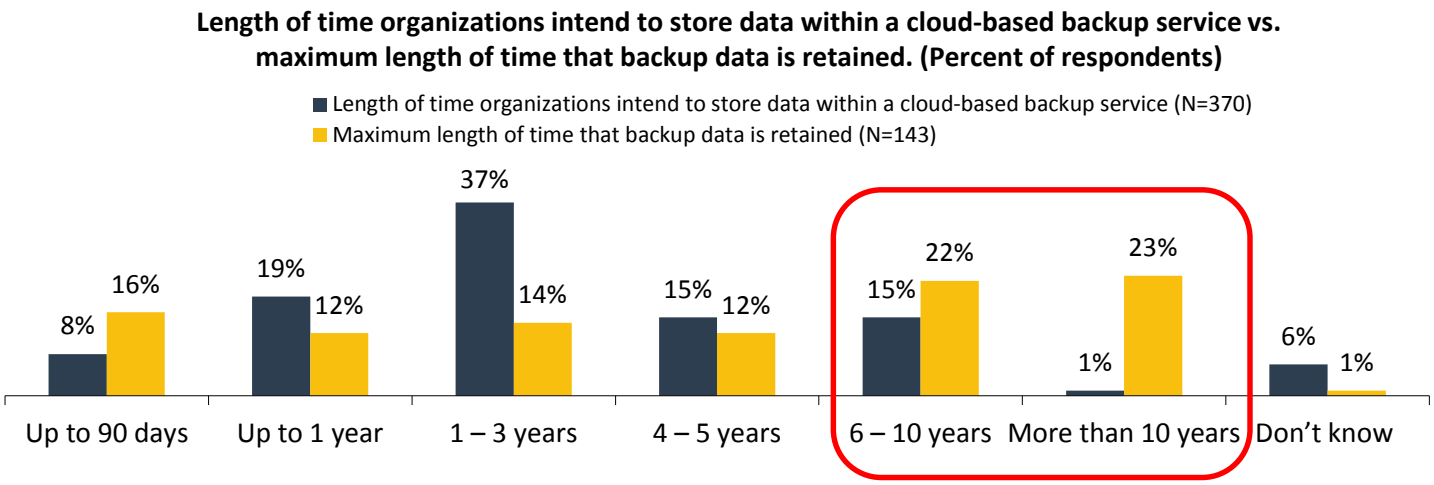
Figure 3. Data Backup Process: 2012 vs. 2015 vs. 2017



Source: Enterprise Strategy Group, 2016

There are several explanations for the persistence of tape in modern data protection. Perhaps the most compelling reason centers on the disparity between how long organizations intend to store data within a cloud and how long those organizations are required to retain long-term data (see Figure 4).[5]

Figure 4. Length of Time Current BaaS Users Plan to Store Data Within a BaaS Service, by Maximum Length of Time Backup Data Is Retained



Source: Enterprise Strategy Group, 2016

As Figure 4 shows, many organizations say that in general, they intend to retain data for *six years or more (often much more)*. However, most of those organizations also say they would store data in the cloud for *three years or less*. The retention discrepancy is a result of two main factors:

- Over time, the cost of cloud as an extended, long-term tier is going to be more variable than tape.
- Warm, cloud-based data offers more operational agility to an organization than cold, tape-based data can. For example, a cloud copy can support better BC/DR preparedness, reporting/analytics, and test/dev enablement. Said another way, the overwhelming value-creation of cloud is not based on lowest price per gigabyte stored, but on the

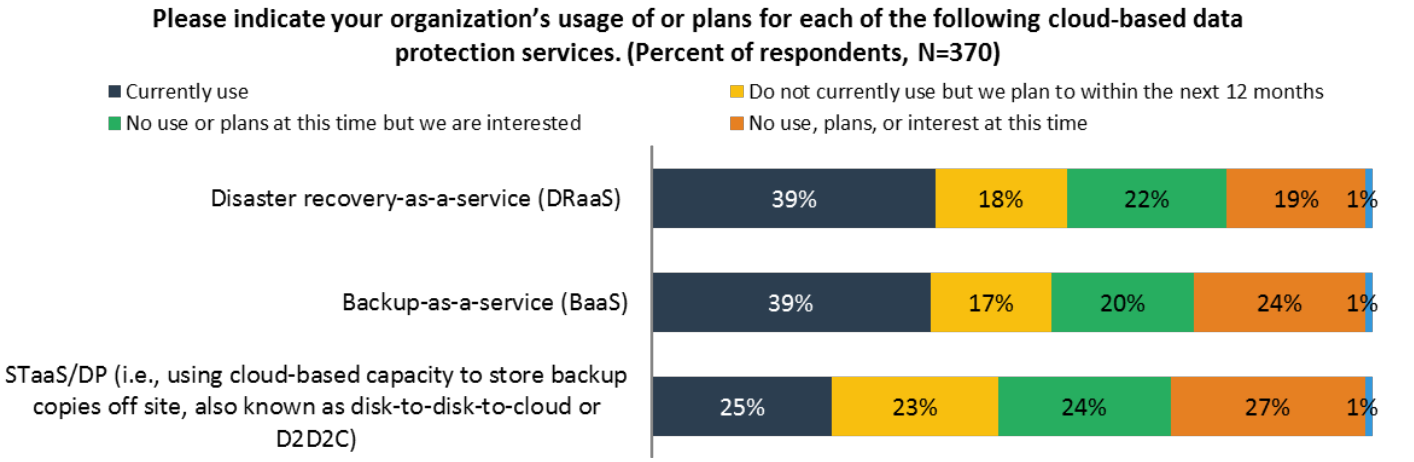
[5] ibid.

agility that organizations can achieve with "warm" data over "cold" data. But that agility is based on more recent data, thus still relegating truly long-term retention to tape.

Choosing Your Cloud-powered Solution

Even after you decide that a cloud service should become a part of your broader data protection strategy, you will still need to answer a few questions regarding which kind of cloud-powered data protection would best suit your environment. At least three solution types are prevalent in the market (see Figure 5), and none is definitively superior to the others.[6]

Figure 5. Current and Projected Usage of Cloud-powered Data Protection Services



Source: Enterprise Strategy Group, 2016

As Figure 5 shows, turnkey services such as BaaS and DRaaS are currently used in more surveyed environments than STaaS/dp (cloud-based storage as part of a data protection strategy) is. But combined, approximately three out of every four of these organizations are at least "warm to the idea" of using cloud-based protection in one or more forms. Altogether in other words, the organizations either are currently using (blue), are planning to use (yellow), or are interested in using (green) one or more cloud-based data protection services.

Storage-as-a-service Used for Data Protection (STaaS/dp)

Arguably, the easiest method of incorporating cloud services into a data protection strategy is simply to embrace cloud-based storage with your existing on-premises solution. This is STaaS/dp, and its appeal is grounded in simplicity. You get to keep using the backup solution(s) you are already happy with, including all the installed agents, schedules, and UIs, while adding a beneficial cloud repository to whichever disk and tape media are already in use.

The easiest method of adding cloud services to a data protection strategy is to embrace cloud-based storage with your existing on-premises solution.

However, cloud storage will only truly meet your needs if your current data protection software can support your current environment's uptime requirements and protects all of the workloads you depend on. *If your current backup solution is mediocre, adding cloud storage won't make it exceptional.*

In fact, some organizations may discover that certain aspects of their IT environments are more modern (e.g., contemporary, virtualized workloads) and are, therefore, better candidates to extend to the cloud for protection. Conversely, legacy backup products that are protecting older physical servers or antiquated workloads may be less cloud extendible.

[6] ibid.

This determination may require you to reassess your heterogeneous data protection strategy and make changes as needed. Or you may happily discover that a single data protection solution is capable of protecting both your physical and virtual servers—and is cloud extendible as well—thus meeting a greater range of goals.

Backup-as-a-service (BaaS)

Some organizations will be delighted to leverage STaaS/dp alongside their existing on-prem backup solution. Others will prefer to use turnkey BaaS or DRaaS offerings that provide a different (and perhaps more convincing) set of capabilities by "consuming" the backup software through the cloud service provider.

Many service providers are now delivering backup-as-a-service using the same kinds of enterprise-class data protection software that previously was available only for on-premises use. A lot of organizations will appreciate the advantages that a backup service of that type can offer, including 1) Remotely managed and monitored data protection jobs and 2) Improved reliability of the backup and recovery process due to the expertise provided by the service provider partner.

Service providers may offer a range of BaaS capabilities to their subscribers—from a simple OpEx-based, remotely hosted version of the same backup software that had historically been in use at the subscriber's data center, to complete "white-glove" expertise and remote management.

Why BaaS When You Can DRaaS?

Typically, STaaS/dp and BaaS are delivered in a disk-to-disk-to-cloud (D2D2C) configuration. When using that architecture for data recovery, organizations try to recover first from speedy onsite disk before resorting to retrieving data from the tertiary copy in a cloud, and their uptime SLAs would likely be established based on the onsite recovery timeframe.

In contrast, a DRaaS architecture leverages the cloud copy for rapid recovery when an on-prem backup is not available. Essentially, DRaaS provides an additional layer of recovery flexibility by combining a cloud-based copy (from STaaS/dp or BaaS) with cloud-based compute, cloud-based automation, and cloud-based orchestration in order to host the organization's business-critical systems during dire circumstances.

The Bigger Truth

To be clear, a cloud service ought to be a part of your data protection strategy unless senior management or relevant regulations prohibit it. That said, there is no single "best" cloud option. Rather, multiple solution scenarios exist, and at least one of them should align with what most organizations are seeking today in a hybrid onsite/offsite data protection architecture. It is also worth noting that some data protection software vendors, Veeam being a great example, are partnering with cloud service providers and are at this point adept at supporting each of the three currently prevalent approaches—STaaS/dp, BaaS, and DRaaS—via cloud-friendly solutions.