White Paper

What to Consider When Looking for Cloud-powered Data Protection

Investigating How the Carbonite EVault Portfolio Could Satisfy Today's Requirements for Effective Hybrid Data Protection

By Jason Buffington, Principal Analyst
and Monya Keane, Senior Research Analyst

December 2016

This ESG White Paper was commissioned by Carbonite and is distributed under license from ESG.

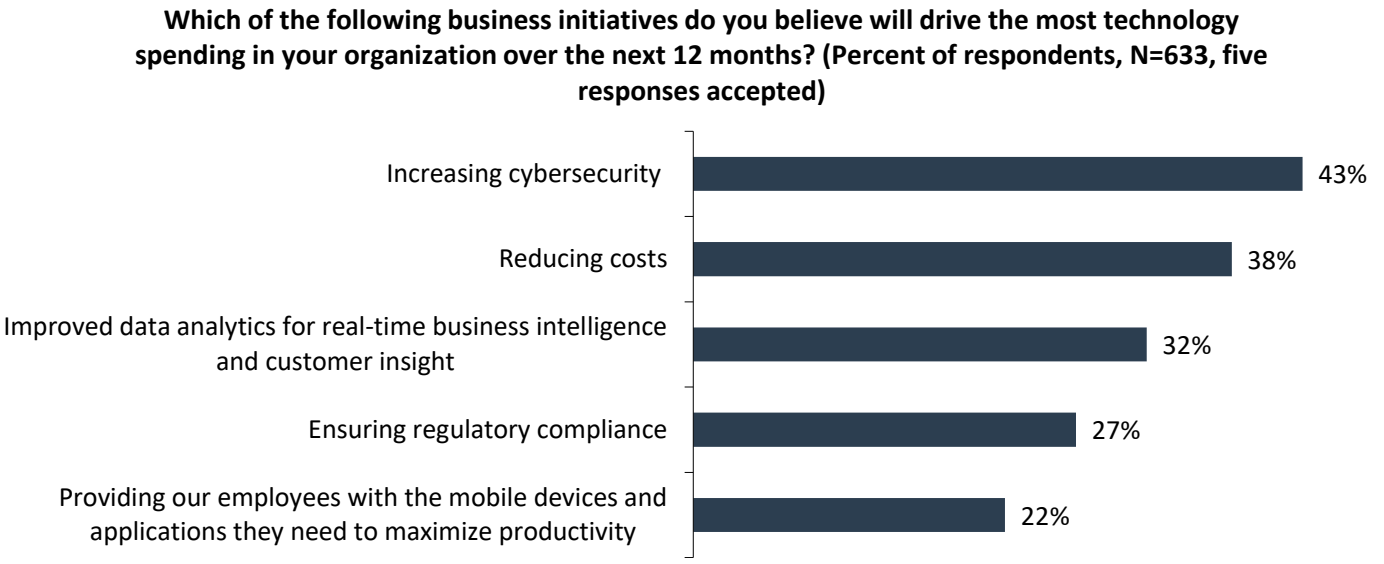
Contents

Introduction

These days, a lot of organizations are looking to the cloud to help them protect their data. They wish to take advantage of the appealing economics and operational agility that are two of the biggest attributes of a cloud-based IT infrastructure.

Leveraging the cloud can be a smart choice for any organization interested in gaining more control over costs (i.e., almost all organizations). According to ESG research, reducing costs was the second most commonly reported business driver affecting IT spending in 2016 (see Figure 1).[1]

Figure 1. Top Five Business Initiatives Driving IT Spending in 2016



Source: Enterprise Strategy Group, 2016

Looking into how organizations intend to contain/reduce IT costs, ESG determined that increasing the use of cloud computing services is the most common way that the organizations it surveys are trying to do so (see Figure 2).[2]

Figure 2. Top Five Cost-containment Measures in 2016

Source: Enterprise Strategy Group, 2016

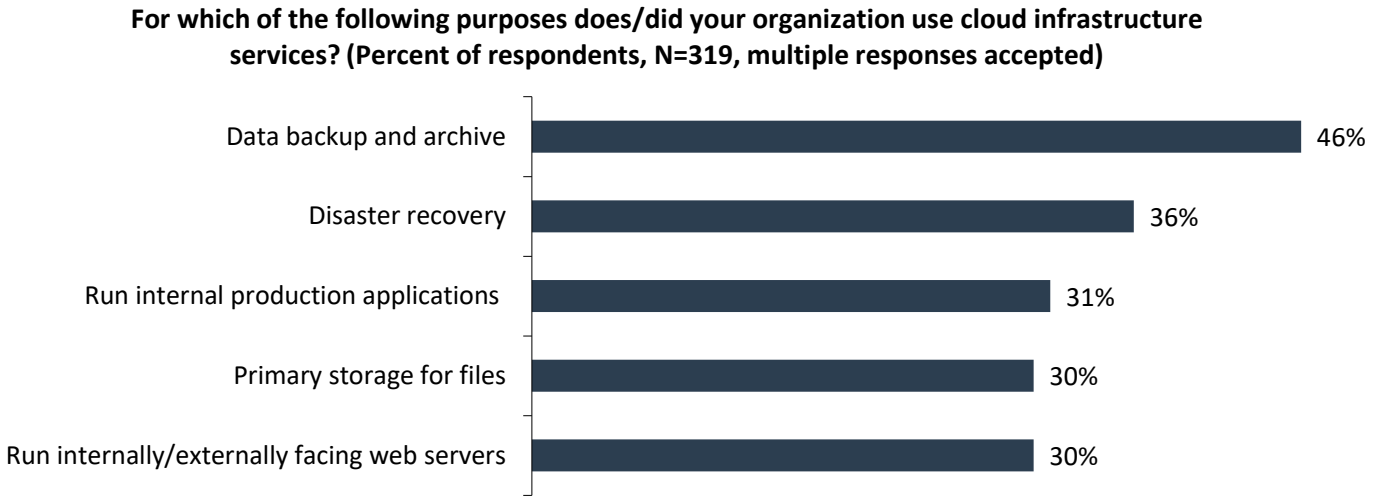
[1] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.
[2] ibid.

Interestingly, while using the cloud is the most-often reported tactic for containing costs, the next most-often-cited tactic—purchasing new technologies with improved ROI—often provides that impressive ROI *thanks to the cloud-enabled capabilities* embodied within the purchased technologies.

Today's Organizations Are Using the Cloud for Protection and Recovery

When it comes to specific cloud-service usage scenarios that are especially popular right now, data backup and disaster recovery both rank very well. In fact, they are the top-mentioned use cases (see Figure 3).[3]

Figure 3. Top Five Cloud Infrastructure Use Cases

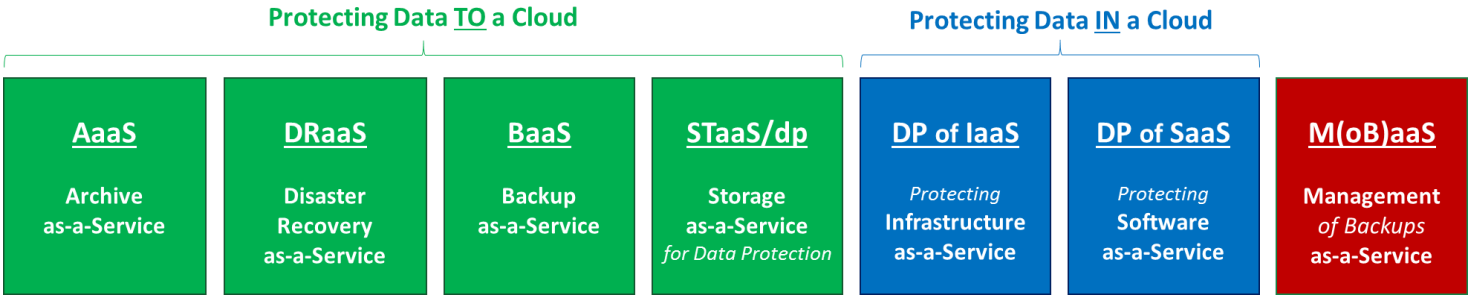


Source: Enterprise Strategy Group, 2016

This finding is to be expected, considering the cost-containment and agility goals at stake. Organizations simply want to leverage better methods to become and remain operational, compliant, cost-efficient, flexible, responsive, etc.

Of course, there's more than one way to interconnect the acts of protecting data and using the cloud (see Figure 4).[4]

Figure 4. The Seven Convergence Points of Data Protection and Cloud Services



Source: Enterprise Strategy Group, 2016

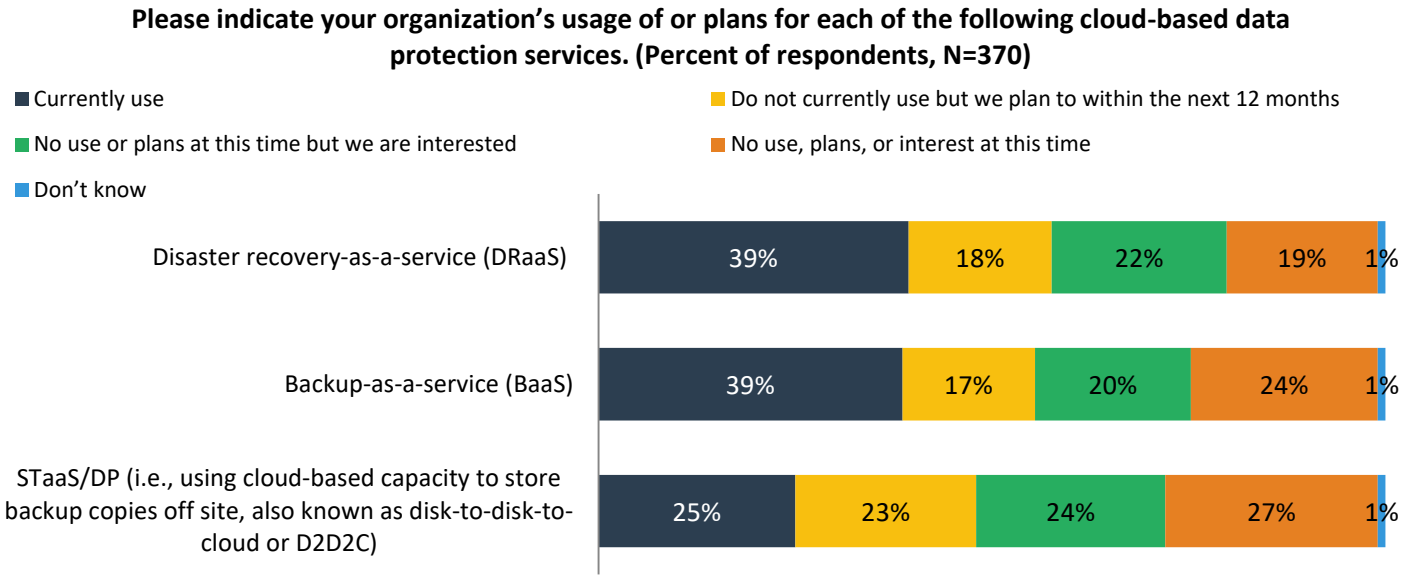
And as Figure 5[5] shows, most of the organizations ESG surveys report they already use (or at least are interested in) the three most common cloud/data protection convergence points: BaaS, DRaaS, and STaaS/dp. It is worth noting that many of these solutions can be consumed as direct-to-cloud services or even be used with an intermediary hardware asset—perhaps included as part of the service—to help the organization better adhere to SLAs.

[3] ibid.

[4] Note: ESG recognizes that "STaaS/dp" is not a generic IT industry term, but it is using the acronym in this document specifically to indicate *storage as a service that functions explicitly to protect data*.

[5] Source: ESG Research Report, *Data Protection Cloud Strategies*, December 2016.

Figure 5. Use of Cloud-based Data Protection Services



Source: Enterprise Strategy Group, 2016

Interest levels vary moderately according to the specific service, but collectively speaking, roughly three out of four organizations surveyed by ESG are at least "warm to the idea" of using the cloud as a part of their data protection strategy.

Factors and Capabilities to Consider When Investigating Cloud-powered Data Protection

There's not one definitive, universally applicable model for assessing the best way a particular organization should pursue cloud data protection. But in general, organizations that want to examine more deeply how much value cloud protection could offer them should make sure to consider:

- Data survivability and BC/DR preparedness.
- Reliability and speed of recovery.
- Security benefits.
- Economic and operational benefits.

Data Survivability and BC/DR Preparedness

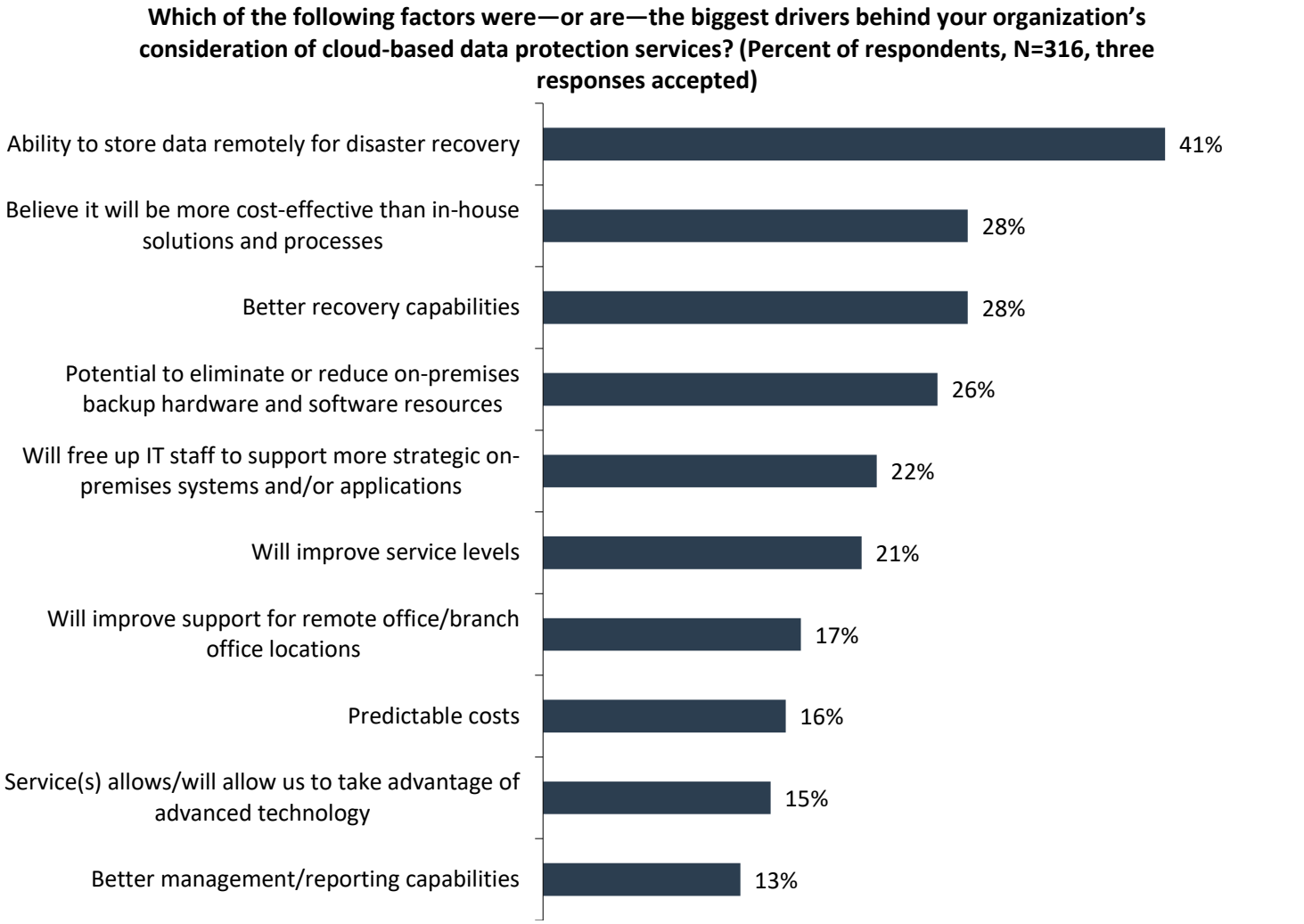
According to the IT decision makers surveyed by ESG, the straightforward benefit of *assuring data survivability* is, by a good percentage, the biggest potential benefit the cloud can offer to them (see Figure 6).[6] In fact, that ability to store data remotely for disaster recovery was also the most common driver for cloud-based data protection the last time ESG explored the topic.[7] The finding is particularly notable for midsized organizations: Unlike their enterprise counterparts, SMBs may not otherwise have a secondary site where they can keep offsite copies for backup/DR purposes.

Organizations should also remember that cloud services alone simply provide data survivability—not authentic BC/DR preparedness. To achieve true BC/DR preparedness, one must combine the data survivability embodied in a second site or cloud with automation and expertise to enable that data to be usable during/following a crisis.

[6] ibid.

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

Figure 6. Top Ten Drivers Toward Cloud-related Data Protection Services



Source: Enterprise Strategy Group, 2016

Reliability of Recovery

One reason organizations struggle with data recoverability relates to the often-antiquated or otherwise inadequate backup tools that they're still using … but that have, in many ways, outlived their true usefulness to a modern, agile IT infrastructure. Organizations that start embracing cloud-based data protection will often discover that they suddenly possess more modern capabilities, and as such, they can begin enjoying a higher degree of sophisticated recoverability.

Security Benefits

Although it is true that many organizations that are hesitant to embrace cloud services cite "security concerns" as an objection, the fact is that organizations already using cloud-powered data protection report improved security as a big benefit—42% of organizations surveyed by ESG that already use cloud protection cited that advantage, making it the second most frequently mentioned benefit of using cloud-based protection.

Backup and DR, although not as wholly proactive as some cybersecurity-centric preventive measures can be, are viewed as good ways for organizations to overcome ongoing ransomware attacks. When an organization possesses technology capable of preserving snapshots with rollback to a safe point in time, that organization can essentially turn back the clock and recover clean versions of data and files that had received automatic backup prior to the ransomware attack.

Many of today's cloud backup offerings also encrypt data onsite, in flight, and in the cloud. The cloud service providers offer modern-day physical protection as well, including measures to restrict data center access via:

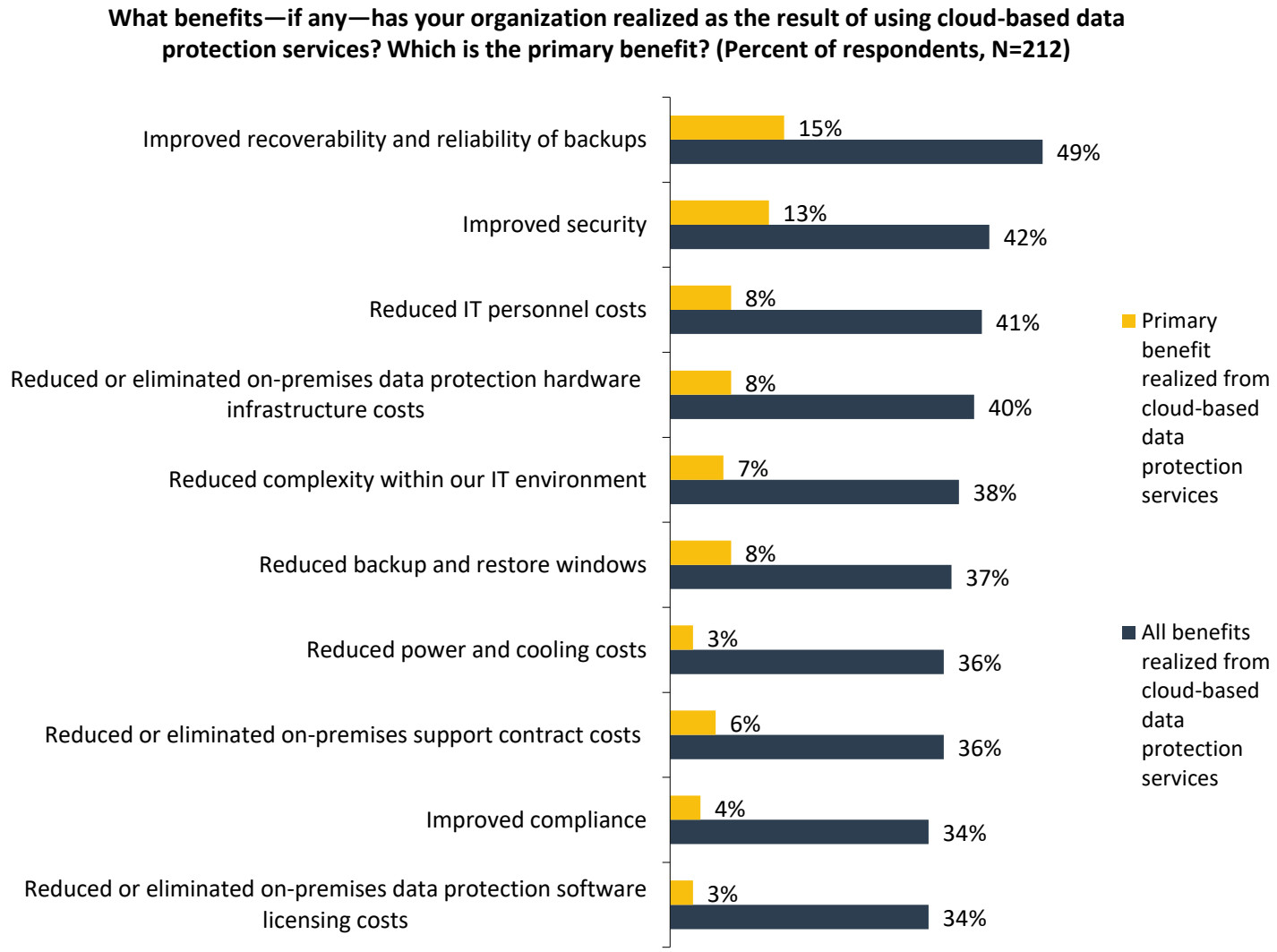
- Biometric scanners.
- Electronic key cards.
- Onsite security officers guarding the locations 24 hours a day, 365 days a year.

Conversely, many traditional onsite protection solutions are hampered by security-exposure issues, and most do not encrypt data in flight or at rest.

Economic and Operational Benefits

As Figure 6 showed, many organizations that are moving to cloud data protection (as well as those already using such solutions and services) wanted something more cost-effective than an in-house protection solution could offer. Using the cloud, these organizations now are seeing reduced hardware, software, and even management/labor costs (see Figure 7).[8]

Figure 7. Top Ten Realized Benefits of Using Cloud-based Data Protection Services



Source: Enterprise Strategy Group, 2016

[8] Source: ESG Research Report, *Data Protection Cloud Strategies*, December 2016.

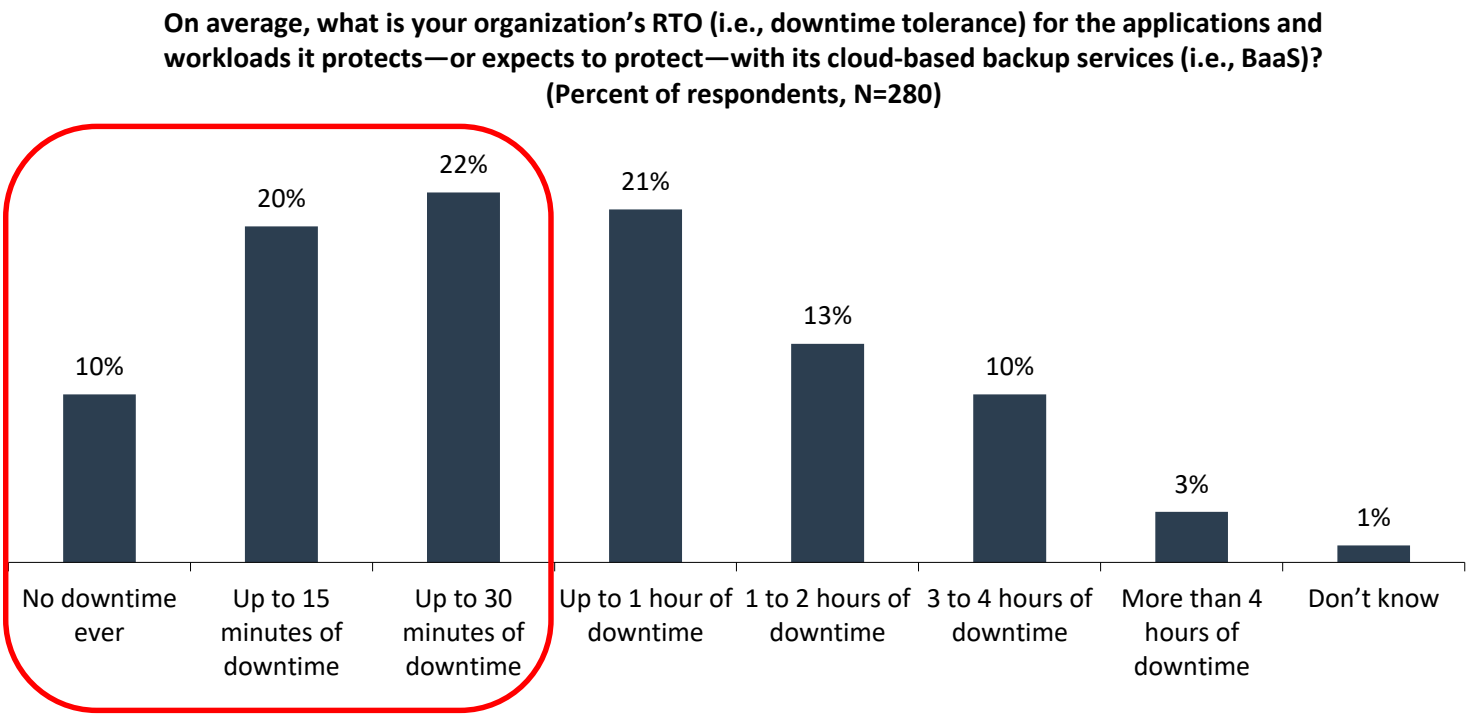
Ensuring SLAs via Cloud-powered Data Protection

The choice of a cloud protection solution should not adversely affect recovery SLAs for the IT services being protected. In other words, an organization shouldn't have to relax its already-established recovery time objectives (RTOs) just because it wants to incorporate the cloud into its data protection strategy.

Therefore, it is important to acknowledge that the types of business-driven service level agreements that IT services are sometimes held to today *may not always be attainable* by a straight-to-cloud data protection solution.

Endpoint devices and remote-office servers are probably fine to be backed up to a cloud service. But mission-critical servers with very low downtime tolerances may require local recoverability in addition to leveraging the cloud as the additional repository for protection. This protection/recovery approach is called "disk to disk to cloud," or D2D2C. Some service providers call this local-and-cloud approach a hybrid model. Further justifying the approach is the fact that a combined 52% of the organizations surveyed by ESG that use cloud-based backup report having a 30-minute-or-less downtime tolerance for those applications (see Figure 8).[9]

Figure 8. Downtime Tolerance for Applications Protected by BaaS Services



Source: Enterprise Strategy Group, 2016

Specifically Addressing Downtime and Data Loss

Downtime can be addressed and resolved via two approaches:

- A failed server can be rectified through rapid recovery via on-premises disk, or via disaster recovery-as-a-service. With DRaaS, you can simply restart the server from within the cloud-based service.
- End-user productivity problems due to lost data can be addressed by performing more frequent protection operations and by using agile recovery mechanisms.

[9] ibid.

As mentioned, there are two approaches or two main architectures (consumption models) for cloud-enabled data protection that are worthy of consideration:

- **Cloud-powered data protection** (a.k.a. BaaS). This is a cloud-service-delivered offering in which agents on endpoints and servers typically send data directly to a turnkey service.
- **Cloud-enabled data protection**, in which cloud-based storage is used to augment an otherwise on-premises backup solution (a.k.a. STaaS/dp, or storage-as-a-service used for data protection).

Notably, some service level agreements will allow an organization to pursue more ambitious return-to-service times than it had previously set—achievable, for example, by leveraging options such as cloud failover.

Solutions to Consider from Carbonite

One company providing both BaaS and STaaS/dp approaches is Carbonite. An early BaaS innovator (first supporting endpoints, later servers), Carbonite recently acquired EVault technologies from Seagate to deliver appliances and backup software that can bolster an organization's BaaS, STaaS/dp, and DRaaS initiatives. Figure 9 illustrates Carbonite's current EVault solution components.

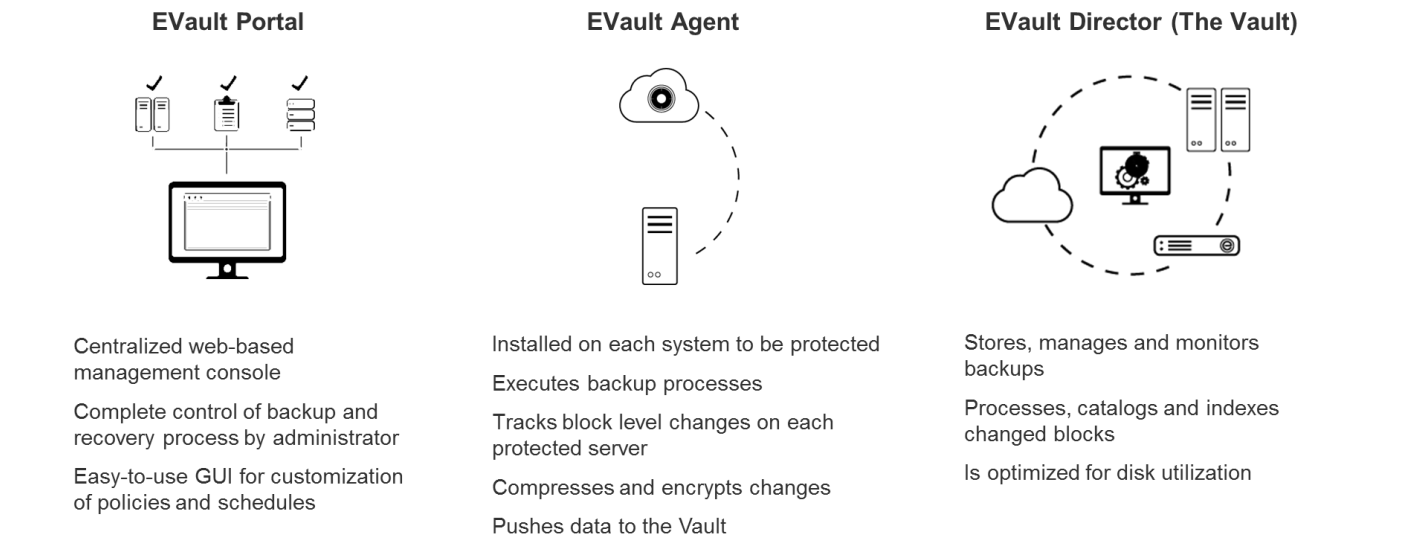
The Cloud Is Better than Tape to Combat Data Loss

Whatever your frequency of data protection activity is, consider half of that timespan to be your data-loss window.

For example, imagine that you back up data to tape each night—the most common frequency when using tape for protection. You have thus established a "daily frequency of protection." So, if an array fails at the *beginning* of the next business day, you'll lose almost no data. But if it fails at the *end* of the next day, you lose eight hours' worth of data. The midpoint of those two scenarios is noon, giving you an average of four hours of data-loss exposure.

Contrast that scenario to a cloud data-loss scenario. Only 17% of cloud-using organizations surveyed by ESG send data for protection nightly. The rest send it to the cloud every two hours, on average, thereby reducing their average data-loss exposure window to just an hour. That is a marked improvement.

Figure 9. Three Key Components of the Evault Solution by Carbonite



Source: Carbonite, 2016

It is advisable to consider the EVault by Carbonite solution(s) within the context of ESG's prescriptive guidance presented earlier, specifically in terms of:

- **Data survivability**—The EVault architecture includes local disk-based protection, which transparently replicates to a cloud-based service. This capability has been offered almost since EVault's inception a decade ago. More importantly,

the EVault Cloud allows for instant failover of systems to a hot site in the EVault cloud whenever needed. In the event of a disaster, this capability allows servers to remain operational and organizations to maintain access to their data until their primary location is accessible.

- Reliability of recovery—As is often the case with modern data protection technologies that leverage cloud services, EVault customers are reporting that these technologies provide better reliability than the ones they used previously.
- Security—EVault uses advanced security at rest and in flight: 256-bit AES encryption before data leaves the server, as well as Secure Sockets Layer (SSL) transport encryption. EVault customers have exclusive access to their encrypted data using a private encryption key. Carbonite states that its EVault data centers/processes operate at the highest classification levels for reliability and performance, and that independent annual audits validate that assertion.
- Economics—Carbonite adheres to conventional per-terabyte pricing models, which is helping its EVault customers to more effectively capitalize on the transformative economic impact that cloud services offer, particularly in relation to the many benefits listed in Figure 7.
- D2D2C—The EVault solution, as part of its foundational DNA, offers EVault Cloud Backup for automatic cloud backup and optional onsite protection for any physical or virtual server environment. This hybrid model provides onsite hardware delivered as a service. As mentioned, many protection solutions are best delivered as a D2D2C architecture to achieve better SLAs. While the industry may refer to this setup as a hybrid architecture (referring to its on- and off-prem characteristics), Carbonite with EVault has gone as far as to call it hardware-as-a-service (HaaS)—thus identifying it as a turnkey offering distinctly different from Carbonite's pure-cloud offerings.

  EVault also offers Backup Software, which is standalone software for private networks. This option allows organizations to provide their own hardware.
- Reduced data loss—The EVault technology for servers and the Carbonite mechanisms for endpoint devices and remote/branch offices together enable frequent, granular replication to a cloud service to reduce data loss across a range of supported devices.

The Bigger Truth

It is impossible to have an IT modernization conversation today without talking about the cloud, especially about its perceived economic benefits, its operational agility, and its often-superior recovery-scenario capabilities.

Two of the earliest innovators in cloud-powered data protection—Carbonite and EVault—are now one entity. Carbonite brings a reputation for simplicity and ease of use to the partnership, and EVault brings more than two decades of innovation in the backup and disaster recovery space, offering automatic data protection plus the ability to recover data quickly.

Essentially, Carbonite has created a one-stop-shop for endpoint, remote office, and server-centric data protection designed to reduce downtime and data loss through a combination of cloud, disk-, and tape-based protection mechanisms. The overall result is an improved recovery outcome.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188