ESG Enterprise Strategy Group | **Getting to the bigger truth.™**

Solution Showcase

Why—and How—Organizations Need to Align Business Priorities and Data Protection Strategies

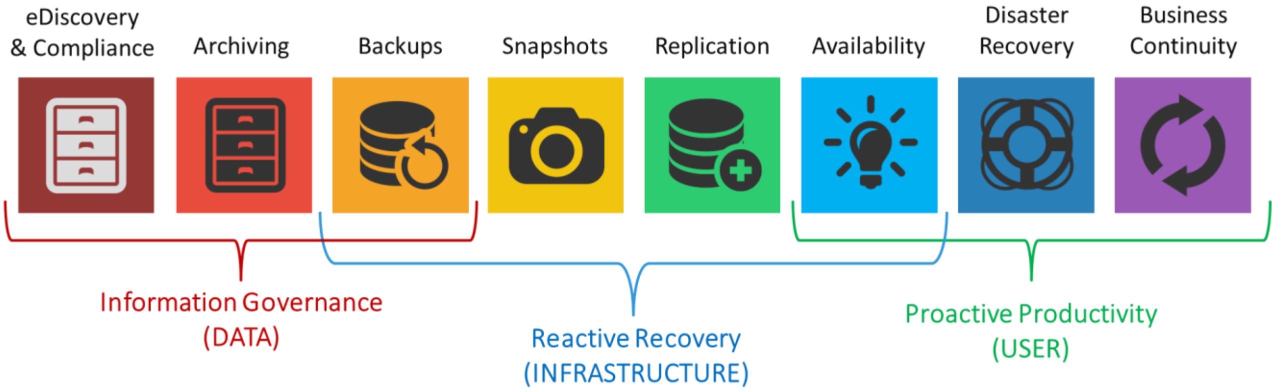
Date: April 2017 **Authors:** Jason Buffington, Principal Analyst; and Monya Keane, Senior Research Analyst

Abstract: Backup alone is not enough anymore. Businesses today must put a range of recoverability options in place. That's why it is encouraging to see Carbonite, a data protection company with cloud and hybrid offerings, making fresh moves to help organizations evolve beyond legacy backup. Years ago, Carbonite pioneered cloud backup for endpoint devices. Then it expanded, buying EVault in 2015 and DoubleTake in 2017. Just as Carbonite has long been at the forefront of offering what people need from cloud-based data backup, it now appears to be just as intent on providing what IT organizations need—hybrid data protection *media* and *mechanisms*.

Introduction

For all organizations, server and component-level crises are unfortunate inevitabilities. Likewise, the need of end-users to revert to previous file versions is a common occurrence due to predicaments large and small. Recognizing these realities, ESG consistently recommends that organizations consider an approach to data protection that is broader than what backup alone can provide (see Figure 1).

Figure 1. The Spectrum of Data Protection



Source: Enterprise Strategy Group

Backup should absolutely be the foundational cornerstone of every data protection strategy. But a range of additional mechanisms should be sought to complement (not replace) backup—mechanisms that can address the multiple recovery and restoration scenarios all organizations face at some point.

Understanding Risks and Downtime

To assess your organization's data protection risk level, you will first need to (1) make a complete inventory of your systems, and (2) develop a deep understanding of which of those systems, if any, can tolerate downtime. That understanding gives you visibility into the cost of downtime at your organization and helps you determine the real ROI of your data protection buying decisions. Here are a few general items to keep in mind:

- The bottom line is that, regardless of whatever specific data protection plans or strategies you intend to implement, the result really has to be *that you have gotten copies of your data out of the building.*

- Not all of your business data is conveniently held in a centralized data center. A large portion will be, but some may be stored at remote/branch office locations, on employees' endpoint devices, or in the cloud already. *It all needs to be protected.*

- As Figure 1 showed, backup and replication are complementary *but different*. Both are necessary parts of a broader data protection infrastructure.

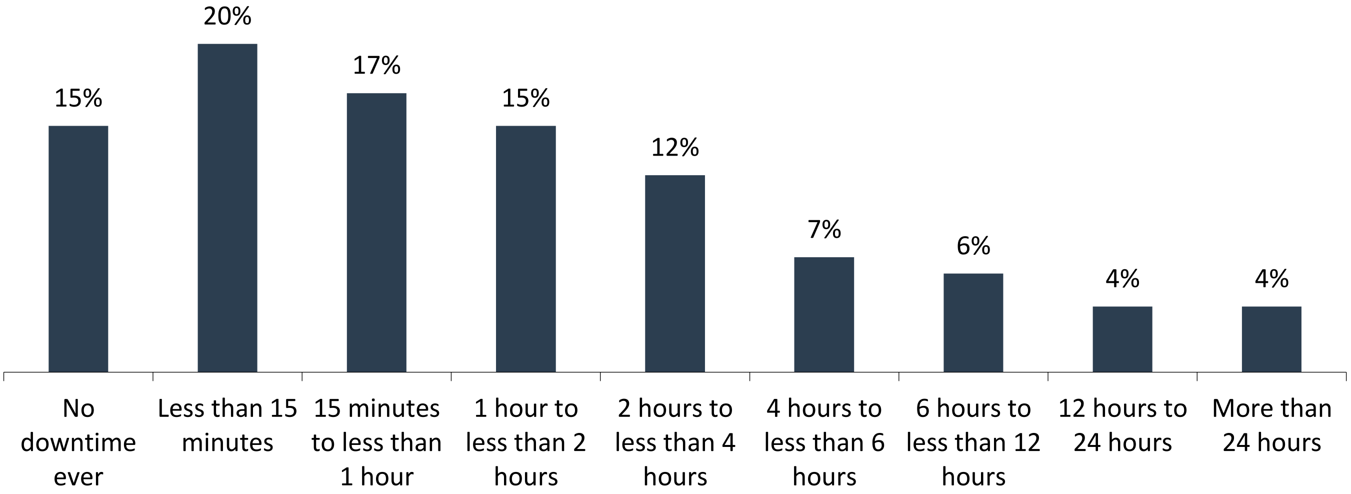
A Checklist to Assist You

As you proceed in evolving your protection strategy, try using this checklist of questions.

- **How much downtime can my systems and applications tolerate?** Different IT systems have different levels of criticality for your organization. A four-hour outage of your mailroom's package-routing application may be tolerable. A four-hour outage of your company-wide email system is not. Armed with such information, you can identify the range of service level agreements your organization's end-users require. It is reasonable for different servers and workloads to have different uptime requirements, yet many organizations underestimate just how many of their servers have SLAs more stringent than what backup alone can accommodate. Figure 2 illustrates the ranges of tolerable downtime that respondents have reported to ESG.[1]

Figure 2. Percentage of Servers, Based on Downtime Tolerance

Considering all of your organization's production applications/workloads (including both "high-priority" and "normal" workloads), approximately what percentage of these production servers/services fall within each of the intended (i.e., target or "desired" recovery time RTO/SLA versus what your organization has actually delivered) recovery times listed below? (Mean, N=391)



Source: Enterprise Strategy Group

[1] Source: ESG Research Report, *The Evolving Business Continuity and Disaster Recovery Landscape*, February 2016.

- **What's the cost of each hour of downtime?** Calculating the cost of downtime used to be relatively simple when servers were physical and fulfilled one purpose. For any single server, you'd add the average length of time necessary to recover (downtime) to the amount of time that effort would have to be repeated due to lost data since the last backup. Then, you'd multiply that window of time by (1) the productivity impact per affected user, and (2) the human cost per idle/impeded user.[2] But in today's highly virtualized environments, there might be 5 to 20 VMs on any virtualization host. Each VM will have a different cost of downtime or business impact.

- **How much downtime can my *non-critical* systems tolerate?** Because almost every business process relies on data, this can be a tough question to answer. One could argue that the combined 14% of systems (see Figure 2) that can tolerate six or more hours of downtime are non-critical, thus requiring simply "mediocre" backup. But with 86% of servers having higher uptime expectations—which must be met via better backup with rapid recovery as well as replication, snapshot, and availability technologies—treating any server as non-critical invites disaster. Remember: Non-critical VMs might run on the same hosts as critical VMs.

- **How far back should I keep copies?** Typically, you should have the capability to roll back to daily versions for at least a month and weekly versions for a year. That setup will enable recovery from a variety of human errors, bad application updates, malware/cybersecurity attacks, etc. Beyond that, most of your data is likely "operational," meaning that after two years, it has limited to no value. A subset may be mandated for longer retention (five to ten years or more). In addition, your business may require long-term retention of some data due to eDiscovery requests or compliance regulations. Always check with your legal team to make sure your retention schedule is sufficient.

- **How do I determine my RTO?** This is an easy question to answer using two additional questions posed by IT to each business unit relying on those IT systems:
  - "How much downtime can you tolerate?" The typical response will be "none." IT should then price out solution prices at three recovery levels: less than 15 minutes, less than 60 minutes, and less than 120 minutes.
  - Next, IT should ask the business unit leader (or shared manager of that BU and IT), "Which tier would the business unit like to pay for?" That is your RTO for the IT systems supporting that business unit.

- **What are all the types of risks that I should consider?** Nearly all organizations experience an outage or downtime event. Those events can be caused by simple human error, natural disasters, mechanical failures, etc. The key is to recognize that minor events may not have the same level of impact, but they are statistically more likely to happen—i.e., a software/hardware failure may only affect one physical server (including all the VMs on it and all users depending on those VMs), yet it is much more likely than a flood or fire affecting an entire site. Look at your system logs per server. You'll be surprised at how often those inconvenient blips (hours) of downtime occur.

Develop a Strategy Encompassing Multiple Mechanisms and Media

Traditional onsite backup, by itself, is likely to be unable to meet rigidly enforced SLAs. With that fact in mind, plan to incorporate some other data protection methods, namely, the methods depicted in Figure 1. At a minimum, attempt to establish a "backup-plus-replication" architecture.

Protection Mechanisms

Backup and replication have distinctive capabilities that your organization needs:

- **Backup**—Backup is the logical and necessary foundation of any data protection strategy because most organizations need to be able to restore data from a given point in time. Whether IT needs to address a human error, correct an

[2] Source: Buffington, Jason, *Data Protection for the Virtual Data Center*. Wiley Press, 2010.

application failure, or cope with a power outage, those saved copies will come to the rescue. In fact, most organizations have to revert to previous file versions for "mundane" reasons far more often than they have to resolve full-fledged server calamities. And although backup is vitally important for all systems, it is especially important for second- and third-tier workloads/systems that might not be protected through sophisticated and expensive high-availability mechanisms.

- Replication—Replication mechanisms stream changes to routinely update another instance of the data on another platform, thus enabling data survivability and agile recoveries from another location. However, replication does not provide historical versions (only the most recent). That is not a limitation; in fact, it actually makes replication quite a suitable complement to backup in most data protection strategies.

Protection Media

When modernizing data protection, leveraging multiple media is just as important as leveraging multiple mechanisms:

- Onsite—Local recovery from onsite backups plus the availability of local replicas to access if needed are, together, the essential standard. It will not be possible for you to adhere to tight SLAs using an offsite approach alone.
- Cloud—However, there's a reason the cloud is considered the most transformative IT concept of the last decade. Cloud services really should be a part of every data protection strategy in some form:
  - Endpoints and remote offices should be protected by cloud-based backups. Of course, do your due diligence in regard to establishing the cloud service provider's security and reliability.
  - If you seek tape replacement or supplementation, leverage cloud-based storage as an extension of your onsite backup and recovery capabilities. This tactic is often referred to as disk-to-disk-to-cloud (D2D2C).
  - The power of the cloud isn't always centered on promising the lowest cost per gigabyte or lowest TCO. The true power of the cloud lies in its agility. Specifically, the cloud can enable you to take advantage of new capabilities (e.g., offsite backup) and new recovery capabilities (e.g., failing over to a cloud service).

Just as you should always be thinking about backup *plus* replication, you should also plan for onsite protection *plus* cloud protection. When you complement and extend your fast local recovery/restoration capabilities with reliable and agile cloud services, you get an up-to-date hybrid architecture working for you and your end-users. Multiple mechanisms address various SLAs, and multiple media achieve better economics and help you to be more responsive and agile.

In this manner, you are effectively and responsibly addressing your organization's ever-changing, ever-heightening data protection requirements. But perhaps the most important fact to internalize is that your approach to data protection should start with addressing your SLAs rather than focusing on maintaining or evolving your existing "status quo" methods. So, look for vendors and solutions that can address those varying SLAs through comprehensive offerings that span mechanisms and media.

How Carbonite's Capabilities Align to ESG's Recommendations

Carbonite has long been a leader in providing offsite data backup for consumers and small businesses. Recently, its across-the-board support for protecting servers (physical, virtual, and cloud based) has arisen as a key differentiator. Carbonite clearly understands that organizations' data protection strategies and needs are continually evolving.

In an effort to support those organizations' demands for better recoverability, it acquired two other equally respected IT innovators to become a much more complete data protection *portfolio* vendor:

- **Carbonite EVault for backup**—Acquired by Carbonite in June 2016, EVault provides server-centric backup through software or a turnkey appliance. Notably, the EVault architecture is built for a D2D2C approach, whereby cloud services extend the organization's data protection initiatives, including enabling server recovery in the cloud.

- **Carbonite DoubleTake for replication**—Acquired by Carbonite in January 2017, DoubleTake software provides replication between data centers and across myriad public clouds. Migration and failover capabilities are two of DoubleTake's signature strengths. Carbonite states that its DoubleTake Move product is able to handle any-to-any migrations, i.e., quickly migrating physical, virtual, and cloud workloads over any distance while minimizing risk and reducing downtime to near-zero levels.

Organizations seeking modern diversity in their data protection mechanisms and media should consider the Carbonite portfolio in light of its newest capabilities:

- **Endpoint and ROBO backups** through the Carbonite cloud service.
- **Server backups and restorations** through EVault software and appliances.
- **Server failovers** to recover from unplanned outages or to support migrations through DoubleTake software.
- **Onsite recovery** through the EVault appliance as well as DoubleTake for site-to-site replication.
- **Cloud services** to leverage as a backup service (via Carbonite), as an extension of protection (via EVault D2D2C), or as an alternate recovery location (via DoubleTake).

Carbonite's across-the-board support for servers has arisen as a key differentiator.

The Bigger Truth

It is practically impossible for an organization of almost any size to meet today's SLAs and their end-users' expectations with onsite backup alone. Therefore, these organizations should strive for a hybrid approach when it comes to their data protection *mechanisms* (i.e., backups plus replication) and their data protection *media* (i.e., onsite plus cloud) to meet or exceed availability/uptime demands.

For many organizations, it should be exciting to discover that three offerings, each of which helped to evolve and transform the data protection landscape, now live under a single portfolio brand—with individual components capable of addressing the broad range of protection and recovery scenarios that modern organizations require. As such, organizations looking to evolve beyond the status quo should carefully reinvestigate Carbonite's "new-look" portfolio, now including EVault and DoubleTake.

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