SOLUTION SHOWCASE

How IBM Spectrum Protect Enables Hybrid Data Protection Capabilities through Cloud Services

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

Abstract: In 2017, data protection should be about "and" instead of "or" if it is going to deliver the agility and recoverability that organizations demand. In other words, modern *hybrid* protection must be the foundation of any organization's production and protection strategies. IBM's capabilities to utilize cloud services and partner offerings continue to prove that Spectrum Protect is as innovative and compelling in a cloudy world as it ever has been.

Introduction

Today's best hybrid cloud backup architectures combine the speed of an on-premises solution with innovative remote-protection cost models and agility models in ways that most pure-disk or pure-onsite options cannot. Aware of this reality, savvy IT managers combine and deploy multiple IT topologies to back up their organizations' primary production data effectively and establish an ideal protection plan.

According to new findings from the *2017 ESG IT Spending Intentions Survey*:[1]

- Cost reduction is the second most common business initiative expected to drive IT spending in 2017, behind cybersecurity.
- When asked how they would be reducing costs, more than one in four organizations said they would increase their use of cloud services.
- Storing data as a repository for backup/archive is once again among the top use cases for current users of cloud infrastructure services.

Looking at the hybrid architectures of many organizations today, snapshots and backups within disk-based systems serve as the first line of recovery; tape supports long-term retention, and the cloud provides DR. Each medium has its strengths:

- Disk is the highly agile, first-tier choice for item-level restores as well as deduplication and compression optimization support. Per ESG's recent data protection research, 74% of organizations leverage disk as their first tier of recovery.[2]
- Tape isn't as ideal as a first recovery tier, but it outshines disk for long-term retention and archiving—it serves as a reliable, economic way to transport data and store it for years or decades. ESG research finds that nearly half (48%) of surveyed organizations use onsite or offsite tape as part of their backup process.[3]

[1] Source: ESG Research Report, *2017 IT Spending Intentions*, to be published.
[2] Source: ESG Research Report, *2017 Trends in Data Protection Modernization*, to be published.
[3] ibid.

This ESG Solution Showcase was commissioned by IBM and is distributed under license from ESG.
© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

- The cloud offers long-distance data survivability, on-demand agility for BC/DR and analytics purposes, and reduced onsite hardware expenditures. Seventeen percent of ESG survey respondents anticipate using cloud services as part of their backup strategy (typically alongside disk and/or tape), and adoption rates do appear to be rising.[4]

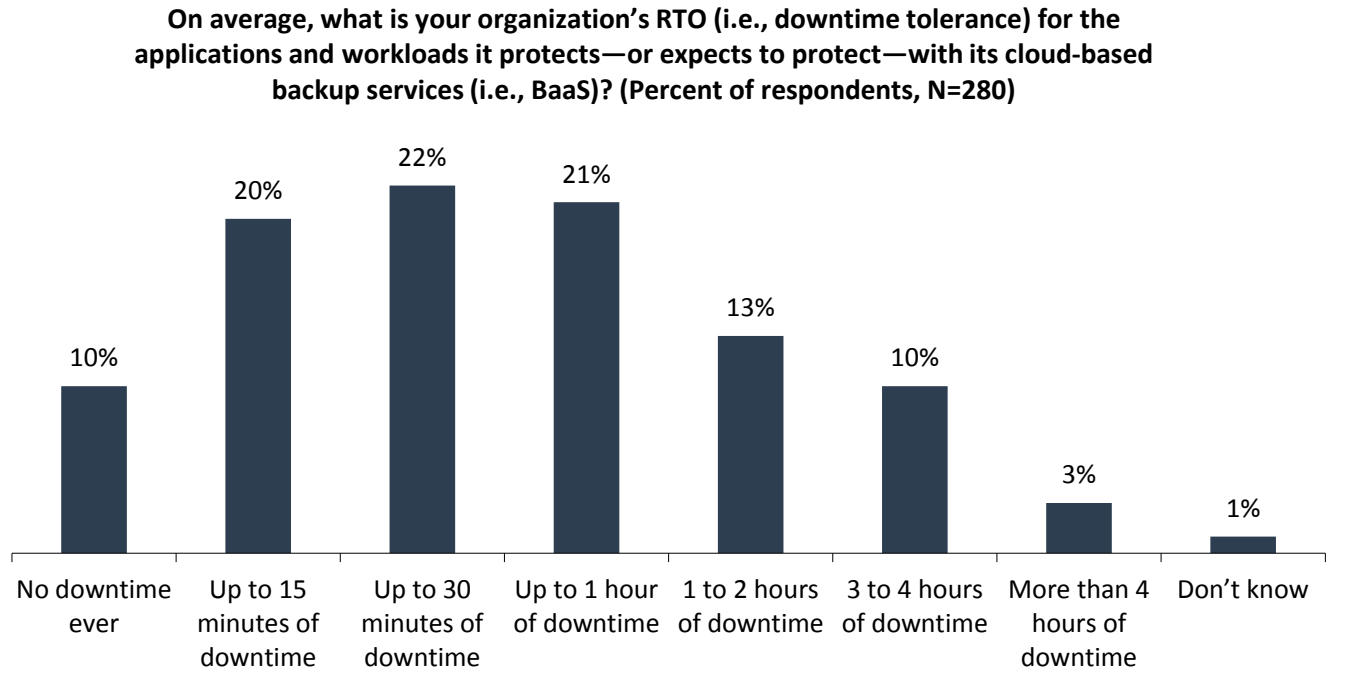
  Technically, of course, "the cloud" is not an actual type of media. It is an alternative consumption model for disk/tape capacity, and it is often coupled with expert management services and delivery at scale to achieve higher reliability and economic savings.

Catches Exist, However

Cloud-based protection is neither indefensibly better in all scenarios nor equitable from all providers. For example, some cloud backup solutions started as consumer services that were "beefed up" to attract enterprise clients, but not all made the transition effectively.

Also, using a cloud service doesn't equate to getting out of the backup business. Many IT managers think they'll start using a cloud solution and everything will be magically better—forgetting they'll still need to maintain/manage backup agents and onsite disk to meet stringent requirements for uptime (see Figure 1).[5]

FIGURE 1. Downtime Tolerance for Applications Protected by a Cloud



Source: Enterprise Strategy Group, 2016

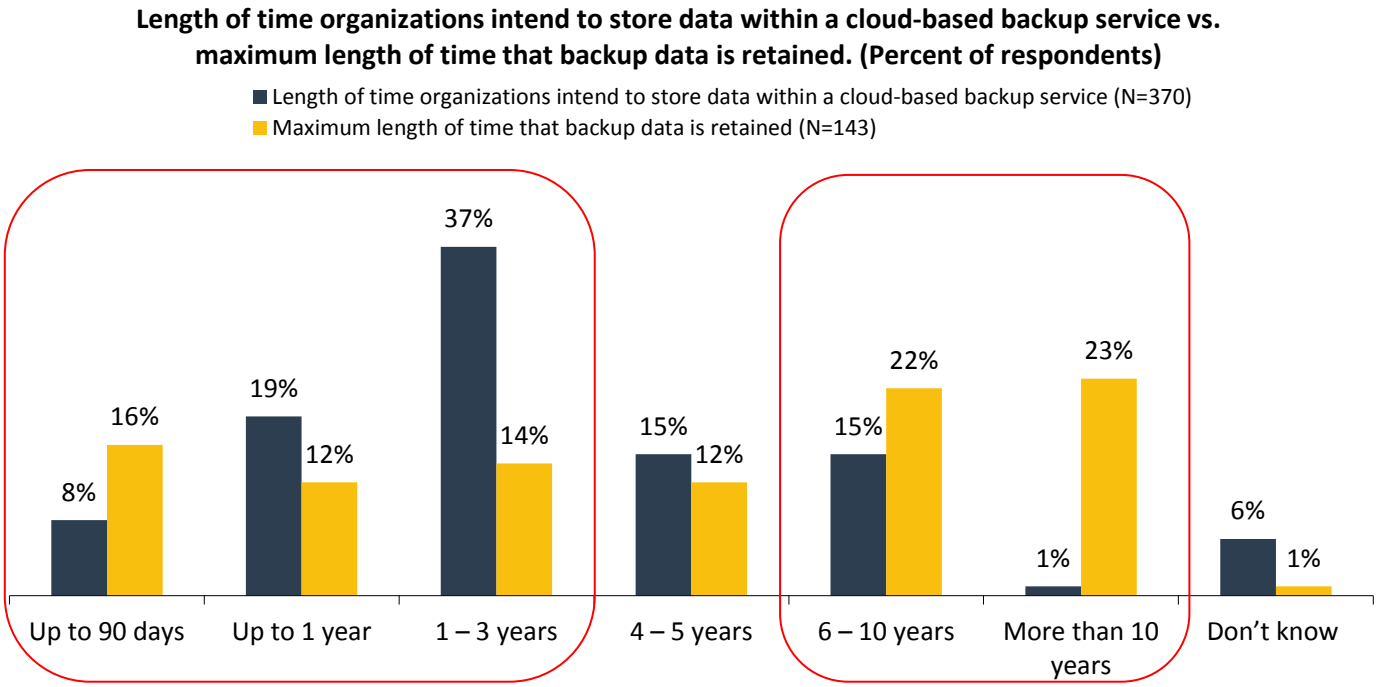
Additionally, cloud providers might not store data for as long as the organization requires, so it will also need economical cold media (i.e., tape) for truly long-term archiving.

As Figure 2 shows, many organizations plan to use tape to support retention windows of six years or more for their "cold" data, while leveraging the agility of the cloud for their "warm" data over shorter retention durations.[6]

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

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

FIGURE 2. Duration BaaS Users Plan to Store Data in the Cloud, by Length of Time Backup Data Is Retained



Source: Enterprise Strategy Group, 2016

It's Time to Do Something Better

Protection challenges facing IT teams can't be overcome based solely on which protection methods or media they choose—at least, not if those tools and methods used are insufficient or are perceived as being insufficient. Interestingly, 43% of respondents surveyed by ESG reported that they would change their current backup solution if they were given the choice to rearchitect it from scratch.[7]

In some cases, the dissatisfaction with backup solutions is warranted, considering that the most common problem surveyed IT pros cite regarding protecting today's highly virtualized IT environments is *data recoverability*.[8] That's a troublesome finding: Being able to recover data is likely the major reason that it was backed up in the first place.

In other cases, dissatisfaction stems from a generalized lack of assurance that things are going well. This phenomenon is similar to the challenges ESG observes related to protecting highly virtualized environments: Five of the top six challenges of protecting virtual server environments reported by ESG research respondents (other than recoverability) relate to inadequacies in some aspect of monitoring, verifying, or troubleshooting the protection environment.[9]

Those findings are virtualization-specific, but the broader dilemma is how IT organizations can accomplish backup better. ESG offers four recommendations reflecting how a hybrid data protection architecture, with both on-premises and cloud capabilities, is beneficial:

- Plan for disk-to-disk-to-cloud (D2D2C). The uptime levels expected of IT today can very rarely be met by a "cloud-only" protection solution, so organizations *must* combine local recovery capabilities (i.e., snapshots and backups) with the agility and survivability options of one or more cloud services, potentially including backup-as-a-service (BaaS) for

[7] Source: ESG Research Report, *2017 Trends in Data Protection Modernization*, to be published.
[8] Source: ESG Research Report, *Trends for Protecting Virtualized Environments*, August 2015.
[9] ibid.

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

endpoints and remote offices, cloud storage for servers throughout the environment, and disaster recovery-as-a-service (DRaaS) for IT resiliency and BC/DR.

- **Look for cloud solution providers who are not just repositories, but sources of expertise.** Economics and agility can make any cloud solution appear compelling. But the expertise to accomplish new recovery scenarios or unlock new value from data is also important. Some service providers offer "turnkey" remote management. Others provide consulting help for BC/DR or IT optimization. Regardless, local partners/resellers who are trained in relevant cloud technologies and services often have a unique perspective, contextual know-how and empathy with the local IT environment, and experience in accelerating this type of digital transformation.

- **Recognize that disparate repositories, such as local disks and remote clouds, can serve as air gaps to mitigate ransomware attacks.** Although cybersecurity should always be addressed first through prevention instead of recovery, using multiple media whose only connector is a data mover for backup can create an additional layer of separation, one that may be key to stopping an infection from propagating. When organizations combine an air gap with analytics that identify radical changes to what had previously been dormant data sets, they may even be able to identify some malware events from within the data protection solution.

- **Use warm data for more than cold storage.** Cloud storage is often first considered because of its economic advantages. However, a lot of its real value comes from its ability to utilize secondary, natively-accessible cloud-hosted data (i.e., warm data) in ways that are more viable than with tape-stored data (i.e., cold data). Examples include performing analytics or generating reports using the information, testing system patches or conducting DevOps testing without changing the protection copy, and performing sandbox orchestration as part of BC/DR planning. These scenarios are possible when one has 1) a dormant but near-current copy of data available, 2) on-demand compute for running processes only when needed, and 3) orchestration and/or expertise. The right cloud provider can deliver these services when the cloud is combined with the right data protection solution.

IBM Spectrum Protect Is a Cloud-enabling Solution to Consider

IBM Spectrum Protect software supports highly available virtualized and hybrid IT environments, offering:

- **VM-optimized, application-aware backup services** for a range of operating systems and production workloads. IBM Spectrum Protect supports a unified strategy for physical and virtual server protection, incorporating hardware-assisted snapshots and traditional backups.

- **Private cloud optimization**, including recently announced support for Amazon and Azure cloud environments.

- **Built-in efficiency** to support requirements for deduplication and incremental-forever backup. IBM Spectrum Protect builds high efficiency into software, reducing or eliminating the need for additional appliances.

- **Integrated, offsite, policy-based replication** to reduce the storage needed to support DR or hybrid clouds.

- **Self-service portals** to maintain service levels and reduce complexity.

- **Encryption and multi-tenancy**, including encryption of data in flight between subscriber and provider and at rest within the provider's repository. Multi-tenancy lets a cloud provider completely isolate each subscriber's data.

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Real-world Perspectives

To fully appreciate how IBM's data protection software product can partner with cloud platforms to help customers gain the huge potential benefits of a hybrid data protection architecture, ESG interviewed three partners who are delivering Spectrum Protect-based solutions.

IBM Resiliency Services

IBM is one of the most venerable names in business continuity and resiliency, with a range of hot-site, cold-site, and cloud services. The IBM Cloud Managed Backup service uses Spectrum Protect as a backup platform for the managed services that it offers. Cloud Managed Backup services are available to anyone but cater to the needs of larger enterprises and service providers.

> "*Many of our customers want to augment the robust protection and recovery capabilities that Spectrum Protect provides onsite with the agility and flexibility that a cloud service enables*," says Michelle Weston, IBM Resiliency portfolio leader at IBM. "*Spectrum Protect gives our customers and our IBM Resiliency Services a single platform that supports the variety of disks, tapes, and cloud repositories that our customers want—and we can combine that with IBM's own global services to ensure a successful outcome through expertise.*"

And while IBM Global Services will always be IBM Spectrum Protect's "first and best" partner, they are not alone.

Cobalt Iron, an IBM Partner

Cobalt Iron is perhaps best known for packaging IBM's backup software (previously known as Tivoli Storage Manager or TSM) within a turnkey appliance and then adding additional management UIs and remote services, in order to deliver IBM's renowned backup solution to a much broader range of organizations. And while Cobalt Iron does now deliver some appliances utilizing other backup software products, their core business is still powered by Spectrum Protect. Today, they deliver both physical and virtualized appliances that combine the on-premises solution with cloud services for both offsite data retention and remote management/support. The enhanced Cobalt Iron instrumentation and expertise has also resulted in huge savings for IBM customers by reducing overprovisioning through analytics, deduplication, usage of cloud capacity for colder data, etc.

> "*As IT complexity continues to increase, Cobalt Iron makes it simple for organizations of all sizes to gain the benefits of Spectrum Protect on- and off-prem, without being long-time backup experts*," said Mark Ward, VP at Cobalt Iron. "*We've built our business on Spectrum Protect, which has given us the opportunity to provide huge service capabilities to our customers through ensuring that they get the agile recovery RTO/RPOs that they need, with rightsized hardware and very efficient deduplication, which is assured through cognitive smart-rule-based protection policies and discovery mechanisms, and managed in partnership with the Cobalt Iron team.*"

Nyherji, a Service Provider

Pétur Eyþórsson from Nyherji, a Service Provider in Iceland, has been watching the shift towards hybrid cloud usage for several years and shared two key observations about the evolution of hybrid data protection architectures regarding compliance achievability and the power of analytics on well-managed data.

- Compliance in heavily regulated industries is absolutely achievable using hybrid on-premises plus cloud services (despite the naysayers), but like any compliance discussion, it is as much about the process/people as it is the technology. That said, IBMSP has some distinct technical advantages when it comes to hybrid DP architectures, most notably in deduplication efficiency, which results in less network-transmission impact, as well as less consumption of cloud storage.

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

- In addition, huge value can be gained by utilizing SP's analytics and insights on the data under management to ensure proper retention and destruction. Even more can be done when combined with third-party analytics and copy data management (CDM) capabilities, like those from Catalogic, in combination with IBM SP's own framework.

The Bigger Truth

A hybrid approach to data protection (specifically in regard to backup, snapshotting, and replication) should be a coveted aspect of a hybrid on-premises/cloud-based IT infrastructure. For many organizations, D2D2C backup is likely in their future—secondary protection disk for agile recovery, and tertiary cloud services providing offsite survivability and boosting BC/DR preparedness. The true value of a hybrid architecture lies in its agility and in its appealing economic model. Those attributes arise from harnessing cloud services and impressive software together.

Aside from offering an alternative economic model and superior service delivery, cloud providers can also often offer outside expertise. By leveraging the technical expertise and on-premises insights of IBM Business Partners who are well versed in helping clients migrate production and protection environments to the cloud, organizations have even less of an excuse to put off reimagining their IT future in a cloud-first world. The expertise of IBM, often in combination with their partners, can be invaluable, particularly considering the complexities of modern heterogeneous IT infrastructures and the assorted skills needed to back up data, recover it, and architect durable BC/DR frameworks and policies.

The word "hybrid" encompasses media (disk, tape, and cloud), topologies (onsite and offsite), and expertise (in-house and external). *But the common denominator is the software.* It leverages the media, operates across the topologies, and is the tool of the skilled experts. As a perennial leader in data protection, IBM knows this. So it should be no surprise that it is continuing to innovate its products, services, and channels to deliver on hybrid protection's great potential.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

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

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.