

Solution Showcase

The Spectrum Data Protection Portfolio from IBM Is a ‘Must See’

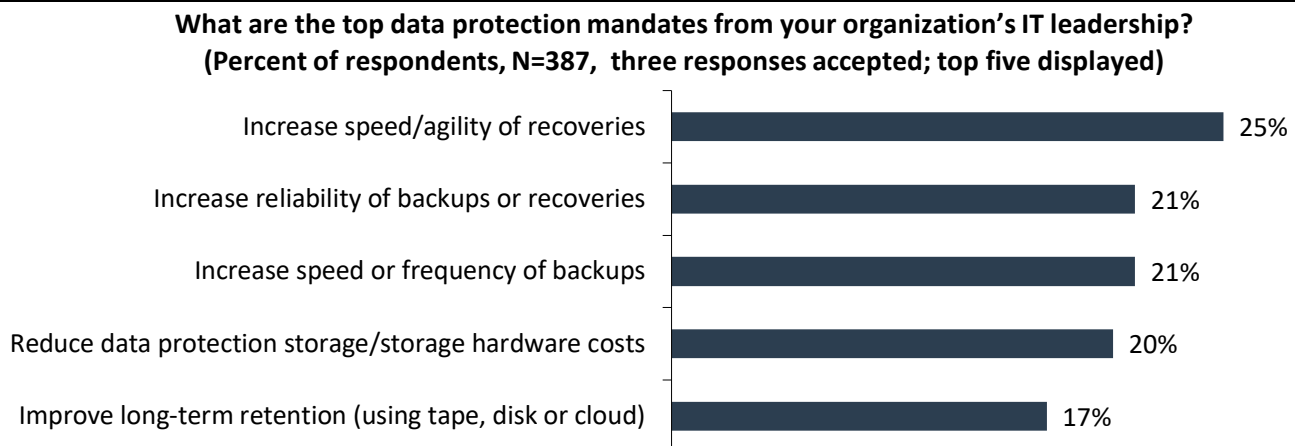
Date: October 2017 **Authors:** Edwin Yuen, Analyst; and Monya Keane, Senior Research Analyst

Abstract: IBM’s Spectrum Protect offering boasts more than 20 years of achievement in the protection and recovery of key IT systems. So, it would be easy to suppose that IBM’s new Spectrum Protect Plus and Spectrum Copy Data Management software offerings simply represent “Spectrum Protect with extra features.” That assumption would be incorrect. They are standalone, reimagined approaches aiming to solve a daunting IT challenge—virtualization protection/recovery—and aspiring to attain a coveted IT outcome—effective data management and enablement (DM&E), referred to by many as “copy data management” (CDM).

Introduction

ESG’s research shows that senior IT leaders are issuing mandates across their organizations to simply “do better” in their data protection initiatives (see Figure 1).¹

Figure 1. Top Five Data Protection Mandates from IT Leadership

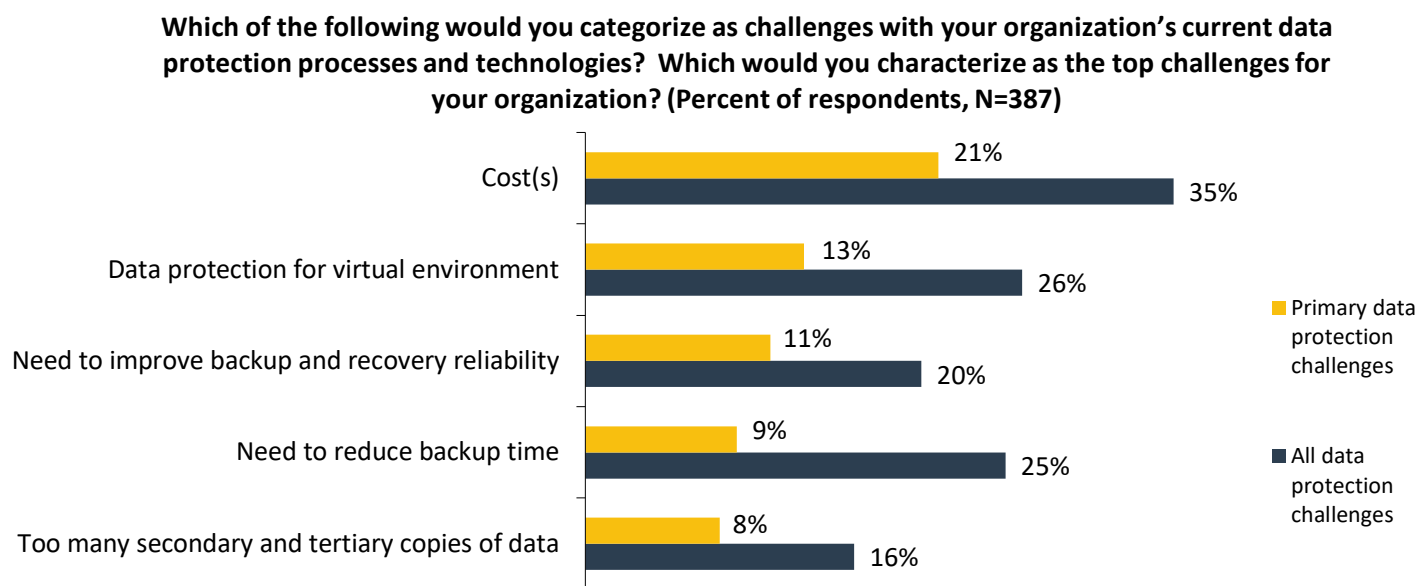


Source: Enterprise Strategy Group

Notably, IT professionals tasked with data protection are focused on similar improvement/reduction-related actions, while also trying to manage costs and the challenges related to protecting and recovering virtualized environments (see Figure 2).²

¹ Source: ESG Research Survey, *2017 Trends in Data Protection Modernization*, December 2016.

² *ibid.*

Figure 2. Top Five Challenges with Current Data Protection Processes and Technologies

Source: Enterprise Strategy Group

Modern Challenges Require Modern Solutions

For 2017, many organizations cited increasing the use of server virtualization and improving data backup and recovery as areas of significant investment for data center modernization.³

But as the data cited in Figure 2 shows, virtualization creates protection-related challenges. Similarly, the many copies of data created in the course of pursuing protection and non-protection initiatives brings challenges, too.

With so much pressure to reduce storage costs while increasing recovery flexibility and agility, it would be easy to wrongly presume that the two initiatives always conflict with each other. Better recovery flexibility really can be achieved while reducing costs (or increasing the business value recognized from those costs), which is exactly what organizations should be striving toward:

- Improved virtualization recoverability and assuredness.
- More efficient, more cost-effective data management and enablement.

Improved Virtualization Recoverability and Assuredness

In 2017, it should no longer be a simple question of *if* you can adequately back up a virtual machine or a set of VMs residing on a host. Although that effort was admittedly once challenging, today's data protection APIs from VMware, Microsoft, and other hypervisor vendors now provide reliable mechanisms for the backup of basically any VM.

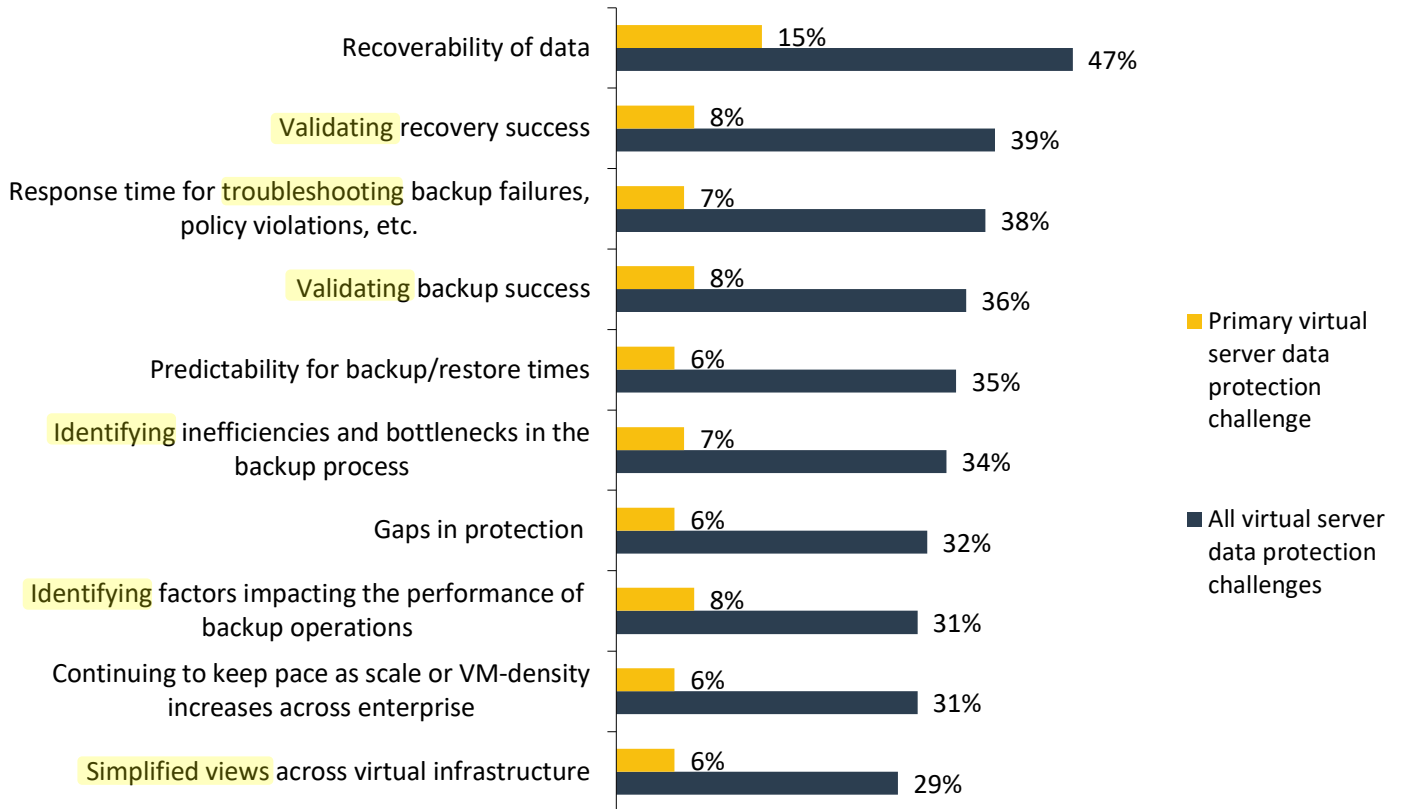
What remains as a true area of differentiation is recoverability and achieving *comprehensive* protection within virtual environments, a goal that often still plagues organizations (see Figure 3).⁴

³ Source: ESG Research Report, [2017 IT Spending Intentions Survey](#), March 2017.

⁴ Source: ESG Brief, [Reliable Virtualization Protection Continues to Elude Many Organizations](#), October 2017.

Figure 3. Top Ten Challenges in Protecting a Virtualized Server Environment

Which of the following would you characterize as challenges for protecting your organization's virtual server environment? Which would you consider to be your organization's primary virtual server data protection challenge? (Percent of respondents, N=400)



Source: Enterprise Strategy Group

As Figure 3 shows, the top virtualization-specific data protection challenge for respondents remains the recoverability of data (which truly should not be the case, yet it is). But also notable are the other frequently cited challenges: As Figure 3's highlighted words indicate, they all relate in some way to *visibility*. Many of these visibility-related challenges still exist because some data protection solutions are simply not "virtualization savvy." In other words, they lack the instrumentation and the contextual awareness to be able to show virtualization admins, IT operations admins, and other stakeholders the true protection and recovery status of their virtual environment.

Going forward, organizations will only increase their level of virtualization further. So those affected IT professionals need to search for modern data protection solutions that are equipped with good instrumentation and designed with the agility of a highly virtualized environment in mind.

Efficient, Cost-effective Data Management and Enablement (DM&E)

The key to effectively delivering the myriad recovery outcomes organizations require is to unlock the business value of secondary data. When the IT organization unlocks that value, it can also better justify the protection mechanisms in use. As the data depicted in Figure 2 showed, cost—particularly the cost of having too many copies of data—is one of the top challenges experienced by data protection professionals today. Similarly, the reduction of storage-related costs is a top mandate from IT leadership (see Figure 1). The conflicting reality for the IT pros is that the level of recoverability and agility that business-unit stakeholders demand can't always be met by backups alone.

That is why data protection admins, to meet their organizations' SLAs, are finding themselves making *more* (actually, a broader range of *types* of) copies via snapshots; replicas; and full, incremental, and differential backups. In truth, the partial and temporary nature of snapshots combined with the flexibility of replication can reduce storage when they are managed holistically and underpinned by a modern storage architecture. But, without those integrations and complementary strategy, protection storage can increase in response to addressing recovery goals, even as executive management is demanding that storage-related cost reductions occur. Exacerbating the problem, other IT teams (i.e., application developers and IT operations personnel) are generating still more copies to support their own development and patch-management efforts.

By enabling “non-protection scenarios” (such as DevOps, reporting, or analytics) while mindfully deleting, compressing, and otherwise optimizing storage *and* utilizing smarter data protection mechanisms, an organization really can:

- Achieve its recovery and business-agility outcomes.
- Establish a holistic long-term approach to data management and reuse.
- Succeed at being responsible stewards of the available IT budget.

As such, any organization striving for modern data protection should be looking for solutions that provide a comprehensive range of recovery capabilities while unlocking incremental business value by enabling non-protection use cases.

Comprehensive Protection with IBM's Software-defined Storage Portfolio

[IBM](#) and its Spectrum Protect software (formerly known to some as Tivoli Storage Manager or TSM) has been a leading innovator in enterprise data protection for many decades. However, it would be a mistake to presume that the offering has grown as stale as some other legacy backup solutions have. The core Spectrum Protect product has continued to evolve to meet the needs of modern enterprises, and IBM has just expanded its storage portfolio with [IBM Spectrum Copy Data Management](#) (Spectrum CDM) and [IBM Spectrum Protect Plus](#) (SPP).

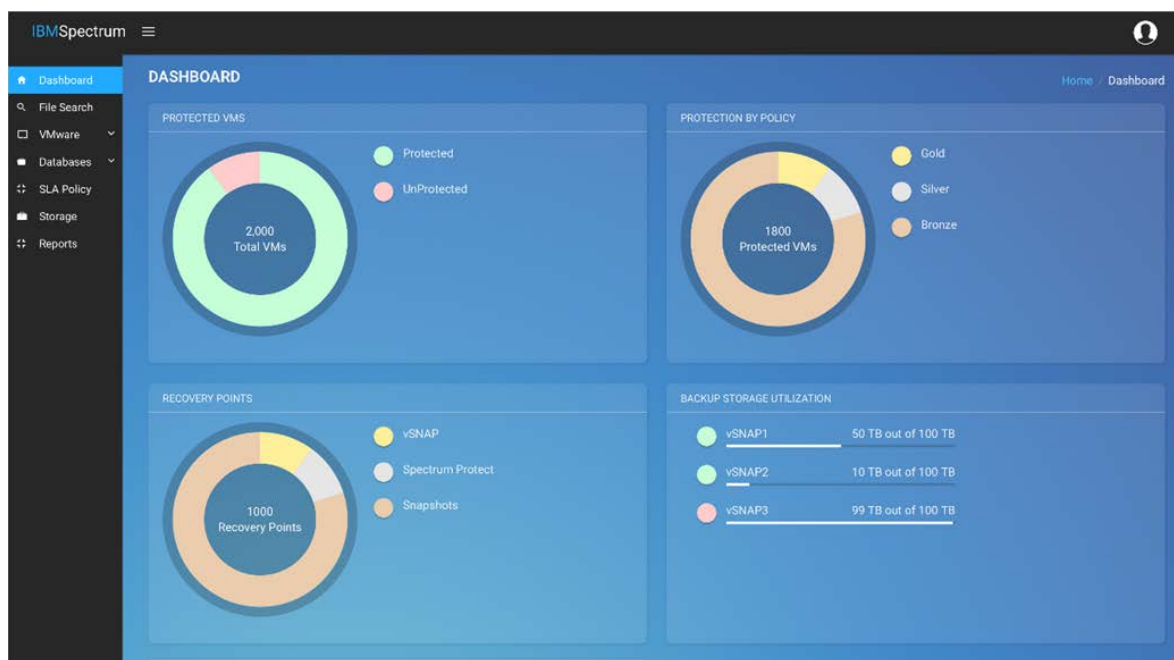
IBM Spectrum Copy Data Management

Spectrum CDM is a new addition to the IBM Spectrum data protection portfolio. It is designed to enable non-protection-related use cases for secondary data—for example, DevOps, patch testing, and reporting/analytics.

As with the other (albeit few) copy data management offerings on the market today, the primary goal of Spectrum CDM is to facilitate access to “production data” without compromising, encumbering, or altering the real production data sets. By leveraging Spectrum CDM, business unit employees, coders/developers, and a variety of other stakeholders are able to unlock incremental business value from that data. And that capability makes it easier for the organization as a whole to justify other investments in modern data protection and recovery.

IBM Spectrum Protect Plus

SPP is designed with IT operations generalists and virtualization admins in mind. It provides an SLA-centric framework for ensuring protection and agile recovery of highly virtualized environments, and it has a user interface (see Figure 4) that is sleek and contemporary enough to surprise long-time IBM stalwarts.

Figure 4. IBM Spectrum Protect Plus—Reporting Dashboard*Source: IBM*

It also possesses the “virtualization savviness” described earlier, whereby SLA policies are defined once by the applicable IT admin and then simply enacted—in either VMs or hosts—as business needs dictate.

And as one would expect, SPP and Spectrum CDM integrate with the core Spectrum Protect software and with the rest of the IBM storage portfolio, thus providing even broader business agility.

The Bigger Truth

Data protection must continue to evolve if it is ever going to address the challenges so many organizations are experiencing now. But interestingly, discrete, standalone backup mechanisms—and even dedicated backup admins—will likely recede in prominence as IT operations professionals continue to deepen their involvement in defining and implementing their organizations’ data protection strategies.

With that likelihood in mind, enterprises will almost certainly continue to rely on comprehensive data protection mechanisms such as IBM Spectrum Protect, even as they seek additional mechanisms that are accessible and purpose-built for their most prevalent workloads—mechanisms capable of unlocking incremental business value in support of a broad-based data management strategy.

Considering the way these trends are unfolding, it is good to see long-time data protection innovator IBM continuing to expand and enrich its portfolio with offerings suited to vAdmins and IT generalists. It is taking the right steps toward enabling the use cases that today’s businesses require.

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.