COMMVAULT

Why Modern IT needs a Comprehensive Approach to Data Protection

ESG GUEST BLOG SERIES

Contents

INTRODUCTION

In support of Commvault's recent announcements, ESG (Enterprise Strategy Group), was asked to provide a series of blog posts. Happy to welcome Jason Buffington, senior analyst at ESG, onto our blog page. He has been focused on data protection for more than 25 years, having worked as an IT implementer, at various channel partners and data protection software vendors, and at Microsoft. Jason will contribute a six-blog series that will focus on key issues related to data and information management, compliance, security and share his perspective on top customer considerations for establishing best practices in today's changing IT landscape.

"First and foremost, I want to congratulate Commvault on what is their most exciting series of announcements yet – and I've been watching them for most of my twenty-five years in the data protection market. One of the key reasons that Commvault continues to be recognized as a leader in the space is how their platform continues to evolve to meet ever-broadening customer needs in data protection." – Jason Buffington

Jason starts with why a **comprehensive approach to data protection** is important to organizations today and in the future. Next, Jason talks about how it can be interesting to consider Commvault's evolution within the backdrop of so many other major changes in the IT vendor landscape. In chapter 3, Jason explores Commvault's initiatives toward **"Governance from Inception."** He moves on to explore Commvault's initiatives toward enabling **"Analytics"** and **"Access & Collaboration."** Next, Jason explores Commvault's initiatives toward **"New Recovery Mandates"** and customer challenges in being **"Unable to meet demands."** Jason wraps up the blog series with his perspective on Commvault's initiatives towards **"Open Standards-based Infrastructure."**

Check out all of ESG's data protection perspectives from Jason at **http://bit.ly/jbESG**.

"One of the key reasons that Commvault continues to be recognized as a leader in the space is how their platform continues to evolve to meet ever-broadening customer needs in data protection."

JASON BUFFINGTON
Senior Analyst, Enterprise Strategy Group

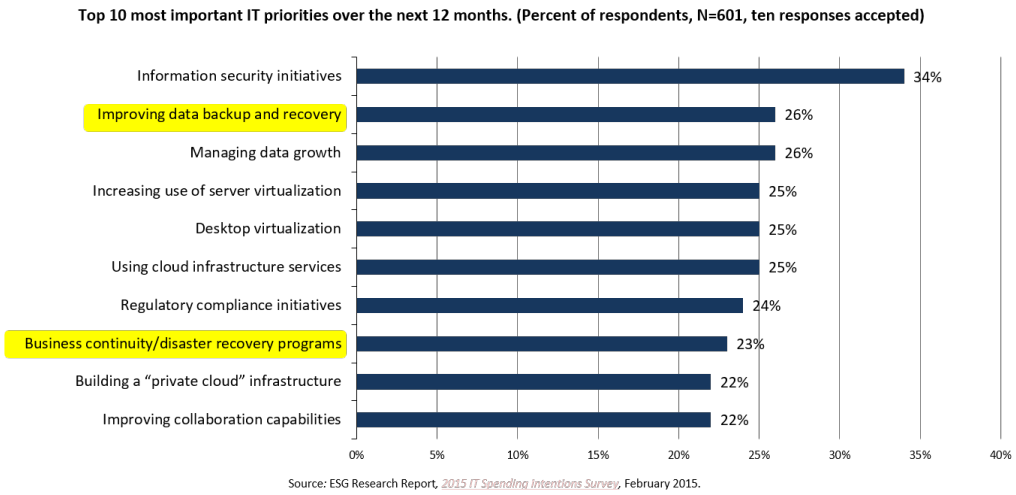
CHAPTER 1: YOUR DATA IS A STRATEGIC ASSET – TREAT IT THAT WAY!

WRITTEN BY JASON BUFFINGTON, SENIOR ANALYST AT ESG

First and foremost, I want to congratulate Commvault on what is their most exciting series of announcements yet – and I've been watching them for most of my twenty-five years in the data protection market. One of the key reasons that Commvault continues to be recognized as a leader in the space is how their platform continues to evolve to meet ever-broadening customer needs in data protection. Below is an ESG blog (http://www.esg-global.com/blog/how-to-plan-your-data-protection-spectrum-video) that encompasses my view as to why a comprehensive approach to data protection makes so much sense for organizations today and in the future. Over the next few weeks, Commvault has invited me to offer a series of blog posts to share ESG observations on changing customer requirements to data protection and data management – and my perspectives on how the new Commvault vision and its upcoming releases align with those market trends.

'Improving Data Backup and Recovery' is the number two most cited priority in 2015, according to ESG's annual IT Spending Intentions report. As important as that is, there is an even bigger story when considering that the most cited priority is Information Security (see FIG).

Top Ten IT Spending Priorities in 2015



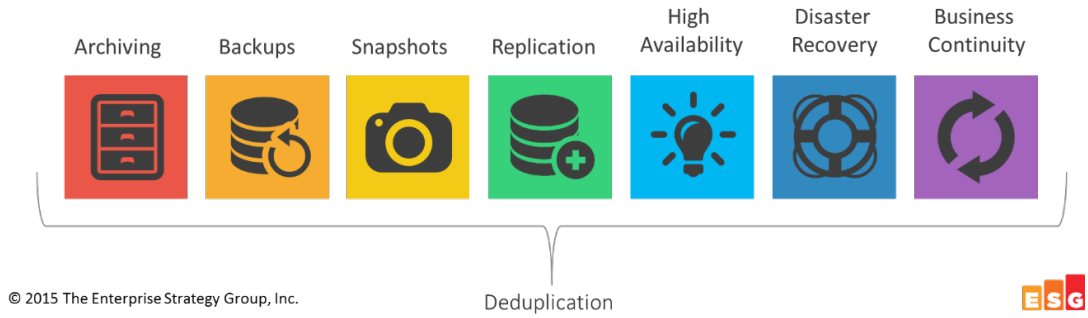
Essentially, what this data implies, continuing a similar story from ESG's 2014 research, is that even more than all of the production-enabling deployments and improvements that folks are doing, the top two most common IT initiatives are around 'protecting' what you have – your data!

There are two key reasons why backup continues to be invested in:

- Business units' reliance on their data and IT systems continues to heighten, such that any downtime or data loss is intolerable.
- The production platforms continue to diversify and evolve, resulting in inadequacies or even business impact when legacy approaches to backup are attempted on modern IT platforms.

In response to these IT realities, organizations of all sizes are looking for ways to increase the agility of their data protection infrastructure; often by supplementing backups with other data protection capabilities, such as snapshots, replicas and archives. Each of these data protection mechanisms offers a different kind of agility that compliment backups, as seen in FIG.

The Spectrum of Data Protection



To learn more about the Spectrum of Data Protection, check out **http://bit.ly/jbSpectrum2**.

As seen above, each 'color' on the Data Protection Spectrum compliments (not replaces) the other colors in the spectrum. In the same way, each data protection mechanism compliments (not replaces) the others, with different kinds of agility and/or recover-ability. And similar to how different colors in the rainbow may appear more prevalent, different 'colors' of the DP Spectrum may have different prevalence; meaning that while 'backup' may be applied across an entire IT infrastructure, snapshots, replicas and archives may only be applied across certain percentages of the organization, based on the varying business value of the data or IT availability mandates.

Unfortunately, while this hybrid DP method approach may be obvious to many, some organizations attempt to address each of the DP Spectrum mechanisms with disconnected technologies that often result in significantly higher costs and complexity, while still not meeting the actual business units' needs of improved and more comprehensive protection and recovery-agility. Instead, ESG recommends that organizations seek out integrated approaches to data protection that enable multiple 'colors' of the data protection spectrum in a single management/policy lens for ensuring one DP strategy that reflects and refracts all of the business units' recovery needs within a single prism.

CHAPTER 2: UNDERSTANDING COMMVAULT'S RELEVANCE IN THESE TUMULTUOUS TIMES

WRITTEN BY JASON BUFFINGTON, SENIOR ANALYST AT ESG

In 2015 alone, we've seen HP separate into two companies, Symantec separate to re-form Veritas and the announcement that Dell will acquire EMC, just a few years after Dell acquired and assimilated Quest – and certainly, the industry is not done expanding, contracting, adding new startups, etc. Each of these events has had markedly different influences on the data protection market within IT, and the Dell-EMC hasn't actually happened yet (and likely won't until well into 2016).

At the beginning of the year, my 2015 Data Protection Predictions video discussed some of the changes that were imminent: **http://www.youtube.com/watch?v=uVgmz36zJmE**

At around the three-minute mark, I talk about the anticipated flux in the industry:

2015 ought to be a year with a lot of change. Not only the what's being backed up by the who, but also the who you're going to get backed up with. A lot of the big data protection vendors are going through different kinds of reorgs of one kind or another. You've got a lot of the smaller data protection folks that are really getting pretty feisty and their tech is actually pretty good. I expect for you to see a couple of more closures, a couple of more acquisitions. There's a few folks I'm especially keen to watch because they're either going to explode and just get huge or they're going to implode based on a failure to execute their go-to-market strategy or their message doesn't line up with their products. But I think 2015 is going to be the year where there's going to be a lot of change and that's going to make it interesting to watch.

One company that hasn't merged, been acquired, split or imploded is Commvault.

To understand the relevance of that, you have to think both big and small:

- In the big picture, most of the other industry leaders acquired or developed their data protection offering(s) through acquisitions, in an effort to deliver a more complete set of solutions to their customers that also included servers, storage, or other systems. Many were successful in those endeavors to varying degrees, though some of those endeavors were later sold off when the 'whole wasn't greater than the sum of the parts.'
- In the smaller picture, many of the vendors in the discussion routinely listened to what their customers wanted from a comprehensive data protection solution. When faced with the recurring 'build vs buy' decision, they consistently chose 'buy' – often to deliver something to market sooner. The challenge then changes from 'building' the solution to 'integrating' within a broader portfolio; something that hasn't always been done well by some of those organizations.

"One company that hasn't merged, been acquired, split or imploded is Commvault."

JASON BUFFINGTON
Senior Analyst, Enterprise Strategy Group

In both lenses, Commvault stands on relatively unique ground:

- In the big picture, Commvault has consistently had a 'partner-centric' strategy, meaning a willingness to integrate with a wide variety of hardware and software partners in a complimentary way, whenever possible. As such, it has enjoyed a variety of OEM and bundling offerings over the years that would have been far less probable, if they were merely part of a hardware vendors' software portfolio.
- In the smaller picture, when Commvault's customers asked for new functionality, the decision was invariably 'build' instead of 'buy.' This resulted in a continually expanding set of integrated functionality – which likely fueled some of the sought partnerships from the bigger picture, regardless of the tumultuousness of the industry.

As the dust settles for HP and Veritas in their new organizations, each will very likely benefit from the refined focus, though each still has a broad portfolio to bring to market, which may be both a challenge and a differentiable opportunity. For Dell and EMC, each will earnestly endeavor to remain 'business as usual' for the next few quarters (since they are still separate), while continually having to fend off 'what/if/when' questions along the way – see other ESG **blog** and **video** on the Data Protection considerations of Dell & EMC.

As the Dell-EMC merger gets closer to reality, there will inevitably be some hesitation by customers and partners of both product lines to make longer-term bets, because **backup administrators are risk-adverse**. Our vocational task is to imagine business impacting scenarios that can be mitigated by IT implementations. A modern and comprehensive data protection solution is about removing risk to IT systems and services by enabling agility for remediation, recovery or restoration. So, anything that introduces risk, like potential end-of-life of products, changes in support systems (pre-sales or post-sales), etc. makes us hesitant.

To be clear, I am confident that each of the industry events mentioned, and others that weren't mentioned, will eventually result in vendors that are more likely able to build from their data protection pedigrees and eventually deliver unique and compelling offerings in market to their segments. But in the meantime, what will be interesting to watch is how more stable vendors that are continuing to evolve their offerings (like Commvault) will benefit as risk-adverse IT teams and their leadership consider who to partner with in 2016.

"In the big picture, Commvault has consistently had a 'partner-centric' strategy, meaning a willingness to integrate with a wide variety of hardware and software partners in a complimentary way, whenever possible."

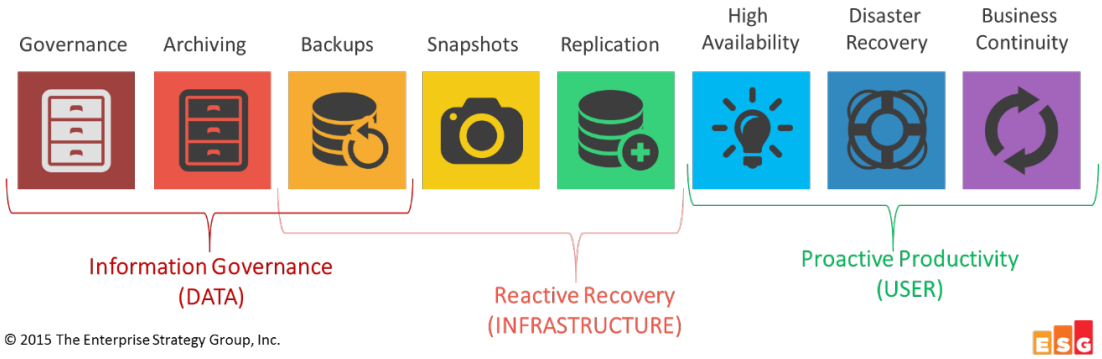
JASON BUFFINGTON
Senior Analyst, Enterprise Strategy Group

CHAPTER 3: 'GOVERNANCE IS MORE THAN IT, BUT THE IT HAS TO BE THERE'

WRITTEN BY JASON BUFFINGTON, SENIOR ANALYST AT ESG

If you've been following this blog series, we've used the Data Protection Spectrum model to describe a complimentary set of activities that are grounded in Backup, but are supplemented by snapshots, replication, etc. Outside of these blogs, ESG often contrasts the 'products/technologies' of backup/snaps/replicas and the 'processes/culture' of Business Continuity and Disaster Recovery (BC/DR) appended to the right side of the graphic.

Figure 3 – The Spectrum of Data Protection and Information Governance



In much the same way that BC/DR builds from the replication & high availability technologies with processes and procedures, Information Governance (IG) often builds from archival technologies with processes and procedures, as well. In fact, to take the analogy further, you can't buy BC/DR or IG.

- **To achieve your BC/DR goals,** you have to acquire reliable backup/snapshot/replication technologies, then add orchestration/processes and drive an operational culture that is prepared.
- **To achieve your IG goals,** you have to acquire reliable archival and backup technologies, and then add orchestration/processes and drive an operational culture that is intentional.

In both cases, it starts with technology that adds a layer of agility beyond *just* 'data protection.' And while BC/DR and IG are both *'more than technology'*, neither is accomplishable without the right IT components underneath.

- **For BC/DR,** you have to understand the business processes, the potential impact on key systems, and the organizational requirements of the users.
- **For IG,** you have to understand the data! You have to understand not what files or file-types (applications) that you have, but the business-value, regulatory-value and disclosure-value of the data itself.

And while the needs of BC/DR must be addressed through collaboration, IG's insight into the data is actually best addressed by technology that can ingest and understand the data, based on rules, patterns (in characters and usage) and policies. In wrapping up the blog series, there are some parallels to earlier entries that can be applied here:

- Similar to how non-DP additional copies are often cost-prohibitive unless part of a broader DP plus non DP strategy under '**Data Management,**' adding an archival solution that is data-savvy and can enable a broader Information Governance schema is also less practical when run as an isolated platform.
- Similar to how organizations' requirements for IT resiliency continue to evolve '**beyond backup-alone**', Information Governance isn't achievable as an afterthought. With data sharing and access technologies being so deceptively simple, your IG strategy (and the technologies that you apply to it) must be applied from the time data is created and govern it throughout its whole lifecycle.
- As discussed earlier, a broad **ecosystem of partners** wants to leverage a modern data protection infrastructure, in order for both solution platforms to help their shared customers with Information Governance needs. As such, having an open architecture that will allow the vertical or other partners (who understand their data even more than the underlying technology) can add tremendous value to a comprehensive IG strategy.
- Considering the convergence trends that have been discussed so far, it should come as no surprise that Commvault has incrementally evolved its platform for Governance in much the same way that it has evolved it for other customer data protection and data management scenarios – through a common code-base that is enhanced by listening to its customers and building what was necessary.
- And, in the spirit of tying the entire blog series, but especially poignant when considering Information Governance … remember, **your data is a strategic asset. Treat it as such.**

"Considering the convergence trends that have been discussed so far, it should come as no surprise that Commvault has incrementally evolved its platform for Governance in much the same way that it has evolved it for other customer data protection and data management scenarios – through a common code-base that is enhanced by listening to its customers and building what was necessary."

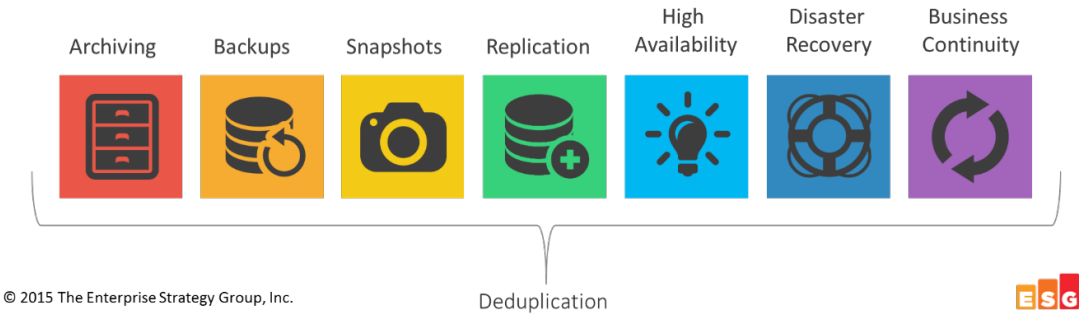
JASON BUFFINGTON
Senior Analyst, Enterprise Strategy Group

CHAPTER 4: 'GET MORE OUT OF YOUR DATA' THROUGH BETTER DATA PROTECTION

WRITTEN BY JASON BUFFINGTON, SENIOR ANALYST AT ESG

In the last installment in this blog series, we discussed the need for broader approaches to data protection that included not only traditional backups, but also snapshots, replication and other mechanisms within a single strategy and ideally managed through a common framework. The problem is that it would be nearly impossible try to address all of the methods of data protection that an organization likely should consider, if those methods were each attempted separately.

Figure 1 – The Spectrum of Data Protection



Because of this, ESG believes that for IT organizations to really be successful at addressing the myriad recovery/resiliency methods described above, the functionality throughout the colors of the Data Protection Spectrum must be integrated. But even that isn't the whole story.

If 'Data Protection' (DP) is the umbrella-term that encompasses all of the various functions depicted above, then 'Data Management' (DM) is an even broader umbrella term, including:

- The copies of data created as part of a data protection strategy
- The copies needed by other parts of the business outside of data protection – e.g. Analytics, Test/Dev, Collaboration, etc.
- The primary or 'production' copy of data

And again, as much as DP is infeasible for most, if attempted through disconnected mechanisms … DM is even more impractical through disjoined approaches. As such, primary data is often 'on its own,' DP mechanisms may or may not be concerted, and the other stuff never seems to happen. If that is the case, then step back and just look at the status quo. According to **ESG research**:

- Primary / production storage is growing at approximately 40% year-over-year
- Secondary / data-protection storage is growing at nearly the same rate (38%) year-over-year
- Unfortunately, data protection budgets are growing at 4.6% year-over-year

Quite literally, you cannot afford to keep doing what you are already doing. Whenever 'lifestyle exceeds budget,' you have two choices:

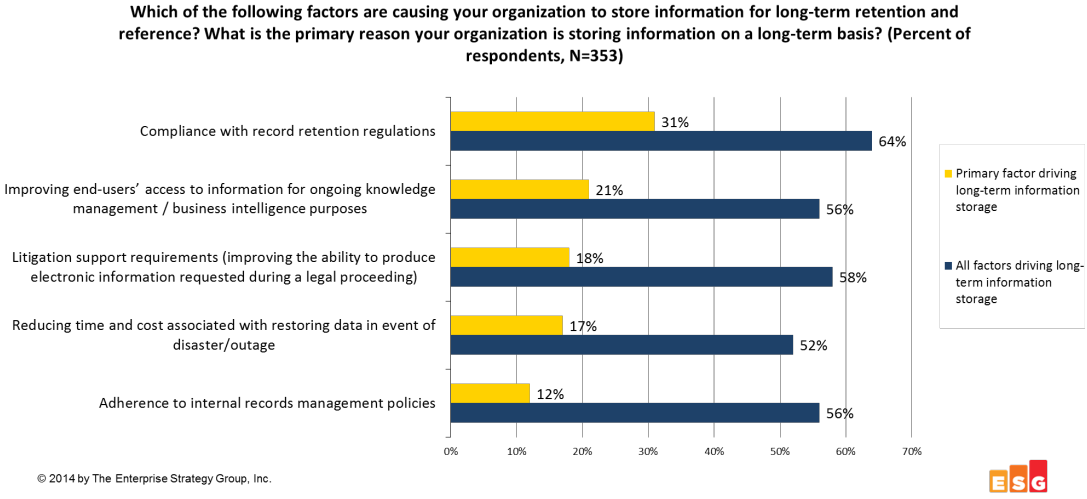
- 'Reduce your lifestyle' – protect less of your data or hold it for less time
- 'Increase your revenue' – get more value out of your data protection infrastructure

In reality, there isn't a choice to be made. It is very unlikely that you'll protect less. But it is highly likely that you can gain additional value out of your data protection infrastructure by leveraging its copies for non-data protection related purposes. After all, you have valid copies and access to your data that won't impact production, and yet is under IT management. The same DP infrastructure that ensures a rapid recovery for production purposes can also deliver rapid access for non-production purposes:

- Analytics – Understand what you have
- Access & Collaboration – Enable users' productivity

When ESG looked at the recognized benefits of their long-term data solution. the top response was what you might expect around regulatory compliance, which I'll cover in more detail around Information Governance in the next installment of this blog series.

Figure 2 – Why organizations store data for long terms



But behind regulatory compliance were user enablement scenarios that might surprise folks that haven't unlocked the value out of their data protection/data management system.

To make this more 'real,' consider the following: By utilizing your DP infrastructure for non-DP tasks, you are gaining more value out of the infrastructure that you already know that you need for the myriad backup/snapshot/replication needs that you already have. As such, one could infer that by unlocking that incremental value, additional funding might be recognized in deference to the new business-enabling scenarios that a modern DP (now DM) infrastructure can provide.

Commvault has steadily enhanced its platform around archival technologies, eDiscovery scenarios and snapshot/replica management to the degree that putting names around those use cases to address the 'Analytics' and 'Access/Collaboration' scenarios that IT organizations are struggling to deliver makes sense.

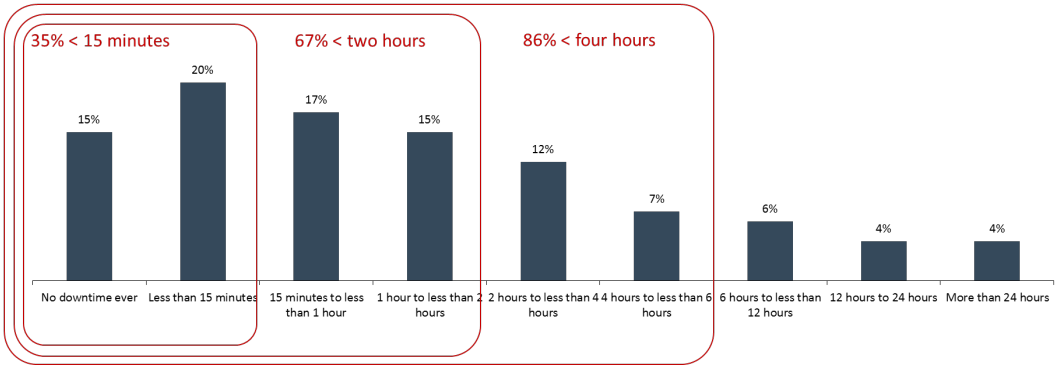
CHAPTER 5: 'NEW AGILITY REQUIREMENTS' IN DATA PROTECTION

WRITTEN BY JASON BUFFINGTON, SENIOR ANALYST AT ESG

According to recent **ESG research**, organizations of all sizes continue to struggle to meet the ever-heightening demands for greater IT durability.

Figure 1 – SLA Expectations by % of servers

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)



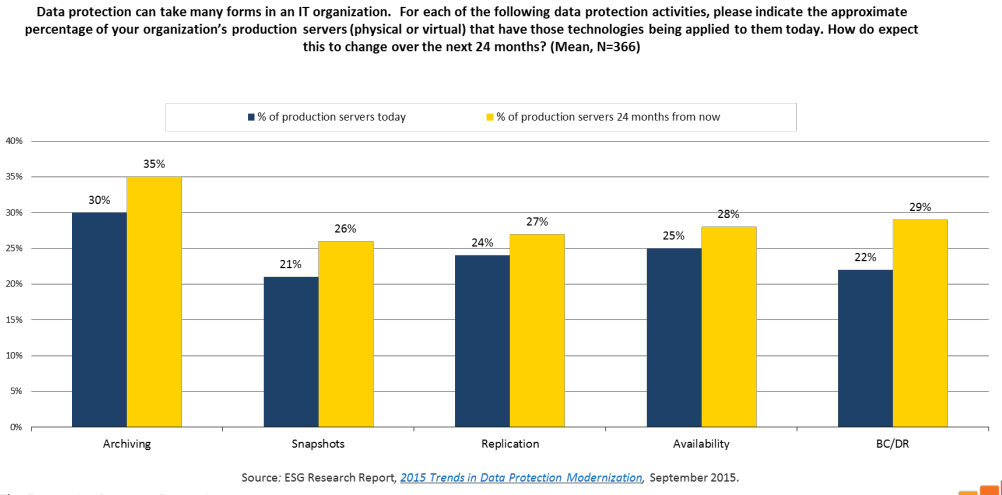
Source: ESG Research Report, *2015 Trends in Data Protection Modernization*, September 2015.

As shown above:

- Over one-third of servers (physical or virtual) have a downtime tolerance of fifteen minutes or less
- Another third of servers (physical or virtual) have a downtime tolerance less than two hours
- In fact, only one in seven servers (14%) can tolerate downtime greater than six hours, which is frankly where traditional backup is most suitable.

For the other 86% of servers that cannot tolerate six hours or less, a combination of rapidly recoverable VMs, snapshots and replication is often used to supplement traditional backup mechanisms. In fact, not only do roughly one in four environments use at least one of these complementary data protection mechanisms today, but their usage is expected to increase moving forward.

Figure 2 – Supplemental methods of Data Protection Beyond Backup (DPM'15)

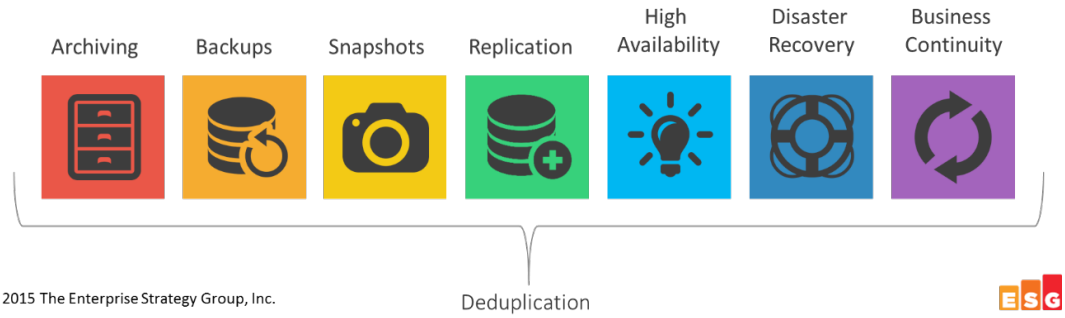


Source: ESG Research Report, *2015 Trends in Data Protection Modernization*, September 2015.

When you look at the service level agreements (SLAs) required by organizations today, and the inability to meet many of those SLAs with traditional backups alone, something has to change! In response to that, the methods for protection used by IT organizations of all sizes continues to evolve, in order to meet heightening yet diversifying recovery goals. Some organizations have attempted to address each of these types of data protection with various point solutions and eventually realized that the separate management frameworks and separate storage solutions used in disparate methods becomes economically and operationally non-sustainable over time.

Instead, ESG recommends that the diverse data protection methods be 1) planned as part of a unified strategy, 2) hopefully managed in consolidated framework(s) and 3) ideally delivered through an integrated set of functionality. ESG covered this in its discussions of the Data Protection Spectrum.

Figure 3 – The Spectrum of Data Protection



This is an area where Commvault has truly excelled, by building on its primary backup/recovery solution and evolving over the years as their customers' requirements for data protection, preservation and agility have grown – including snapshots, replicas and archives – all managed within the same UI that helps ensure a single strategy is enacted that enables various recovery scenarios (near-immediate, secondary-site or years-ago). In fact, some organizations are first introduced to Commvault, not for their own backup offering, but through their Intellisnap offerings that were made available by a range of storage solution providers looking for either snapshot management or integration between snapshot and backup recovery methods, including NetApp, Nimble, Fujitsu, Hitachi and more.

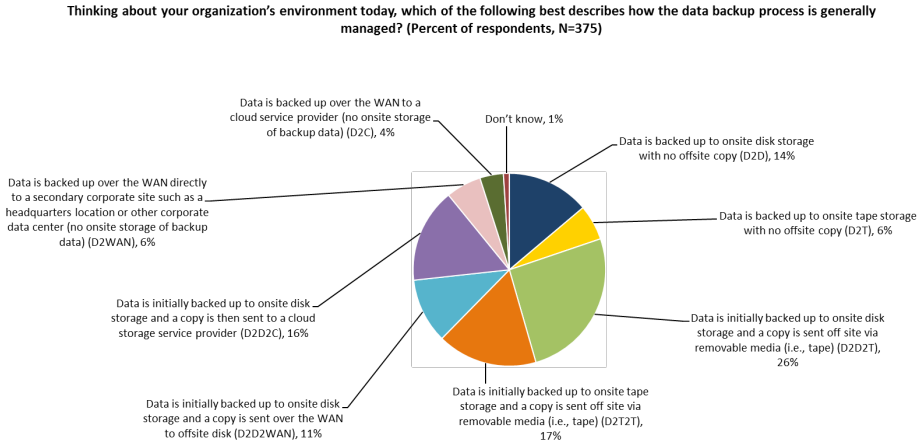
CHAPTER 6: 'HYBRID EVERYTHING' IN DATA PROTECTION

WRITTEN BY JASON BUFFINGTON, SENIOR ANALYST AT ESG

According to recent ESG research, in validation of what you likely have presumed, data protection infrastructures are becoming more diverse.

- Only a fourth (27%) of IT organizations utilize a single backup tool for their data protection solution today.
- Most organizations are supplementing backups with snapshots, replicas, archives and availability capabilities for more agility
- And organizations to use every possible permutation of disk, tape and cloud media in various combinations for their backup solution, as shown in FIG.

FIG – Primary Backup Media Topology in use in 2015 (DPM'15)



Source: ESG Research Report, *2015 Trends in Data Protection Modernization*, September 2015.

This should NOT be misinterpreted to read that organizations should acquire multiple disparate tools and storage technologies, thereby creating isolated islands within their IT infrastructure. What it does mean is that modern IT architectures should encompass a single data protection strategy that includes various data protection behaviors (snaps, replicas, backups, archives) and utilizes whichever mediums of storage make the most sense, based on operational requirements and economic initiatives.

In some cases, you can absolutely use a single data protection and management framework for everything (e.g. Commvault software as an example). In other cases, there might be reasons (business, organizational, technical or cultural) that justify secondary technologies as part of your broader data protection or data management strategy. The challenge for DP vendors (like Commvault and others) will be to either stubbornly believe in an 'all or nothing' approach to enabling their customers' data protection goals, or be open to being a good citizen within a heterogeneous world.

With its forward-looking emphasis on 'Open Standards,' Commvault is showing itself to be the latter – by enabling third parties to leverage its management and storage platforms, Commvault is showing that it recognizes what is truly important: providing value-creating management and agility within a complex IT infrastructure, while ensuring its customers have the flexibility necessary to achieve unique recovery and agility requirements. This can be seen first through the modularity of new Commvault solution scenarios, growing to where the whole is greater than the sum of the parts – and taking it a leap forward by adding even more parts from partners, within a unified framework from Commvault. To be more specific, Commvault now delivers a unified UI, a unified storage capability (including a very wide array of disk, tape, and cloud offerings), and a refined operational experience based on which functionality has been acquired. One analogy for this approach might be a hamburger:

- The top bun = an all-encompassing management UI.
- The bottom bun = a unified approach to hybrid storage for secondary, tertiary, or other copies.
- The meat = a flexible and heterogeneous data protection engine.
- The condiments = where the flavor is tailored to the Commvault customers' scenarios and preferences.

Now consider what an open-platform approach might yield: swap Commvault's data protection built-in burger for a chicken filet, a veggie patty, or a Portobello mushroom from one of its partners, and the customer experience (enablement) becomes radically enhanced, with the same management top bun, the same flexible and ubiquitous storage bottom bun, and the same diversity of condiment flavors for customization. Now consider serving the same burger/flavors in a different bun … e.g., a customized UI offered by a cloud provider or vertical partner!

Ironically, by growing beyond a monolithic approach of 'must protect it all,' Commvault may actually find more increased affinity, instead of reduced penetration, across diverse teams throughout a growing customer base.

"…Commvault is showing that it recognizes what is truly important: providing value-creating management and agility within a complex IT infrastructure, while ensuring its customers have the flexibility necessary to achieve unique recovery and agility requirements."

JASON BUFFINGTON
Senior Analyst, Enterprise Strategy Group

ABOUT JASON

Jason Buffington is the senior analyst at the Enterprise Strategy Group covering Data Protection. He has been focused on data protection for more than 25 years, having worked as an IT implementer, at various channel partners and data protection software vendors, and at Microsoft. Check out all of ESG's data protection perspectives from Jason at **http://bit.ly/jbESG**.

ABOUT COMMVAULT

Commvault's data protection and information management solutions provide mid- and enterprise-level organizations worldwide with a significantly better way to get value from their data

Commvault can help companies protect, access and use all of their data, anywhere and anytime, turning data into a powerful strategic asset.

Founded in 1996, Commvault is publicly traded (NASDAQ: CVLT) and headquartered in Tinton Falls, New Jersey.

As the world becomes increasingly data-driven and reliant on digital technology, all businesses have a once-in-a-generation opportunity to revolutionize themselves — to get more value from their data by activating it. Read more at **commvault.com/data-management-platform**.

COMMVAULT

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM