Technology Brief

‘Multiple Data Protection Solutions’ Does Not Have to Mean ‘Multiple Vendors’

Date: June 2014 **Authors:** Jason Buffington, Senior Analyst; and Monya Keane, Research Analyst

Abstract: *Although modern backup solutions can offer significant recovery agility, backup as an IT process is generally less than “enough” for the data protection goals that IT is being asked to deliver. As IT is embracing snapshots, replication, archiving, and availability mechanisms to enhance business continuity/disaster recovery (BC/DR) preparedness, it is important to realize that there is a better way than piecemealing each component, and then wondering why CapEx and OpEx are so out of line.*

Overview: Backup Alone Is No Longer Enough

ESG research shows that today, 83% of organizations have a downtime tolerance for high-priority applications of three hours or less, and 49% have a downtime tolerance for those high-priority apps of just *15 minutes or less*.[1]

Those downtime tolerances are extremely low, but they are what one would expect for a business’s most vitally important workloads. The research’s more interesting finding actually relates to the downtime tolerance levels reported for the various “normal” apps that support operations but aren’t quite mission critical. Today, 23% of organizations reported *also* having a 15-minutes-or-less downtime-tolerance profile for these “normal” apps. And most organizations (62%) reported a downtime-tolerance profile of three hours or less for those apps. The findings reinforce a big point: *We have never before been so dependent on **all** of our data.*

That’s one reason why backup alone is not enough anymore—for a global enterprise or for a small business. By itself, backup can’t provide the level of infrastructure agility and data-recovery assurance we all need today. Consider this: In a traditional backup environment, it can take more than three hours just to pinpoint that a problem has occurred, figure out where it happened, why it happened, and how to fix it. Then, finally, data restoration can begin.

Backup and restore alone don’t allow IT organizations to meet the demands of their end-users regarding constant data access. Because of that, ESG sees the majority of folks looking at supplementing backup with snapshots, replication, or both.[2]

Backup, snapshotting, and replication are parts of the myriad data protection strategies that are available to customers today. But candidly, it is becoming mere table stakes to include all of those methods somewhere within an IT environment. It is not just that “backup is good enough” and snapshots are aspirational. To meet the data availability goals that we see today, organizations really need to be leveraging *more*.

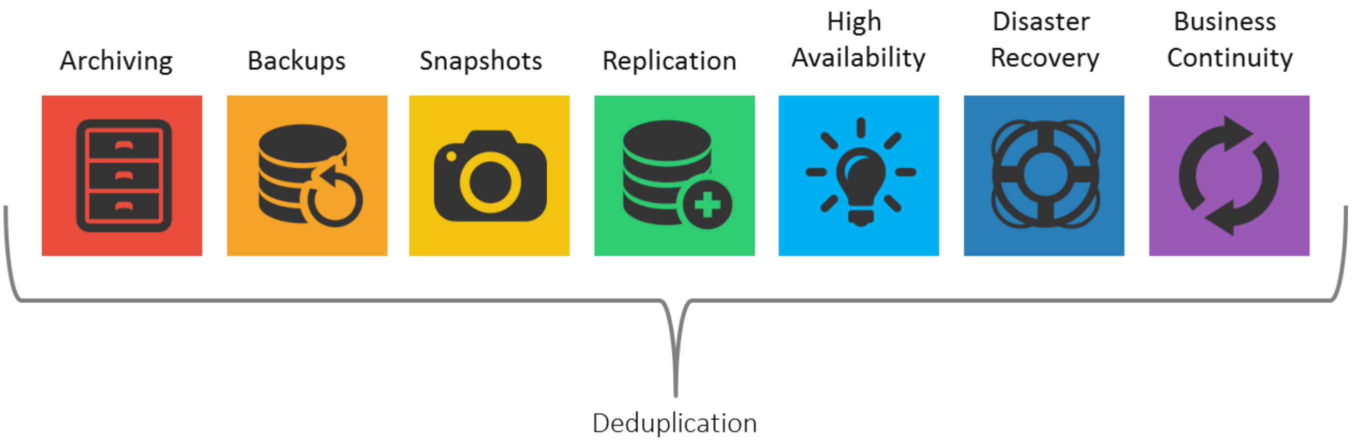
According to ESG research, less than 10% of all data protection strategies for virtualized environments (which basically covers everybody these days) are using only VM-specific backups. The other 90% are using snapshots, replication, or both to supplement their backup strategies.[3] The point isn’t that backup is dead or going away; the point is that the foundation—the basis of data protection—may be in traditional backup and recovery, but for environments of almost all sizes, the solution really ought to be broadened to include snapshots and/or replication.

[1] Source: ESG Research Report, *Trends for Protecting Highly Virtualized and Private Cloud Environments*, July 2013.
[2] For more information, including a video, visit *How to Plan your Data Protection Spectrum*, February 2014.
[3] Source: ESG Research Report, *Trends for Protecting Highly Virtualized and Private Cloud Environments*, July 2013.

Defining a Data Protection Spectrum, Architecture, and Strategy

How does one define a data protection spectrum, a solution architecture, and a DP strategy? Start with understanding the business's availability and recoverability goals, and then select the right "colors" from that data protection spectrum—representing the activities that matter to your organization's success (see Figure 1).

Figure 1. The Data Protection Spectrum



Source: Enterprise Strategy Group, 2014.

Base your activities and goals on business-centric objectives. Using the spectrum, start with your goal, and then consider the "color" or IT process that will help you achieve it. For example:

- If you need to preserve data for content-specific purposes, *implement **archiving***.
- If you need to recover data selectively or en masse according to a range of previous timeframes, *use traditional **backups** in a deduplicated storage pool or contemporary tape or cloud solution.*
- If you need to recover to near-current points in time, *utilize **snapshot** technology (ies) within primary storage*.
- If you need data to be in more than one location, ***replicate** it*.
- If the data must be accessible all of the time, *safeguard that continuous usability through **high-availability** mechanisms on production servers and resilient storage*.
- If remote data needs to be accessible, *leverage your replicated copies for **BC/DR***.

Within any IT infrastructure, each of those colors has a most appropriate point of implementation.

Cohesive Interoperability

So, clearly, backup alone is not enough. But backup and all the other capabilities embodied in your data protection strategy do need to "talk" to one another in order to work together well. That outcome can't happen, however, if (for example) the application owner purchased the availability solution, the storage admin implemented snapshotting, and the backup admin implemented a backup/recovery disk solution that doesn't work with the archive administrator's installed platform.

If every one of the admins who owns a piece of the data protection infrastructure deploys a solution in a vacuum and is not part of the larger strategy discussion, you end up not only with technologies that don't talk to one another, but also with significantly more CapEx and more complexity/administrative effort because you've deployed more storage than you really need on the floor. Not to mention, when you buy point solutions from seven different IT vendors, none of them are as likely to be creative in pricing or configuration.

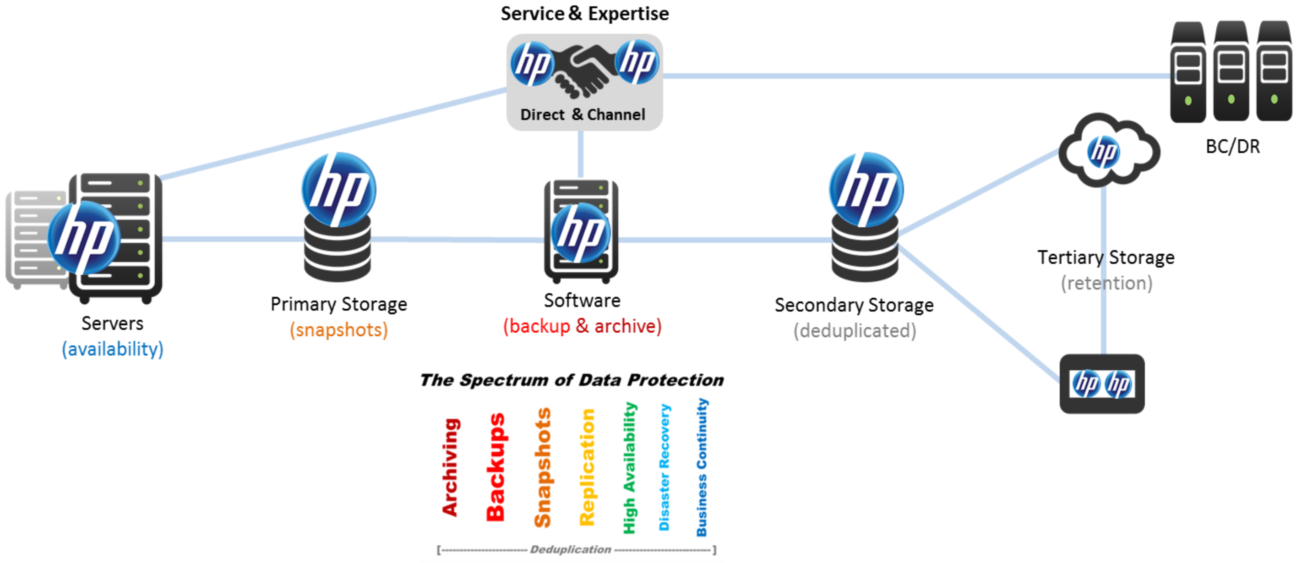
You have to reach a range of goals. But if you're buying your tools from a range of vendors, you may be creating another problem for yourself and your organization.

Don't Settle for Piecemeal

If you had an unlimited budget, you could pick seven solutions from seven vendors, each giving you the single capability that you need, and everything would be great. But *no one* has an unlimited budget. Thus, start thinking about the fact that diverse components, diverse technologies, and diverse mechanisms—while tying into the idea of creating an agile data center—do not necessarily entail buying only from a diverse set of vendors.

This is not to say that point solutions are bad; they are not. But a holistic approach should be considered carefully. Hewlett-Packard is one of the few IT vendors that can offer a complete portfolio (see Figure 2).

Figure 2. The HP Solution Architecture for Comprehensive Data Protection



Source: Enterprise Strategy Group, 2014.

If one were to move left to right across this solution architecture, it is apparent that HP has something in every bucket:

- On the left-hand side are the **servers**. HP has built its name by engineering servers that have revolutionized the IT industry as we know it today. That revolution did not stop with standalone servers. For example, the *HP ConvergedSystem* family of engineered systems (optimized for virtualization, cloud, and big data) combines server, storage, and networking into building blocks for the modern data center. Availability is best achieved where the application lives. Applications live on servers, and almost no one makes more servers than HP.
- Next is **primary storage**. One of the most recognized brands in high-performance primary storage today is *HP 3PAR StoreServ*. It offers a single, interoperable set of tier-1 data services across midrange, enterprise, and performance-optimized all-flash arrays known for their scalability, flexibility, and management simplicity. And of course, this is where storage availability and snapshotting come in through HP 3PAR StoreServ software including *Virtual Copy* and *Recovery Manager* to enable the integration of HP's storage protection capabilities with production applications and hypervisors.
- At the center of the image is the **backup and archive software portfolio**. The backup capability set includes *HP Data Protector* for backup and *HP Consolidated Archive* for archiving and discovery. According to ESG research, 83% of IT pro respondents indicated that the archiving capabilities within their backup solution were part of, if not their entire, archiving capability—with a strong preference for integrating archiving and backup within their solution portfolio.[4]

[4] Source: ESG Research Report, Backup and Archiving Convergence Trends, April 2014.

- Continuing to move to the right in Figure 2, HP has two entire product lines of **secondary storage**:
  - *HP StoreAll*, suited for archival scenarios. According to HP, it scales out to 16PB (potentially representing billions of files and objects), and it provides archive-services capabilities such as policies for data retention, "write once, read many" (WORM) write protection, auditing, and long-term data integrity validation. HP also claims that metadata analytics and searches can be performed up to 100,000 times faster through a mechanism the vendor calls Express Query.
  - *HP StoreOnce* has been making serious waves over the past three or four years for its higher performance, more predictable performance for backup and restore, and claims of lower TCO than many of the more recognizable brands and mindshare leaders in the deduplication storage market. Recognizing that *backup to disk is the first tier of recovery* really should be the standard approach for IT environments of almost any size. However, without **deduplication**, protecting to disk can be cost prohibitive for almost any organization. A high-performing, reliable, deduplicated storage silo is of paramount importance for the modern data center. This product now boasts "Federated Deduplication" to further ensure once-deduplicated, stays-deduplicated functionality, as well as HP's "Get Protected" guarantee of 95% deduplication.[5]
- "**Tape**" is not the four-letter word it used to be, with *HP StoreEver* providing contemporary tape solutions including LTO-5, LTO-6, and the LTFS technologies that enable tape to perform like disk in access and in performance.
- Then there's the *HP Helion Cloud*. From the CEO on down, HP has exhibited a commitment to the **cloud** as key to the strategy of the company, with data protection enablement certainly included in that viewpoint.
- Lastly, all the data protection capabilities HP offers are architected, implemented, and **supported** by HP's broad field salesforce, professional services organization, and channel partner ecosystem.

The Bigger Truth

A data protection strategy needs to be all-encompassing. "Backup" and "data protection" are no longer synonymous. Backup is a subset of a modern data protection spectrum that also should include the other colors of that rainbow because the business demands a greater amount of agility in recovery—more than backup alone can satisfy.

That being said, multiple methods of recovery and agility should not necessitate seven different point products from seven different vendors. Certainly, justifiable reasons to insert a best-of-breed component here or there based on a given workload or scenario exist, but many environments will find better CapEx and OpEx efficiency by using a portfolio designed by a single vendor to work together.

The key is to (1) assess the business's recoverability and agility requirements, (2) define the data protection capabilities that are required to achieve those objectives, (3) assess the current capabilities within the data protection product(s) that one currently owns, and (4) explore adjacent products and capabilities from the vendors one already works with to see where those solutions may be "broadened" to provide the rest of the required portfolio elements. In other words, if you are already using HP servers or HP storage, consider what the other parts of the data protection portfolio from HP might be able to do to enhance your IT environment. Between the assessment (the first key) that is offered with HP Get Protected and the portfolio of data protection capabilities described earlier (the last key), you may find that you don't have far to go in achieving the entire data protection spectrum with a single partner.

HP pub # 4AA5-1417ENW

[5] HP, Get Protected Guarantee, June 2013.