White Paper

Why the Cloud Should Be Part of Your Data Protection Strategy

How to Accelerate Production and Protection Capabilities in the Cloud-first Era

By Jason Buffington, Principal Analyst
and Monya Keane, Senior Research Analyst

July 2016

This ESG White Paper was commissioned by Microsoft and is distributed under license from ESG.

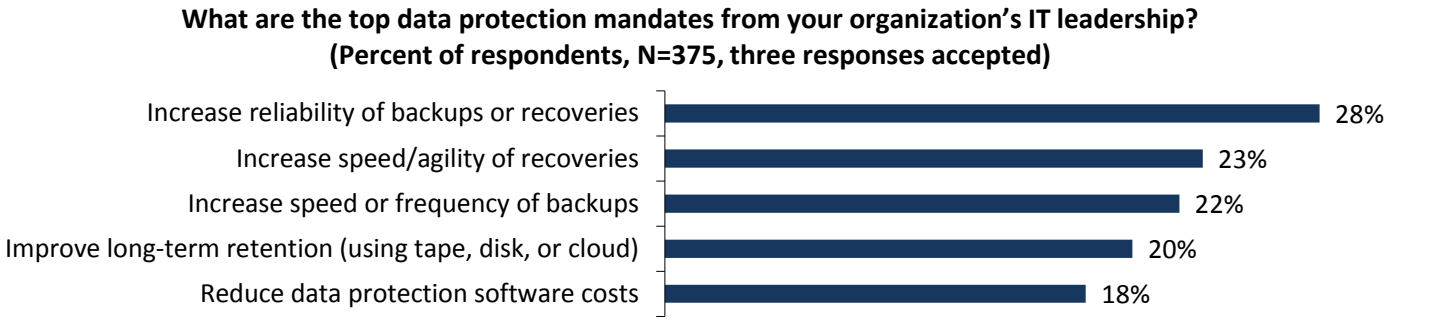
Contents

Introduction: Both Technical and Business Concerns Drive Data Protection Innovation

Many organizations are looking to allocate budget resources to increase their IT agility. That's because they know that improved agility can ultimately help them cut costs, ensure regulatory compliance, boost security, glean new value from their digital information, and achieve other important business drivers affecting strategic IT spending today.

However, not all organizations fully appreciate that IT agility initiatives will affect both *production* platforms and data *protection* efforts. The fact is that a number of IT leadership mandates can tie directly to protection, as Figure1 shows.[1]

Figure 1. Top Five Data Protection Mandates from IT Leadership



Source: Enterprise Strategy Group, 2016

Meeting executive-level mandates while simultaneously addressing cost concerns might require purchasing new technologies, considering new approaches, assessing new vendors, or even rediscovering long-familiar vendors that could support the desired improvements.

How Important Is the 'Protection Layer'?

It shouldn't come as a surprise that many organizations end up prioritizing backup and recovery either proactively (as part of their modernization efforts) … or reactively (after discovering that their legacy backup tools can't reliably protect their newer business platforms). Tactical efforts to improve backup and strategic efforts to improve overall agility were among the biggest priorities for 2016 among the IT decision makers surveyed by ESG.[2]

Large enterprises lead the way in seeking the latest approaches to data protection and systems management. In many large Microsoft IT environments, those deployments involve using Microsoft System Center (SC) and the Microsoft Operations Management Suite (OMS), delivered by Microsoft Azure.

It all ties back to the notion that the protection layer—e.g., data backup and information security—are often higher priorities than any single production-enablement solution. Smart IT leaders know that efforts to update a production platform always require incremental additional investments to strengthen that platform's protection. To put it simply: When you upgrade production, you *must* upgrade protection.

Why the Cloud Should Be Part of Your Data Protection Strategy

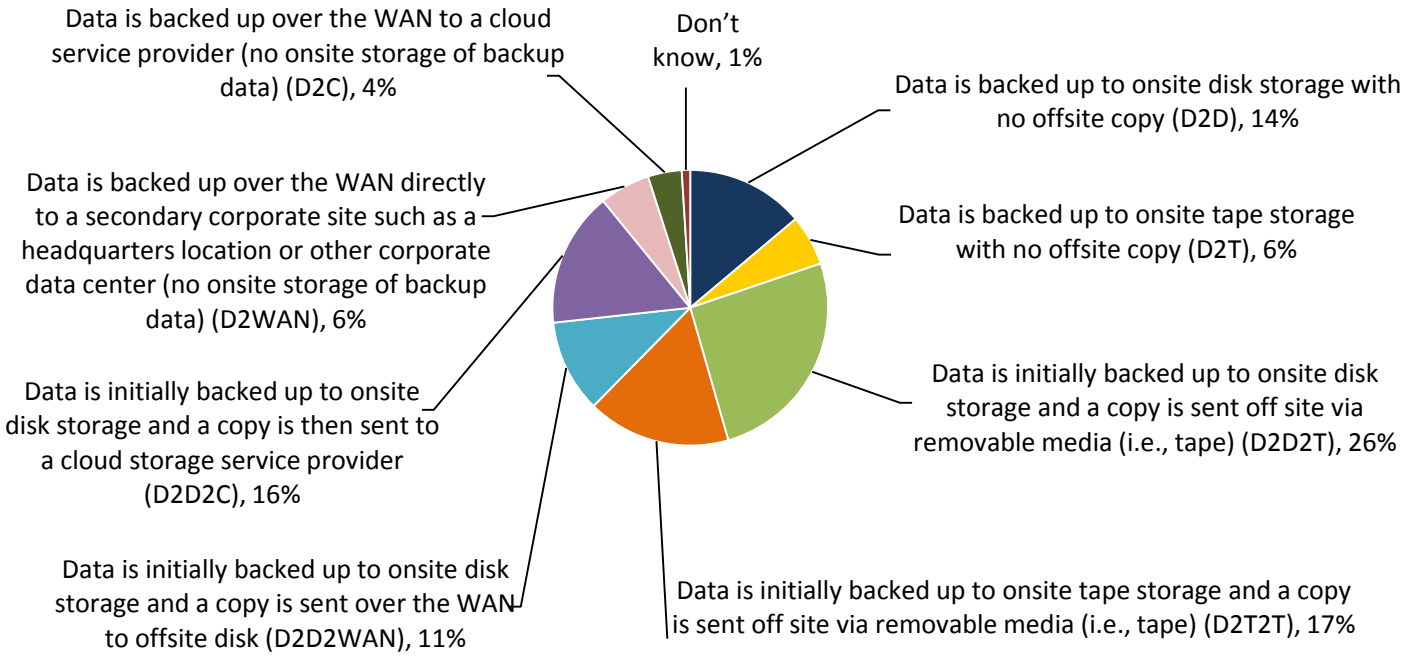
For organizations trying to improve IT agility and control costs, it's easy to understand why both cloud services and technologies associated with good ROI hold such appeal. Among the organizations surveyed by ESG, those two measures sit at the top of the list of cost-reduction/containment strategies being pursued this year.[3] Essentially, IT decision makers are holding costs down in 2016 by "doing IT smarter."

[1] Source: ESG Research Report, *2015 Trends in Data Protection Modernization*, September 2015.
[2] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.
[3] ibid.

With such emphasis on how the cloud and ROI drive decision making these days, it is appropriate to delve into where both the cloud and alternative protection media fit into data protection efforts. When it comes to backup, the choices aren't so simple; diverse topologies are all in use, as Figure 2 illustrates.[4]

Figure 2. Primary Data Backup Process

Thinking about your organization's environment today, which of the following best describes how the data backup process is generally managed? (Percent of respondents, N=375)



Source: Enterprise Strategy Group, 2016

Based on the topologies depicted in Figure 2, it is reasonable to reach two conclusions:

- **Most organizations are using local disk-based storage for first-tier recovery**, either through snapshots within production storage, or via highly agile, rapid restores from backup protection storage.
- **Tape protection is still more common than cloud protection, although that is evolving**. ESG research shows that the "tape versus cloud" decision shouldn't necessarily be a debate of "tape *or* cloud" but more often "tape *and* cloud"—with cloud usage growing faster than tape is declining (see Table 1), implying that each have their place in IT strategy while recognizing that cloud-based data protection is quickly becoming a mainstream scenario.[5]

Table 1. Data Backup Process: 2012 versus 2017

Media	2012 Reported Usage	2017 Anticipated Usage	Five-year Change
Tape	56%	45%	-22%
Cloud	7%	22%	+314%

Source: Enterprise Strategy Group, 2016

[4] Source: ESG Research Report, *2015 Trends in Data Protection Modernization*, September 2015.
[5] ibid.

Economic, Operational, and Functional Considerations for Data Protection

The choice of media for data protection is rarely determined by just one criterion. Thus, it is important to understand the broader implications of tape or cloud as a tertiary medium:

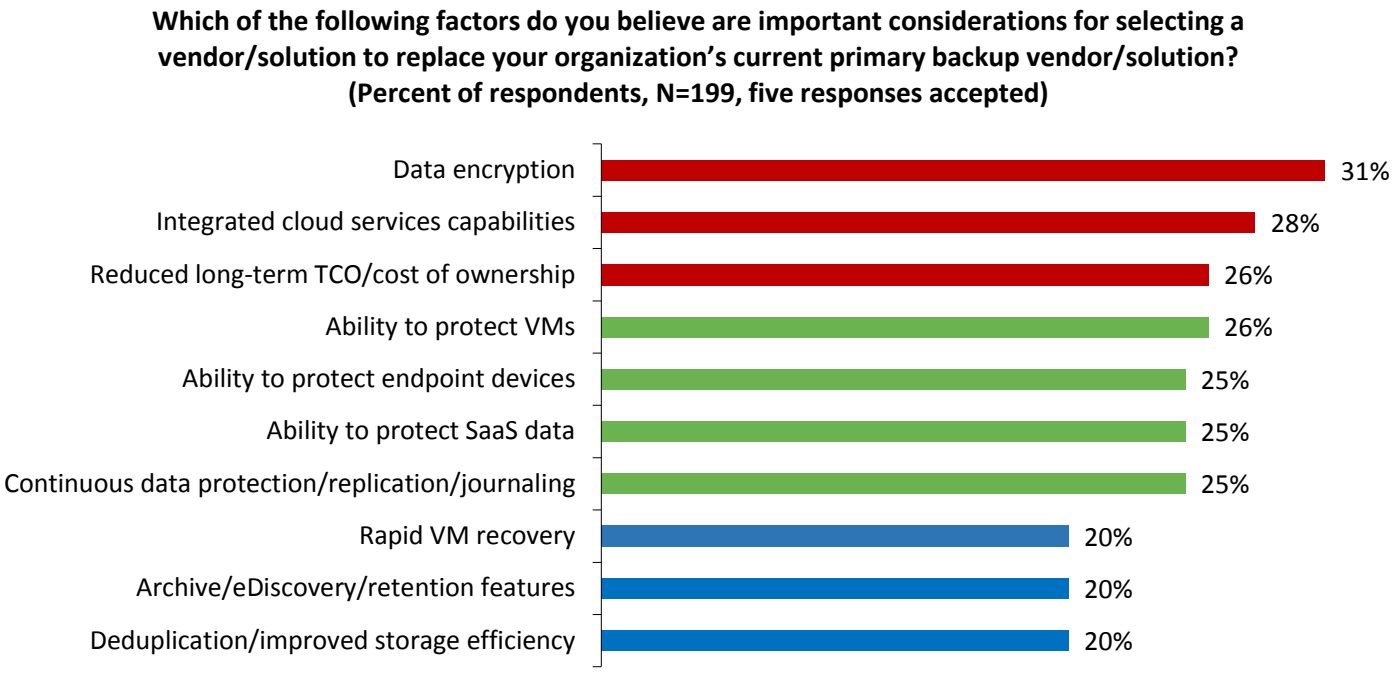
- Economic implications—Is "price per gigabyte" your main goal? The reasonable cost of tape and its lack of ongoing management requirements may be more compelling than disk solutions and even some cloud scenarios. However, cloud solutions offer a much wider range of operational and functional capabilities that tape doesn't.
- Operational implications—What level of effort does it take to manage your repositories? A tape farm is only as good as the inventory management and physical security controls in place around it. A cloud repository is an always-accessible live infrastructure managed by a professional service provider.
- Functional implications—What can you do with the stored copies? Tape's function is to store data until a restoration event arises. Cloud-based data can often be leveraged for other business-enabling purposes and may more effectively support data protection and recovery behaviors such as remote failover or BC/DR preparedness.

While many organizations may continue to rely on tape technology, particularly as part of their long-term retention or archival strategy, a growing number recognize the agility to be gained and the potential for unlocking incremental business value that comes with utilizing a cloud-based data protection capacity, as well (or instead).

What to Seek Out in a Data Protection Portfolio and Platform

When respondents are asked about important considerations related to selecting a new data protection vendor or solution, it is not a coincidence to again find them putting cloud and TCO near the top of the list, as well as expressing a need to protect diverse platforms such as highly virtualized environments and endpoint devices (see Figure 3).[6]

Figure 3. Top Ten Considerations for Selecting a New Backup Vendor/Solution



Source: Enterprise Strategy Group, 2016

[6] ibid.

Notably, even among the top seven considerations (red and green), two distinct types of drivers are propelling a better methodology for holistic data protection:

- Encryption, cloud, and TCO all point toward modernizing data protection approaches.
- Endpoints, VMs, SaaS, and replication all point to the assortment of systems and requirements needed to ensure robust data protection, regardless of the platform (server, service, or device) that the data resides on.

Microsoft's Hybrid Data Protection Solution

As organizations' IT environments grew more complex and expanded from traditional data centers to private and public clouds, a new system built "by the cloud, for the cloud" needed to emerge.

In today's heterogeneous world of multi-OS, multi-hypervisor, and even multi-cloud architectures, Microsoft has evolved its product strategy and its manageability framework and vision to accommodate ever-broadening platforms requiring management and protection. Some, but not all, of the Microsoft data protection technologies included within the vendor's broad vision are:

Microsoft has evolved its product strategy and its manageability framework and vision to accommodate ever-broadening platforms requiring management and protection.

- Azure Backup, an Azure service.
- Azure Backup Server (ABS).
- Microsoft System Center Data Protection Manager (DPM).

It is important to regard these technologies not as three different offerings but as vehicles for delivering Microsoft's overall backup offering. Azure Backup is the core service delivered through OMS, and the components can be combined in ways that provide the best outcome for a given organization. Microsoft wants its customers to know that it offers a single cohesive solution, namely, SaaS-based backup delivered through the Microsoft Operations Management Suite (OMS).

With Microsoft's SaaS strategy for backup, Azure Backup is the core service. Existing System Center customers can continue to use DPM as a client to leverage the Azure Backup service, thus building on what they already have. To gain similar benefits, new customers can quickly start deploying hybrid cloud-first backup and start using ABS, which is available from the service directly from day one. Essentially, DPM and ABS provide the same offering, but ABS is particularly exciting because of its cloud-first direction.

Azure Backup

With so many transformative business and IT abilities being delivered through the Microsoft Azure cloud platform, it is natural that many of Microsoft's newest data protection innovations would be grounded in the Azure manageability suite—in other words, in the Microsoft Operations Management Suite. This work contrasts that of some other vendors that were early entries into cloud-based data protection enablement:

- Data protection solutions from some other vendors just "check the box" on cloud-based data protection by simply adding cloud-based storage to the on-premises solution.
- Organizations that are already running infrastructure-as-a-service (IaaS) may find their approach requires running another vendor's virtualized data protection solution as "just another VM or server" within that IaaS framework.

The Microsoft Azure approach is different. The Azure backup service runs as one of many services within the Azure SaaS and PaaS platform stack, with merely an agent being installed on either an on-premises server or an IaaS VM. In either case, the backup service provides a single lens whereby onsite and hybrid/IaaS servers are protected to the same platform.

On a relevant note, when ESG asked organizations how they use cloud-based services in their infrastructures, the top-cited use case scenario this year was improving backup and archive, and the second-most cited response was enhancing BC/DR preparedness.[7]

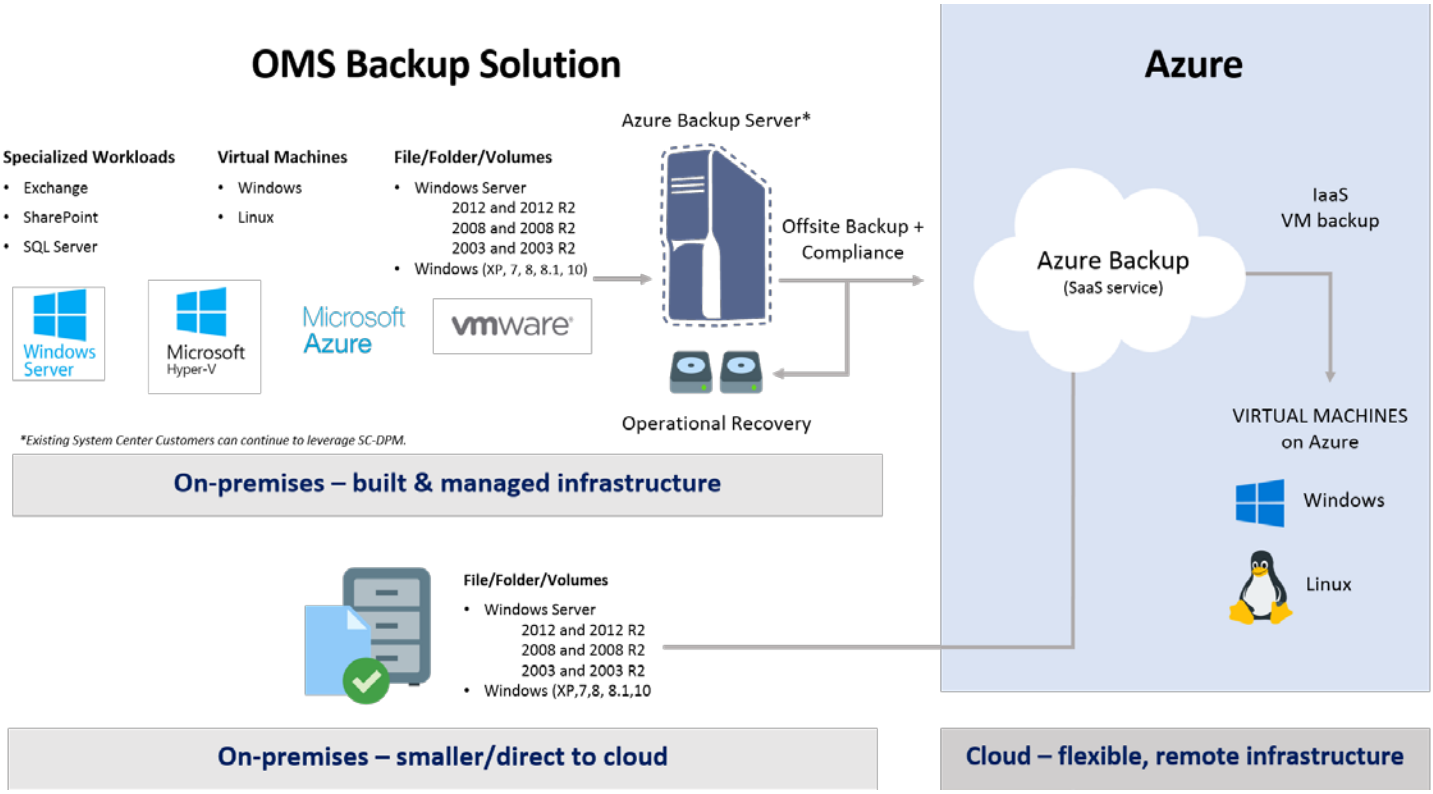
Azure Backup Server

Perhaps the most exciting (and most recent) addition to the Microsoft data protection portfolio is the Azure Backup Server. It should appeal to a very broad range of organizations that:

- Need to protect more than a few machines per location.
- Require the ability to recover data.
- Do not require the entire System Center portfolio across their environment.

It cannot be overstated how vitally important the OMS manageability framework is in delivering Microsoft's cloud-first yet heterogeneously supported data protection family, whereby its *backup agent* and *service* as well as its *backup server* provide comprehensive protection (see Figure 4).

Figure 4. Azure Backup Server and Azure Backup Service Solution Diagram



Source: Enterprise Strategy Group, 2016

[7] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.

Microsoft System Center Data Protection Manager (DPM)

While most organizations will look at the OMS offerings for data protection, no "Microsoft" data protection discussion would be complete without mentioning the enterprise-grade data protection module of the comprehensive onsite management framework, Microsoft System Center—System Center Data Protection Manager. It is interesting to observe that because Microsoft views data protection as an intrinsic part of a broader management strategy, the various components of System Center are not individually monetized or licensed, and it is logical to see the Azure Backup Service within the broader OMS offering.

Other Microsoft Data Protection and Availability Technologies

As stated earlier, System Center DPM, Azure Backup Server, and the Backup Service within Azure provide a variety of options for backup and recovery that are all cloud managed—as well as, in many cases, cloud powered—while providing customers with flexibility between on-premises, hybrid, and pure-cloud configurations (respectively). That being said, Microsoft's approach to data protection is pervasive across many other facets of its offerings as well. For example:

- For over a decade, Microsoft has been enabling robust data protection through its Volume Shadow Copy Services (VSS) that are built in to the Windows OS (client and server), thereby ensuring that Microsoft partners can develop and deliver reliable backup and recovery of applications and data sets in a Windows ecosystem.
- Built-in Windows recovery tools leverage various snapshot and/or previous versions' technologies to rapidly revert single machines or file systems to a known good state.

In addition to "backup," Microsoft ensures "recoverability" and "durability" of IT in other ways:

- Also available as part of OMS, Azure Site Recovery within the Azure platform helps enable business continuity and disaster recovery (BC/DR) preparedness through failover technology to a cloud-based service, often referred to as disaster recovery-as-a-service (DRaaS).
- In addition, the SaaS offerings from Microsoft (e.g., Office 365, SharePoint.com, and various Azure services) are replicated across geographies with transparent reconnection to mitigate node-centric or regional outages.

The Bigger Truth

With organizations of all sizes being so dependent on their data, but with production platforms evolving and data growth exploding, it is no surprise that IT groups continue to struggle with transforming their data protection.

What might be a surprise is that, for many organizations, the most appropriate answer may not be which data protection products should be "added into" the infrastructure, but rather which Microsoft foundational data protection technologies could be leveraged or enabled instead.