Solution Showcase

Office 365 Users Should Check Out HubStor

Because Data-management Mandates Apply to Data on Servers AND Services

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

Abstract: Just because you may choose to utilize cloud *services* instead of (or along with) onsite *servers*, you are not absolved from performing the data protection/data management tasks that all responsible data custodians must complete. One company that could help with these efforts, particularly in relation to protecting and managing content within Microsoft Office 365, is HubStor.

Introduction

At this point, mission-critical IT platforms such as email and collaboration are moving inexorably to a SaaS-based delivery model. A huge number of organizations are getting on board with the approach. When it comes to organizations migrating to Office 365 in particular, the trend is incontestable. Microsoft's own growth rates confirm it. In its most recent quarterly earnings statement,[1] Microsoft reported that revenue generated from its Office 365 cloud productivity suite rose 42% from the same period a year earlier.

Everyone Needs Data Management

Regardless of whether an organization chooses *servers* or *services* as the delivery mechanism for its productivity platforms, IT's role as data custodian, including handling data backup and data archiving, remains. Organizations protect their data for two main reasons:

- They need a way to recover and resume operations after something bad happens.
- They need to maintain previous versions of data for all sorts of other reasons. Sometimes, they need to keep those old versions for long periods.

SaaS-based delivery satisfies the first need (resiliency) elegantly. If one cloud site or connection goes down, a different site elsewhere takes over immediately and invisibly. SaaS platforms are inherently durable this way. They don't require their subscribers' IT department staffs to "failover" or otherwise expend energy recovering from outages.

But when it comes to the second requirement—keeping previous versions of data generated by the Office 365 productivity suite—Microsoft itself does not fully address those needs. That is not a disparagement; it is simply a recognition that Microsoft's strategy has always been and continues to be the enablement of a partner ecosystem to fill those scenario gaps. One gap is backup and long-term retention capabilities. Microsoft (like most other prominent SaaS vendors) explicitly

[1] Source: *Microsoft Earnings Release, FY18 Q1*, October 26, 2017.

states in its terms of service that data protection is the responsibility of the subscriber. The presumption is that the subscriber would utilize a third-party solution, but in the case of cloud archiving, there aren't many options yet.

As a whole, however, in-house IT organizations should strive to apply the same set of data protection actions to service-based data as they do to server-based data. Those actions center on:

- Backup for previous versions—Among organizations surveyed by ESG that allow their business units to select and use cloud-based applications autonomously, nearly three-quarters (72%) reported that their IT group has data protection and recovery responsibilities for those applications and associated data (31% have complete responsibility; 41% have partial responsibility).[2]
- Archiving for storage-cost management—Long-term retention and data deletion are actions that apply equally to service- and server-based data.
- Regulatory compliance and eDiscovery preparedness—These initiatives touch both server-based and service-based data, and protection actions should include at a minimum:
    - Immutable retention to ensure data authenticity.
    - Audit logging to monitor activity and behavior.
    - Email journaling to capture message records.

A big chunk of an organization's data management function consists of *data protection* (backup/replication) and *data preservation* (retention/deletion) underpinned by an archival strategy—not just a backup strategy. To succeed in short-term operational recovery and long-term retention, one must think holistically. Secondary storage repositories should address a set of needs broader than just "backup."

Everyone Should Archive, and not Just to Achieve Compliance

Archiving isn't synonymous with compliance. Yes, archiving is a foundational part of many regulations, and archiving reduces production storage costs because primary storage is an expensive place to keep inactive data. But it delivers a great deal more value to organizations than a checked box during an audit or savings in terms of space:

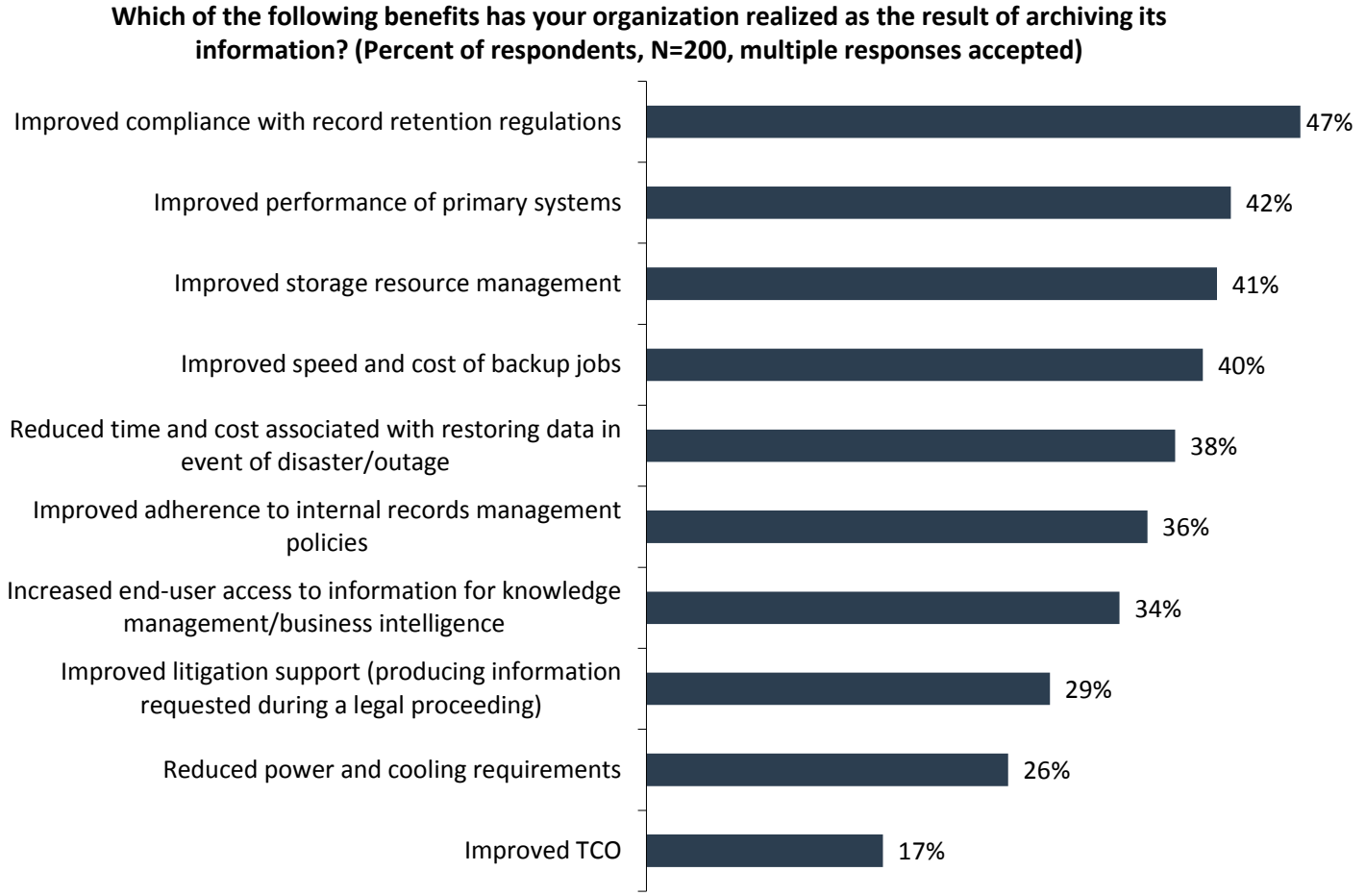
- Regulatory compliance—Organizations trying to adhere to data retention/deletion mandates often need to follow sometimes-contradictory regulations issued by a variety of governments, industry bodies, and business units. Deletion can be as important as retention, and automation can be the key to success.
- Operational recovery—Organizations using archival software to remove stagnant data from production platforms enjoy a couple of nice benefits. Specifically, they:
    - Have less data to back up, resulting in faster backups, less protection storage consumed, and more savings.
    - Have less data to restore, enabling the IT group to meet tighter SLAs during recoveries. During a BC/DR crisis, having less data to recover means that the business might resume operating faster.
- User enablement—Many organizations have amassed an assortment of production platforms so large and diverse that it becomes hard for end-users to find data. Rather than making workers comb through various production platforms'

[2] Source: ESG Research Report, *Data Protection Cloud Strategies*, December 2016.

data stores, those organizations could consider implementing an archiving product designed to locate data quickly. Such software typically has built-in data indexing, a rich catalog, and self-service portals to make searching efficient.

But wait … there are still more reasons to archive, including the ones identified in Figure 1.[3]

Figure 1. The Benefits of Archiving Data

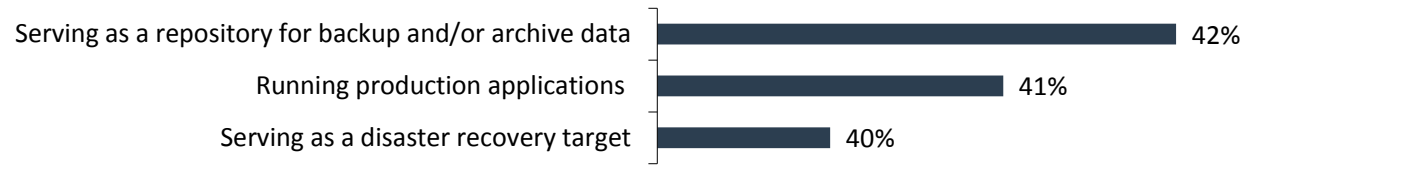


Source: Enterprise Strategy Group

The Cloud Should Be Part of Your Strategy

For the past several years, a frequently cited use case for cloud-based infrastructure among ESG survey respondents has been as a repository for backup and archival storage (see Figure 2).[4]

Figure 2. Top Three Use Cases for Cloud Infrastructure in 2017



Source: Enterprise Strategy Group

[3] Source: ESG Brief, *Long-term Data Retention Drivers and Trends*, April 2017.
[4] Source: ESG Research Report, *2017 IT Spending Intentions Survey*, March 2017.

A lot of those organizations are using cloud infrastructures to reduce their onsite capital expenditures. But the real power of cloud protection is not always grounded in *economics*; it is truly more grounded in *agility*.

Just ask yourself: "*What could I do with a warm, usable, accessible copy of data in a cloud that I can't do with a cold, dormant, inaccessible copy on a tape cartridge?*"

Aren't These Capabilities Built in by Microsoft?

The capabilities discussed thus far are *not* provided within Microsoft Office 365. Similar to Microsoft's strategy with its earlier platforms such as Windows and Windows Server, it has equipped Office 365 with only rudimentary data protection and data management capabilities (e.g., Windows Backup Utility, or the File Classification Infrastructure within Windows Server) to meet basic needs. Microsoft deliberately refrains from competing with its partner ecosystem. It relies on those software-innovation partners to supply the requisite enterprise-class capabilities.

In this case, Microsoft:

- Did not build backup into Office 365.
- Makes archiving with capabilities for legal hold available only in the most expensive Office 365 licensing tier.
- Holds audit logs for only a few months—sufficient for change-control management perhaps, but not for litigation, data security, or HR scenarios.
- Sets storage limits in SharePoint Online which, when they are exceeded, result in an added premium storage cost for long-term retention.

That's the "bad" news. Here is some good news.

The HubStor Solution for Office 365 Using Microsoft Azure

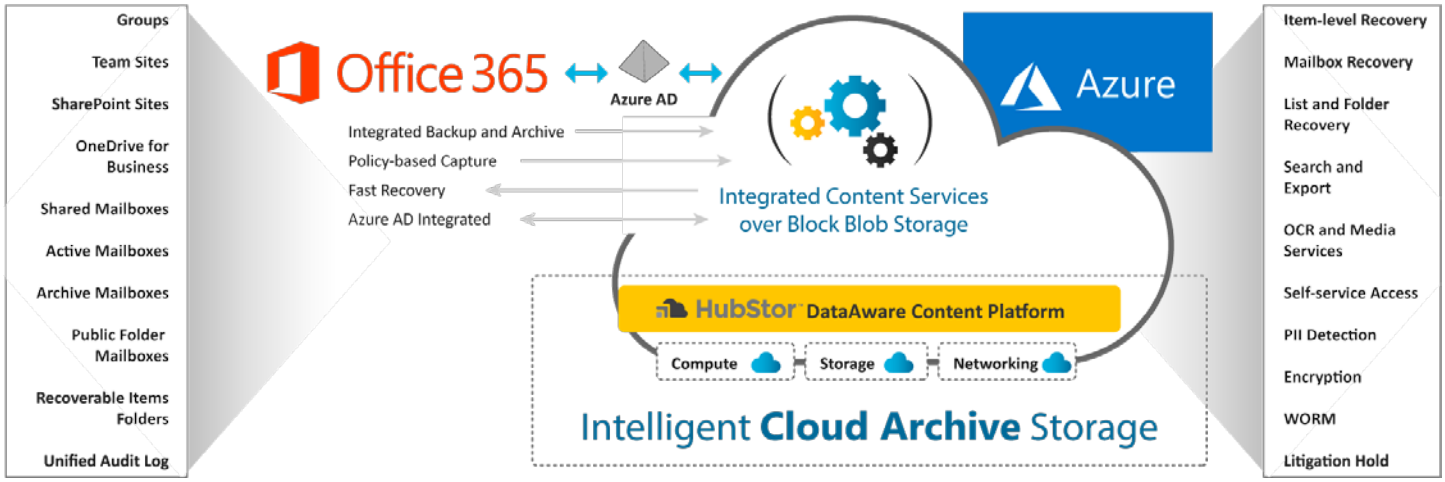
HubStor software is designed to be used with Office 365 and Microsoft's comprehensive set of cloud services known as Azure. It helps organizations take better advantage of public cloud storage to streamline and generally improve archiving efforts. Specifically, an IT team can use HubStor software to customize policies for offloading primary storage to the secured Microsoft Azure cloud—e.g., tagging data as "private," "auditable," "partner-sharable," and so on.

ESG Lab recently assessed HubStor's data-aware cloud archiving solution and found that it practically eliminates archiving complexity. Data managed via HubStor is searchable at scale, meaning an organization can respond faster to audits, legal claims, and external requests for data sharing. HubStor sells its solution under a "pay-as-you-grow" structure based on capacity consumed.

For many Office 365 users, the HubStor solution appears to be an ideal "onramp" for consuming cloud storage the way cloud storage is *supposed* to be consumed—conveniently, securely, and cost effectively.

Figure 3 depicts HubStor Intelligent Cloud Archive Storage for Azure.

Figure 3. HubStor Intelligent Cloud Archive Storage



Source: HubStor

Organizations' Intended Repositories for Office 365 Data—How HubStor Software Fits In

ESG research into organizations' intended repositories for cloud-based production data shows that most organizations surveyed prefer to have their secondary/protection storage reside physically apart from their primary/production environment.[5] Most respondents want their data in a cloud. But that preference varies between the original environment (presumably to facilitate fast restores) and an alternative cloud (presumably to ensure access across a variety of distributed crises). What makes the HubStor architecture so interesting is that HubStor software makes both the above repository options achievable when it comes to Office 365. Archival data can live in the same IT environment as the Office 365 data's primary location, or it can reside in a different geography (Azure region).

To put it another way, Microsoft Azure, Microsoft Office 365, and HubStor used together can enable an organization to achieve what a majority of organizations are seeking: to protect their data outside of the purview of the original servers or services in some fashion. HubStor's loosely coupled architecture with Azure storage addresses the long-term desire of the 44% of ESG survey respondents who said they want their data in another cloud environment or region, as well as the 24% who want to protect it within the same hosted infrastructure[6] (accommodated by Azure's intra-datacenter connections).

HubStor Fills the Gap

Here are the most common ways organizations are using HubStor along with their Microsoft Office 365 subscriptions:

- SaaS backup—To protect against malicious or accidental deletions—especially true for organizations that believe the built-in 14-day deleted-item retention span is not sufficient and do not want to place all their content on litigation hold forever as a workaround.
- Write once, read many (WORM) storage—If they have to adhere to strict regulatory compliance requirements for tamper-proof storage, and their content needs this level of record keeping.
- Archiving for optimal storage cost—Organizations quickly encounter size limits in SharePoint and OneDrive for Business. Sometimes, it happens immediately when migrating home directories and departmental file shares as part of a datacenter-scale shift to Office 365. Microsoft charges a premium monthly fee for expansion storage capacity.

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

According to HubStor, its users are saving on storage costs by moving older data from SharePoint Online and OneDrive for Business over to Azure's Cool and Archive Blob Storage using HubStor.

- Unified audit log preservation—Ninety days is the maximum retention time for the Office 365 unified audit log. But some organizations must retain that log data far longer for compliance reasons. Others want to preserve it for security purposes, HR purposes, and perhaps even eDiscovery early-data assessments.

- Email journaling – While some (albeit few) organizations are willing to use an "on litigation hold always" approach to replace journaling, others only need to journal internal or external communications. Or, they simply don't want to spend the extra money to upgrade to the Office 365 plan that includes litigation hold. HubStor addresses their needs.

The Bigger Truth

An organization's choice of IT platforms, be it "servers" or "services," does not relieve that organization's IT administrators of their data-custodian responsibilities. They still need to protect and preserve data.

With so many organizations adopting Microsoft Office 365 as part of their broader digital transformation strategy, it is imperative for them to apply the same zeal to their data protection and preservation policies for this platform.

Most SaaS offerings, including Office 365, do not provide built-in data protection or preservation mechanisms that meet any true level of operational recovery or regulatory compliance. It is a situation that requires responsible organizations to seek out solutions, such as HubStor, that can accomplish those feats instead.