Enterprise Strategy Group | **Getting to the bigger truth.™**

Solution Showcase

# Data Protection for Modern Workloads: Protecting Office 365 with Cohesity

**Date:** June 2019 **Author:** Christophe Bertrand, Senior Analyst

**Abstract:** In a context of mass data fragmentation on-premises and in the cloud, organizations now struggle with the compounded complexities brought about by modern workloads such as containers, NoSQL/NewSQL databases, and SaaS applications. These new workloads are turning traditional backup and recovery approaches on their head—in particular, in Microsoft Office 365 deployments for which new backup, recovery, and data management schemas must be deployed.

## Market Landscape

### The Roots and Consequences of Massive Data Fragmentation

There's just too much data! It's everywhere in the IT infrastructure, and it keeps on growing with little control and no end in sight. Worse: Copies of data are also generated for recovery or other business purposes, creating additional layers of complexity. At the heart of the issue is not just the volume of data and data copies, but its management. Copies are spread across the whole infrastructure, on-premises and in the cloud, generating cost and complexity as all of this data is challenging to track, manage, and optimize. Data is *massively fragmented*.

A recent study conducted by ESG reveals that on average data is copied and stored six times, and that managing this fragmented data makes up 42% of a typical administrator's job.[1] With data spread across storage on-premises and in the cloud, 82% of surveyed organizations believe that mass data fragmentation has created a visibility challenge. Today, it takes on average five separate vendors to provide data management[2] across on-premises and multiple cloud environments. Over 73% of organizations are leveraging multi-cloud topologies. It should come as no surprise that 57% of respondents are not very confident in their ability to recover from a major data loss event.[3]

### Emerging Workloads Compound the Issue

Many traditional workloads have contributed to the issues of data growth and fragmentation for many years. As technology evolves, new types of solutions get adopted in production environments on-premises and in the cloud. These "modern" workloads such as NoSQL/NewSQL databases, distributed frameworks such as Hadoop, and containerized and

[1] Source: ESG Custom Research, *Mass Data Fragmentation Validation and Branding Survey*, , April 2019.

[2] Data operations related to backup, archive, test/dev, analytics, etc.

[3] Source: ESG Custom Research, *Mass Data Fragmentation Validation and Branding Survey*, , April 2019.

SaaS-based applications are all creating a double challenge: More data *and* the need for new management and protection schemas. Workload modernization triggers data management and data protection modernization as a domino effect.

The proliferation of Hadoop and NoSQL in what can be petabyte-scale clusters creates business and IT imperatives of stringent data protection SLAs. ESG research showed that 96% of organizations were already using NoSQL in 2017 or planned to within the following year, and 50% of organizations were using Hadoop.[4] Hadoop and NoSQL backups using traditional backup, recovery, and data management methods are no longer enough.

Protection of VMs and containers is the second most often cited primary challenge with current backup and recovery processes and technologies.[5] ESG also identified that 31% of respondents see protecting containerized workloads as equally important as protecting virtual machines within the next 12 months.[6]

Software-as-a-service (SaaS) data is on the rise. Email and collaboration are essential to business. Not surprisingly, these applications have migrated from their traditional on-premises deployments to the cloud SaaS consumption model.

## The Big Disconnect with Office 365 Backup, Recovery, and Data Management

Zooming in on Office 365 environments, disconnects for IT professionals have emerged in our research. Leveraging a SaaS workload does not absolve IT from its traditional backup and recovery stewardship.

### It's Always Your Data!

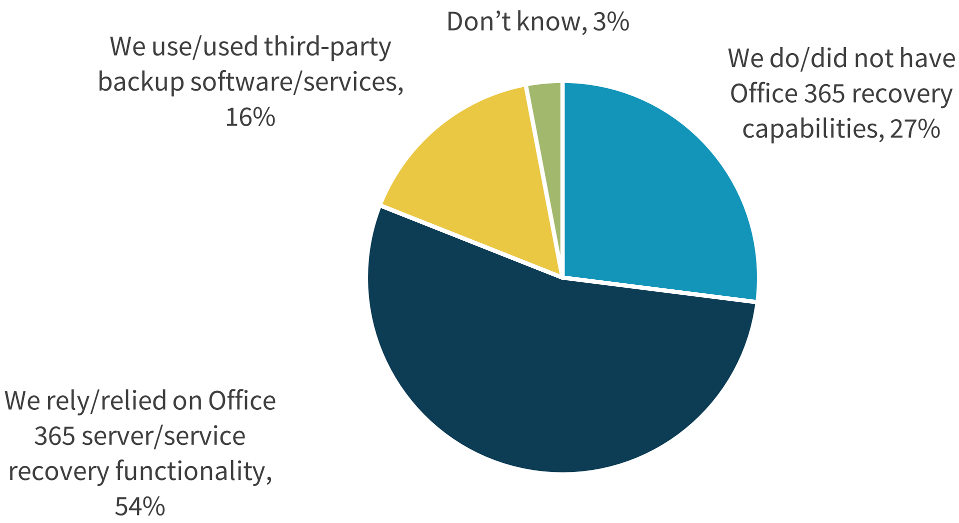
Put simply, organizations are always "responsible" for their data—from creation, through destruction for compliance purposes, to recovery should the data become unavailable, deleted, etc. For these and many other business reasons, data must be retrievable under the control of its owner or on its behalf. Backup/recovery and archiving cannot be afterthoughts, nor should there be any assumption that someone else will miraculously take on this responsibility on behalf of the organization. That's where a disconnect exists in the market when it comes to SaaS, based on ESG's research. As a matter of fact, **33% of respondents believe that there is no need to back up SaaS applications!** Further, 37% confirmed that they solely rely on the SaaS vendor because they believe the vendors are responsible for protecting their organization's SaaS-resident application data, which is simply not true.[7] This may be due to confusion about rights and responsibilities, or a misunderstanding of what is included in service availability versus backup. This misconception is a recipe for bad surprises.

### Recoverability of Office 365

ESG research shows that 71% of organizations leverage Microsoft Office 365 solutions. Inarguably, this suite of SaaS applications is critical to keep any organization up and running, yet the lack of protection of its data is pervasive: One in four (27%) organizations do not have Office 365 recovery capabilities (see Figure 1).[8]

[4] Source: ESG Brief, *Market Disruption: Next-generation Databases*, April 2017.
[5] Source: ESG Master Survey Results, *2018 Data Protection Landscape Survey,* November 2018.
[6] Source: ESG Master Survey Results, *2019 Cloud Data Protection Strategies*, June 2019.
[7] Ibid
[8] Ibid

**Figure 1. One in Four Do Not Protect Office 365 Data**



*Source: Enterprise Strategy Group*

Compounding the issue, recoverability of Office 365 is far from a sure thing when using a recovery service or capability. Higher success rates are possible using a third-party backup solution. When looking at users who report a data recovery rate of more than 75%, three out of four are using a third-party solution versus the built-in services or no capabilities.[9]

With these facts in mind, IT leaders need to take a close look at their SaaS data protection/recovery capabilities and consider engaging the support of trusted third-party solutions to get the job done.

## Cohesity's Solution for Office 365

This is an area in which Cohesity can help with a solution designed for protecting and managing traditional and modern workloads, including Microsoft Office 365. The offering provides backup and recovery for Exchange Online and OneDrive, on-premises or in Microsoft Azure, and provides capabilities such as fast backup ingest by streaming backups with Cohesity's unique parallel data ingest technology. Backup policies are easy to deploy to deliver automated protection for any new mailbox or file added to an Office 365 account. The solution also uses incremental forever backup technology, which results in faster and more efficient backups. Recoveries are granular, and the solution delivers both powerful metadata indexing as well as in-place analytics to search for individual emails and files. Users also have the flexibility of recovering to the original or an alternate location from any point-in-time copy.

## The Bigger Truth

Data is all over the place and it keeps on growing. The price tag is rising as more data in more "silos" generates operational inefficiencies and heightens business risk. It has become imperative to reduce data fragmentation across the hybrid IT infrastructure, on-premises or in the cloud, in order to unlock its value.

At the same time, IT professionals cannot ignore new workloads, which add further complexity from a backup, recovery, and data management perspective if left separated. SaaS data and applications have exposed a new battlefront for IT. Protecting SaaS data is still an afterthought for many organizations, but great recoverability results can be obtained by leveraging third-party solutions, in particular for Office 365 environments.

[9] Source: ESG Master Survey Results, *2019 Cloud Data Protection Strategies*, June 2019.

The next battleground for IT is the intelligent management of all this data on a massive enterprise-level scale so that true business value can be derived from alternate uses (beyond production) of the data assets organizations produce on a daily basis. That's where IT professionals should take a look at Cohesity's platform and solutions for both traditional and modern workloads. Cohesity's approach is focused on addressing the fundamental issue of mass data fragmentation, while adding a broad spectrum of platform coverage *and* unlocking value through services directly on the platform. Its recent addition of solutions in the space of NoSQL/NewSQL and Office 365 only expands the perimeter it can help unify.

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.

**Enterprise Strategy Group** is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.