COHESITY

Beyond Backup

A guide to getting more out of your data on the cloud

aws

The data age

We are in the age of data. There is so much of it, stored in disparate sources, and stored in myriad ways (on-premises, on the cloud, or a mix).

There is also deep awareness and sensitivity about that data, as consumers and companies alike have shrewd attention to data privacy and protection practices.

Companies know they must retain data in archives, but many let that data sit idle. Yet savvy companies know that they can do so much with that data—test, develop, and innovate—if they can access it.

In this eBook, we'll examine considerations for backing up your data, show you how you can take steps to ensure it is protected and restorable, and explore how you can even move into new territory, like testing and developing, using your data. Finally, we'll share how Cohesity and Amazon Web Services (AWS) can help you manage and protect your data.

The trouble with data

It is estimated that 2.5 quintillion bytes of data are created every day.[1] That data—of different types—is often stored in myriad places around an organization. The vast majority of enterprise data—including backups, archives, file shares, object stores, and data used for test/dev and analytics—sits in fragmented infrastructure silos that makes it hard to protect, expensive to manage, and difficult to analyze.

Cohesity found that more than 80 percent of enterprise data is scattered across different locations, trapped in infrastructure silos, and buried unseen in long forgotten storage systems. Results from a recent Cohesity study indicate data is often stored in triplicate.

This concept, called "data fragmentation," is a serious problem. Data fragmentation is cited as the root cause of data difficulties, according to a recent Cohesity survey. In that same study, Cohesity found that IT teams predict it will take up to half their working year by 2020—time that detracts from more valuable projects that could help drive the business forward.

1. *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, Forbes, May 2018

It is common practice to make and store more copies of the same data in cloud environments—on average three copies of the same data according to our respondents.

Source: *Mass Data Fragmentation in the Cloud, A Global Market Study*, Cohesity, 2019

Backup and data management, front and center

Data must be protected, and urgency has only increased on this front. Consumers and companies alike are aware of high profile breaches and skittish about data privacy. As well, regulations, such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), are keeping the topic in the news.

Before we step into the tactics of how to protect your data, here are a few key considerations for data protection:

- **Consider types of data:** What kind of data do you have? Examples include structured, unstructured; in-house, third-party, or social data.
- **Consider compliance:** Are there any industry-specific or regional regulations to which you must adhere? Consider GDPR, HIPAA, and the like.
- **Consider privacy:** This can include consumer and company data privacy.

Next, let's get tactical about data storage. There are a few additional questions to investigate:

- **Where is your data currently stored?** You may keep data on-premises in physical tapes and vaults; maybe you store your data on the cloud; maybe, it is a combination of the two.
- **How long do you need to store your data?** There are really two options: short-term or long-term. Long-term storage is often a pain point; you know you might need that data, it's just not something you need all the time.
- **How often do you need to access your data?** Consider whether you need frequent or intermittent access; if the latter, you can consider "cold" storage for your archives.

Data decision:

When you need to access your data…

With all of this in mind, now it's time to make some decisions about backing up and storing your data.

Traditional backup and restore solutions cost more, both in terms of personnel time and licensing. There are inherent risks to physical storage solutions. Tapes may breakdown, be stolen, or lost. Physical storage requires physical space, too—which adds up in terms of real estate and management costs. In the event of necessary data restores from physical media, this may involve unpredictable elements such as delivery equipment malfunction and user-error. Any of these issues can create obstacles to recovery time objective (RTO) attainment, can reduce business performance and agility, and can leave your organization at risk of non-compliance.

Instead, the cloud offers a scalable, cost effective, and resilient way to store and manage your data.

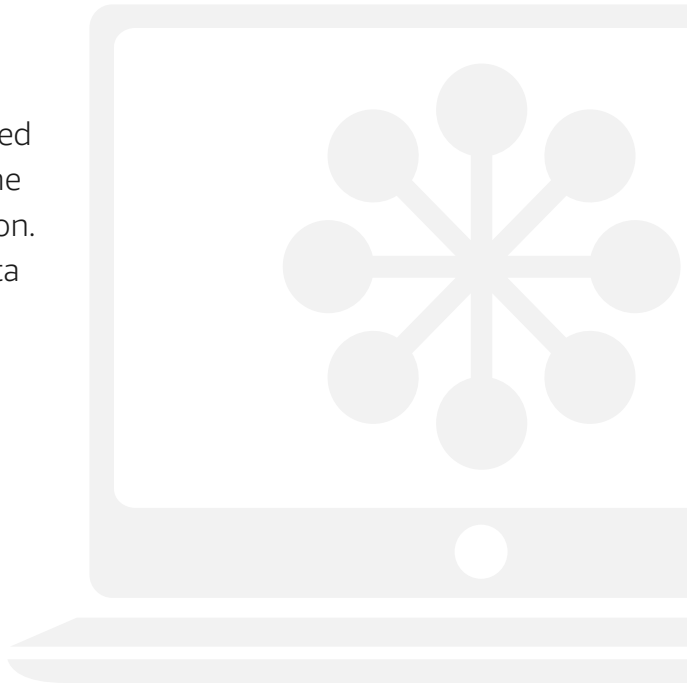
Look beyond your immediate needs:

Keep an eye toward innovation

Let's pause for a final moment and dream:

If you weren't focused on data management and storage, what would you be doing? What do you and your company really want to focus on? In other words, what would you rather be doing instead of managing storage and backups? The answer is probably a lot.

Managing physical data storage infrastructure and ensuring that data is secure and protected takes a lot of time and resources away from the things your business is really about. Imagine if you did not need to spend time, effort, and resources on data management and protection. What if it worked seamlessly in the background? In that scenario, you could access your data and use it for advancing your business—such as to test, develop, and innovate.



Securely backup and manage data in one place—and gain time for innovation—using Cohesity and AWS Cloud

Using Cohesity and AWS, you can:

Store and access your data

Archive backup data to AWS storage services for long-term retention. Utilize policy-based thresholds to move cold data to AWS using Amazon Glacier, designed for long term storage. Reformat your data and store it on the cloud where it can be accessed quickly and at any time.

Protect your data

Protect AWS applications with cloud-native backup. With Cohesity, data is backed up to Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Elastic Block Store (Amazon EBS) snapshot management. You can also replicate data from an on-premises Cohesity cluster to AWS, and leverage failover and failback capabilities to enable disaster recovery on AWS.

Innovate with your data

It is possible to forget about data storage, get time back, and focus on what's next for your business. Leverage automation, an intuitive and simple UI, and a single pane of glass for data management—all of which help you save time that you can instead use to move beyond data management and actually use your data for innovation.

Cohesity consolidates silos onto one web-scale platform, spanning on-premises, cloud, and the edge, and uniquely empowers organizations to run apps on that platform—making it easy to back up and extract insights from data.

Cohesity addresses and reduces the problem of mass data fragmentation problem with a web-scale, software-defined platform designed to manage all secondary workloads such as backups and archiving, file and object storage, test/dev, and analytics.

There is a way out of the dilemma: a more modern data management solution that consolidates inefficient silos, minimizes copies, and reduces compliance risk by providing visibility into the data. Almost nine in ten respondents were optimistic that the promise of the public cloud could be realized with a solution that could solve their mass data fragmentation issues.

Source: *Mass Data Fragmentation in the Cloud, A Global Market Study*, Cohesity, 2019

LEARN MORE ABOUT COHESITY WITH AWS