COHESITY

TIPSHEET

Top 3 Myths about Backing Up Cloud-Native and SaaS Data

Overview

Organizations worldwide are making the move to the cloud, and that means more of their data lives there than ever before. Yet, many of these businesses pursue the cloud with misconceptions around their data protection needs. Let's look at some of those myths:

1. You don't need to back up cloud data and workloads

Many organizations believe that the cloud is inherently safe and as a result there is no need to implement effective data backup and recovery. But, cloud data security is a shared responsibility between the cloud provider and the customer. The responsibility of the cloud provider is to safeguard the infrastructure, ensure access, and configure physical hosts, storage and other resources. In short: to ensure the underlying infrastructure is available.

The responsibilities of the customer are to manage users and their access privileges, safeguard cloud accounts from unauthorized access, encryption and **protection of cloud-based data assets**, and managing compliance[1].

As a result, it is up to the customer to ensure an effective backup and recovery solution is in place to ensure the data itself is available. Otherwise, cloud data can be subject to malicious threats as well as unintentional deletions, impacting key workloads across the IT environment.

2. Cloud-native tools are sufficient to protect my data

Cloud providers have developed native tools for basic retention or backup functions. However, adoption of and reliance upon these solutions can create several challenges. First of all, these often have default retention periods (e.g. 30 days for M365) that fall far short of enterprise requirements. They also can be complex to use when modifying defaults—and typical recovery times may fall short of SLA requirements, particularly at scale. These native services are also siloed—in the sense that they are not designed to also protect data sources beyond those they host, i.e. those running on-premises or in other clouds. As a result, organizations often end up with multiple systems to manage when using such tools, which drives up complexity and costs, creates a broader attack surface for security risks and breaches and poses challenges in meeting business SLAs and compliance requirements.

[1] "Shared Responsibility Model Explained." *Cloud Security Alliance*, 26 Aug. 2020, https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained.

3. Recovering cloud workloads is fast and easy

Many believe that recovery of cloud data is quick and seamless. Yet, what many have come to realize is that both backup and recovery speed in the cloud is highly network dependent. As a result, there is no guarantee that there won't be any lags or latency in data recovery, which can have a significant impact for businesses with tight Recovery Time Objectives (RTOs). This is why a hybrid solution that can be managed from one place and that provides both self-managed and SaaS options is paramount. This way, you can choose where cloud backup data resides in order to meet SLA expectations properly when it comes to restores. Having that solution also be optimized for network performance, transmitting only delta change blocks across the WAN is also important.

Backup remains critical to business operations, and organizations need to be aware of their responsibilities when storing data in the cloud.

To solve for many of these challenges, Cohesity offers a choice of consumption models for data backup and recovery. With Cohesity DataProtect organizations can take advantage of an on-premises backup solution which is self-managed and as Backup as a Service (BaaS) which can extend to cloud-native and SaaS workloads. With Cohesity DataProtect delivered as a service, organizations can simplify backup with a service that's optimized for a true hybrid experience from datacenter to cloud to edge environments, all while using a simple, unified UI and capacity-based pricing. As you can see, we've got you covered when it comes to protecting your cloud data sources.

Register today for a free trial of Cohesity DataProtect delivered as a Service.

COHESITY