COHESITY | aws



Safeguard Your Cloud Data with the Right Data Backup Solution

The top 3 misconceptions about backing up cloud data

Organizations worldwide are relying more on cloud-based data and workloads than ever before. While the public cloud delivers significant benefits, there are several misconceptions about what is needed to ensure this data remains as secure and protected as possible.

Let's look at some of those myths:

1

Myth: I don't need to implement additional backup and recovery solutions when my data is in the cloud.

Truth: Cloud data security is a shared responsibility between the cloud provider and the customer.

Cloud data security and compliance is a shared responsibility between the cloud provider and the customer. The responsibilities of the cloud provider are to safeguard the infrastructure, ensure access, and configure physical hosts, storage, and other resources.

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

As a result, it is up to the customer to ensure an effective backup and recovery solution is in place to safeguard cloud data.

Customer Responsibility for Security 'in' the cloud	Customer Data		
	Platform, Applications, Identity & Access Management		
	Operating System, Network & Firewall Configuration		
	Client-Side Data Encryption & Data Integrity Authentication	Server-Side Encryption (File System &/or Data)	Network Traffic Protection (Encryption, Integrity, Identity)

AWS Responsibility for Security 'of' the cloud	Software			
	Compute	Storage	Database	Networking
	Hardware/AWS Global Infrastructure			
	Regions	Availability Zones	Edge Location	

"Security and compliance is a shared responsibility between AWS and the customer. Highly successful security organizations are proactive about gaining clarity on what they must take on themselves, what AWS can do for them, and what we both work on together."
-Stephen Schmidt, AWS CISO

2

Myth: Cloud-native tools are always sufficient to keep my data fully compliant.

Truth: Cloud-native tools may not meet all your enterprise requirements, especially when protecting both cloud and on-premises workloads.

Organizations implement multiple tools to successfully manage all workloads, especially when running cloud-native and on-premises. However, this can drive up complexity and costs, create a broader attack surface for security risks and breaches, and pose challenges in meeting business SLAs and compliance requirements.

- Native tools have default retention periods that may not always meet enterprise requirements. (e.g., 30 days for M365.)
- Native tools may have intricate processes for modifying default settings. (e.g., Typical recovery times may fall short of SLA requirements.)
- Native services are not designed to fully protect data sources beyond those they host. (i.e., Those running on-premises.)

82% of enterprises have a hybrid cloud strategy.

3

Myth: Recovering cloud workloads is fast and easy.

Truth: Data backup and recovery speed in the cloud is highly network dependent.

Because of this network dependency, there is no guarantee there won't be any lags or latency in data recovery. This can have a significant impact for businesses with tight Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), especially in the event of ransomware or a cyberattack. Often, ransomware variants target accessible, in-network data, so having a robust backup solution in place can go a long way in preventing damage caused by cyberattacks.

Cyberattacks will cause $10 trillion in damage by 2025.



Cohesity DataProtect delivered as a Service

Backup as a Service (BaaS) provides a more predictable cost model while delivering unified backup for all types of workloads through a single UI. More and more organizations are leaning towards this type of solution to free up IT resources and improve productivity. With Cohesity DataProtect delivered as a Service, organizations can take advantage of the flexibility and deployment of a robust backup and recovery solution, available as self-managed software or BaaS, which can extend to cloud-native and SaaS workloads. Now 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 upfront capacity-based pricing.

Learn more about data protection strategies in the cloud.

Get the Ultimate Reference Guide

COHESITY aws

[1] https://d1.awsstatic.com/executive-insights/en_US/ebook-traits-of-highly-successful-security-organizations.pdf
[2] www.flexera.com/blog/cloud/cloud-computing-trends-2021-state-of-the-cloud-report
[3] www.cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025

© 2022 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

620008-002-EN 1-2022