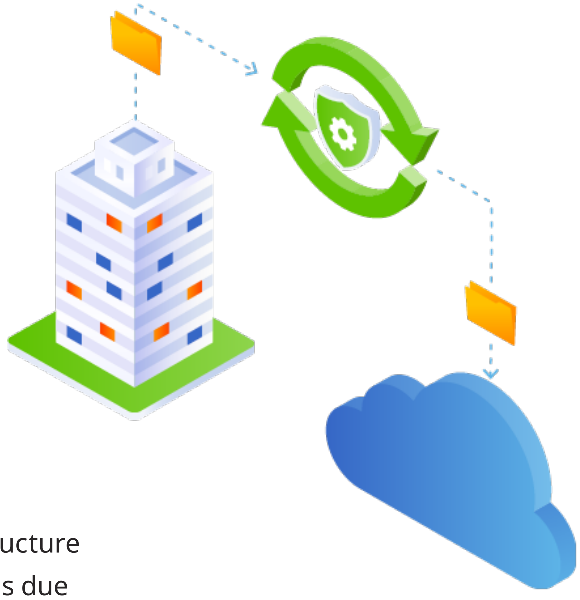
5 Hybrid Cloud Backup and Disaster Recovery Mistakes to Avoid



Overview

Every company expects to have some part of their applications or infrastructure in the cloud by 2021.[1] Yet most won't fully achieve the benefits cloud brings due to mass data fragmentation, challenging businesses to gain visibility into all their data across siloed environments. Legacy point products are ill-equipped to support modern data management strategies that include hybrid cloud, particularly hybrid cloud backup and disaster recovery. As a result, teams are trying to force-fit existing solutions and commonly make five big mistakes.

1. Assuming your cloud data is backed up

Cloud data security and compliance are a shared responsibility between the cloud provider and the customer. The cloud provider is responsible for high-availability of physical infrastructure (i.e., datacenter, servers, wiring, etc.) while businesses are responsible for access privileges, safeguarding cloud accounts from unauthorized access, encryption, protection of cloud-based data assets, and managing compliance. Organizations need a backup and recovery solution that works seamlessly across multiple environments—datacenter, cloud and edge. The goal is to simplify backup and recovery with a flexible solution that is available as self-managed software, or as backup as a service (BaaS) and should support a variety of data sources from on-premises to cloud-native and SaaS-based workloads.

2. Believing you can retrofit point solutions for cloud

Complexity doesn't have to be a by-product of introducing cloud into your IT vision. Yet that's exactly what happens when you rely on legacy and/or disconnected point products for your on-premises and cloud backup. Why? Because each additional tool adds complexity. A bolt-on cloud gateway alone adds a new hardware expense and management headache when protecting data in virtual machines (VMs), databases, containers, physical servers, and the cloud. Organizations need a modern data management solution that works seamlessly across on-premises and cloud environments. By consolidating management of all your data and apps in one place and utilizing global deduplication search to make things easy to find and restore, businesses can turn backup data into a competitive advantage by enabling it to be analyzed or used for dev/test.

Mass Data Fragmentation Impacts[2]

- **More time** – IT teams spend 19 weeks/year managing data and apps infrastructure across public cloud environments.
- **More staff** – IT teams would need to expand by over a third to glean maximum insights from all the data they store across public clouds.
- **More money** – IT budgets would need to increase by nearly half.

> "
>
> 69% of businesses use a hybrid cloud solution.[3]

[1] IDG. "2018 Cloud Computing Survey."

[2] Vanson Bourne. "Mass Data Fragmentation in the Cloud: Global Market Study," 2019.

[3] Right Scale. "2019 State of the Cloud Report."

3. Thinking snapshots are free

In an on-premises environment, snapshots—a quick copy of data—are commonly stored on the same hardware device or storage array. In cloud deployments, snapshots may be in different tiers, but always in the same region or datacenter. As your organization moves workloads to the cloud, managing snapshots across multiple cloud users, accounts, and providers is extremely challenging. So is protecting hundreds or thousands of VMs or storage volumes from growing silos. To combat these challenges, organizations need a solution with a unified policy-based data management and global search that lets you easily manage snapshots across multiple accounts, clouds, and environments and ensures backup copies can be moved and made safe from tampering in another location.

4. Focusing more on backup than recovery

Backup software is often considered an insurance policy. Everything is fine, until it isn't. And that's when recovery speed matters just as much as your backup solution features. Too many organizations focus on backup windows and dedupe ratios, neglecting to prioritize key recovery capabilities such as fast, error-free, granular, and cloud ready. Look for a modern data management solution that protects backup data with erasure coding and across multi-node clusters to help prevent failures. Select one that provides seamless failover of interdependent applications to the cloud of your choice. Make sure it can restore hundreds or thousands of VMs at once—possible only with a parallel file system that significantly improves speeds for large scale recoveries. The right data management solution ensures you and your team can search for the exact data you need, so you don't have to scramble to recover to any point in time.

5. Implement Disaster Recovery without Planning

5% of organizations worldwide still don't have a disaster recovery (DR) plan in place. Of those that do, 29% have never tested their plans, and 34% have experienced outages from improper failover to the cloud.[4] In order to avoid downtime and data loss, businesses need a modern data management solution that ensures data recovery preparedness for continuity of operations. With automated orchestrations for failover and failback, data can be rapidly retrieved and recovered if it's needed, no matter where it's stored. Furthermore, businesses can meet SLAs across application tiers with limitless scalability provided through a web-scaled architecture. The solution should provide ultimate choice of deployment model with self-managed DR between locations or cloud accounts to Disaster Recovery as a Service (DRaaS) on public and managed clouds.

Avoid These Common Mistakes with Modern Hybrid Cloud Backup and Recovery

The ideal solution to combat many of these challenges is a software-defined data management platform that spans a hybrid data estate across clouds and data centers. Now is the time to adopt a globally efficient platform that runs on any hardware or virtual cloud infrastructure and features seamless native cloud integration—Amazon Web Services, Microsoft Azure, Google Cloud Platform, and other service providers—without additional bolt-on cloud gateways. And don't forget the deployment choice is yours - whether it is self-managed on-premises, software as a service (SaaS), all managed through a unified, single UI.

[4] Spiceworks. "Disaster recovery survey." and Cohesity research.

Download this eBook to learn more about hybrid cloud backup and disaster recovery.

COHESITY