Compliance and the cloud

ONTAP 9

NetApp
February 24, 2022

Table of Contents

Compliance and the cloud

NetApp Cloud Data Sense

Each industry and each country has different compliance requirements. Whether you have an on-premises system or are working in the cloud, ONTAP helps you maintain compliance.

Powered by artificial intelligence, NetApp offers Cloud Data Sense (formerly Cloud Compliance service) to keep your cloud resources in compliance with many regulations. This always-on service is the best way to navigate complex compliance regulations.

Related information

NetApp Cloud Data Sense

Data sovereignty

Data sovereignty refers to national laws concerning the collection, storage, and transmission of data. The General Data Protection Regulation (GDPR) in Europe and the Health Insurance Portability and Accountability Act (HIPAA) in the US are examples of these laws. Data residency refers to where data is physically stored and is often specified by data sovereignty laws. Personal data about individuals is a primary target of regulations, but other data can be regulated too.

When you store data on premises in your own data center, you have complete control over how and where the data is stored. When you store data in the cloud, you are responsible for understanding how and where that data is physically stored, and you are responsible for ensuring you comply with applicable data sovereignty laws. For hybrid cloud configurations, you need to pay attention to where both the on-premises tiers and the cloud tiers are stored.

The good news is that all the major cloud providers are fully aware of the laws and have procedures and information to help you comply. But it's still important that you select the appropriate products and procedures for your specific needs.

In many cases, storing your data in the cloud makes it possible to keep data within the boundaries of a country where your company has no physical presence.

Here are some examples of the compliance information from NetApp and from cloud providers:

- Architecting GDPR- and HIPAA-Compliant Storage
- Questions on data residency and compliance in Microsoft Azure
- General Data Protection Regulation (GDPR) Center for Amazon Web Services
- Compliance resource center for Google Cloud
- Alibaba Cloud Security & Compliance Center

Cloud WORM storage

An important aspect of compliance is being able to guarantee that certain data is maintained unchanged for a required period of time. You can activate write once, read many (WORM) storage on a Cloud Volumes ONTAP system to retain files in unmodified form for a specified retention period. Cloud WORM storage is powered by SnapLock technology, which means WORM files are protected at the file level.

Once a file has been committed to WORM storage, it can't be modified, even after the retention period has expired. A tamper-proof clock determines when the retention period for a WORM file has elapsed.

You can activate WORM storage on a Cloud Volumes ONTAP system when you create a new working environment. This includes setting the default retention period for files. You can't activate WORM storage on individual volumes—WORM must be activated at the system level.

Related information

WORM storage

Archive and compliance using SnapLock technology

NetApp Cloud WORM: Enhancing Data Protection with Locking Features