



# **Compliance and the cloud**

## **ONTAP 9**

NetApp  
February 24, 2022

# Table of Contents

- Compliance and the cloud ..... 1
  - NetApp Cloud Data Sense ..... 1
  - Data sovereignty ..... 1
  - Cloud WORM storage ..... 2

# 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](#)

## Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system- without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.