Frequently asked questions about Cloud Compliance

Cloud Manager

Tom Onacki, Ben Cammett
February 08, 2021

Table of Contents

Frequently asked questions about Cloud Compliance

This FAQ can help if you're just looking for a quick answer to a question.

What is Cloud Compliance?

Cloud Compliance is a cloud offering that uses Artificial Intelligence (AI) driven technology to help organizations understand data context and identify sensitive data across your storage systems. The systems can be Azure NetApp Files configurations, Cloud Volumes ONTAP systems hosted in AWS or Azure, Amazon S3 buckets, on-prem ONTAP systems, databases, and OneDrive accounts.

Cloud Compliance provides pre-defined parameters (such as sensitive information types and categories) to address new data compliance regulations for data privacy and sensitivity, such as GDPR, CCPA, HIPAA, and more.

Why should I use Cloud Compliance?

Cloud Compliance can empower you with data to help you:

- Comply with data compliance and privacy regulations.
- Comply with data retention policies.
- Easily locate and report on specific data in response to data subjects, as required by GDPR, CCPA, HIPAA, and other data privacy regulations.

What are the common use cases for Cloud Compliance?

- Identify Personal Identifiable Information (PII).
- Identify a wide scope of sensitive information as required by GDPR and CCPA privacy regulations.
- Comply with new and upcoming data privacy regulations.

Learn more about the use cases for Cloud Compliance.

What types of data can be scanned with Cloud Compliance?

Cloud Compliance supports scanning of unstructured data over NFS and CIFS protocols that are managed by Cloud Volumes ONTAP and Azure NetApp Files. Cloud Compliance can also scan data stored on Amazon S3 buckets and on-prem ONTAP systems.

Additionally, Cloud Compliance can scan databases that are located anywhere, and user files from OneDrive accounts.

Learn how scans work.

Which cloud providers are supported?

Cloud Compliance operates as part of Cloud Manager and currently supports AWS and Azure. This provides your organization with unified privacy visibility across different cloud providers. Support for Google Cloud

Platform (GCP) will be added soon.

How do I access Cloud Compliance?

Cloud Compliance is operated and managed through Cloud Manager. You can access Cloud Compliance features from the **Compliance** tab in Cloud Manager.

How does Cloud Compliance work?

Cloud Compliance deploys another layer of Artificial Intelligence alongside your Cloud Manager system and storage systems. It then scans the data on volumes, buckets, databases, and OneDrive and indexes the data insights that are found.

Learn more about how Cloud Compliance works.

How much does Cloud Compliance cost?

The cost to use Cloud Compliance depends on the amount of data that you're scanning. The first 1 TB of data that Cloud Compliance scans in a Cloud Manager workspace is free. A subscription to the AWS or Azure Marketplace is required to continue scanning data after that point. See pricing for details.

How often does Cloud Compliance scan my data?

Data changes frequently, so Cloud Compliance scans your data continuously with no impact to your data. While the initial scan of your data might take longer, subsequent scans only scan the incremental changes, which reduces system scan times.

Learn how scans work.

Does Cloud Compliance offer reports?

Yes. The information offered by Cloud Compliance can be relevant to other stakeholders in your organizations, so we enable you to generate reports to share the insights.

The following reports are available for Cloud Compliance:

Privacy Risk Assessment report

Provides privacy insights from your data and a privacy risk score. Learn more.

Data Subject Access Request report

Enables you to extract a report of all files that contain information regarding a data subject's specific name or personal identifier. Learn more.

PCI DSS report

Helps you identify the distribution of credit card information across your files. Learn more.

HIPAA report

Helps you identify the distribution of health information across your files. Learn more.

Reports on a specific information type

Reports are available that include details about the identified files that contain personal data and sensitive personal data. You can also see files broken down by category and file type. Learn more.

What type of instance or VM is required for Cloud Compliance?

- In Azure, Cloud Compliance runs on a Standard_D16s_v3 VM with a 512 GB disk.
- In AWS, Cloud Compliance runs on an m5.4xlarge instance with a 500 GB GP2 disk.

  In regions where m5.4xlarge isn't available, Cloud Compliance runs on an m4.4xlarge instance instead.

You can also download and install Compliance software on a Linux host in your network or in the cloud. Everything works the same and you continue to manage your scan configuration and results through Cloud Manager. See Deploying Cloud Compliance on premises for system requirements and installation details.

Cloud Compliance is currently unable to scan S3 buckets and ANF files when it is installed on premises.

Learn more about how Cloud Compliance works.

Does scan performance vary?

Scan performance can vary based on the network bandwidth and the average file size in your cloud environment.

Which file types are supported?

Cloud Compliance scans all files for category and metadata insights and displays all file types in the file types section of the dashboard.

When Cloud Compliance detects Personal Identifiable Information (PII), or when it performs a DSAR search, only the following file formats are supported:
.PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF, and .JSON.

How do I enable Cloud Compliance?

First you need to deploy an instance of Cloud Compliance in Cloud Manager. Once the instance is running, you can enable it on existing working environments and databases from the **Compliance** tab or by selecting a specific working environment.

Learn how to get started.

Activating Cloud Compliance results in an immediate initial scan. Compliance results display shortly after.

How do I disable Cloud Compliance?

You can disable Cloud Compliance from the Canvas page after you select an individual working environment.

Learn more.

To completely remove the Cloud Compliance instance, you can manually remove the Cloud Compliance instance from your cloud provider's portal.

What happens if data tiering is enabled on Cloud Volumes ONTAP?

You might want to enable Cloud Compliance on a Cloud Volumes ONTAP system that tiers cold data to object storage. If data tiering is enabled, Cloud Compliance scans all of the data—data that's on disks and cold data tiered to object storage.

The compliance scan doesn't heat up the cold data—it stays cold and tiered to object storage.

Can I use Cloud Compliance to scan on-premises ONTAP storage?

Yes. As long as you have discovered the on-prem ONTAP cluster as a working environment in Cloud Manager, you can scan any of the volume data.

Alternatively, you can run compliance scans on backup files created from your on-prem ONTAP volumes. So if you're already creating backup files from your on-prem systems using Cloud Backup, you can run compliance scans on those backup files.

Learn more.

Can Cloud Compliance send notifications to my organization?

Yes. In conjunction with the Highlights feature, you can send email alerts to Cloud Manager users (daily, weekly, or monthly) when a highlight return results so you can get notifications to protect your data. Learn more about highlights.

You can also download status reports in .CSV format that you can share internally in your organization.

Can I customize the service to my organization's needs?

Cloud Compliance provides out-of-the-box insights to your data. These insights can be extracted and used for your organization's needs.

Additionally, you can use the **Data Fusion** capability to have Cloud Compliance scan all your data based on criteria found in specific columns in databases you are scanning — essentially allowing you to make your own custom personal data types.

Learn more.

Can Cloud Compliance work with the AIP labels I have embedded in my files?

Yes. You can manage AIP labels in the files that Cloud Compliance is scanning if you have subscribed to Azure Information Protection (AIP). You can view the labels that are already assigned to files, add labels to files, and change labels when a label already exists.

Learn more.

Can I limit Cloud Compliance information to specific users?

Yes, Cloud Compliance is fully integrated with Cloud Manager. Cloud Manager users can only see information for the working environments they are eligible to view according to their workspace privileges.

Additionally, if you want to allow certain users to just view Cloud Compliance scan results without having the ability to manage Cloud Compliance settings, you can assign those users the *Cloud Compliance Viewer* role.

Learn more.