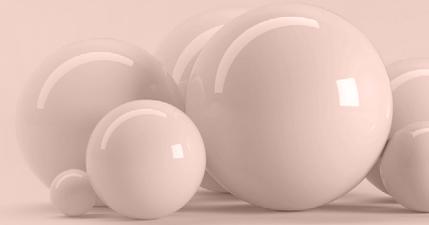


How One Company Meets GDPR Cloud Requirements and Maintains Data Privacy with Cloud Compliance



Data privacy entered a new age with the enactment of GDPR. Cloud requirements to meet cost and service availability were now joined by a new challenge: managing and protecting extremely sensitive personal data. For one prominent California-based tech company, this meant finding an automated way to identify such data and report on it. The solution they found was [NetApp Cloud Compliance](#).

In this post, we look at the challenges this customer faced in meeting the requirements of the GDPR, why they chose Cloud Compliance, and their experiences of using the product so far.

Customer

California-based SaaS unicorn with a worldwide customer base and more than 35 industry awards

Customer's Offering

Digital Adoption Platform

Challenge

Reduce manual workload involved in identifying and protecting or removing personal data to meet GDPR requirements

NetApp Solution

Cloud Compliance for Amazon S3

Value Created

Faster response to potential compliance issues and 80% reduction in time spent reviewing data.

Privacy by Design for Personal Data: The Company's Compliance Journey

The customer's software is an invisible overlay across any website, application, or online platform. The software is designed to help organizations gain value out of their digital assets by improving digital experiences for customers and employees, through actionable data that identifies problem areas and visual cues that help users complete tasks and navigate their way through software.

The company's software uses **artificial intelligence (AI)** and **machine learning (ML)** to analyze usage patterns and provide proactive support at potential roadblocks in the user journey. In order to do that, it collects large amounts of usage data, stored in Amazon S3, that must remain GDPR compliant.

The company was concerned with ensuring compliance with the highest degree of security standards as well as the ability to technically control and oversee the [personally identifiable information \(PII\) stored in their system](#).

To sort through this data manually would have required a level of oversight that would not only be very time-consuming but also open to human error. To avoid those concerns, the company decided to tighten their data governance by implementing a state-of-the-art data privacy technology.

An Automated Solution with Cloud Compliance

Since manually reviewing the data for personal information was untenable, the company decided it needed a solution that could automatically scan its data for personal information that could fall within the scope of the GDPR and other data privacy legislation. The solution they chose was NetApp Cloud Compliance.

The security team, led by the chief information security officer, researched a number of data privacy tools. However, it found other services didn't offer the same range of benefits. Cloud Compliance was comprehensive: it was able to automate the search process and it allowed data to be scanned in multiple storage repositories, beyond Amazon S3. It also allowed the company to keep their data within their control at all times, which was a major security concern.

All Set for Time and Cost Savings

The security team selected a trial S3 bucket to put Cloud Compliance through its paces and immediately noticed how quickly and easily they could set the service up. Within around 36 hours, the application had already completed a full initial scan of hundreds of GB of data.

Using Cloud Compliance, the team automatically identified all of the private data in their system and any data that was stored in publicly accessible buckets. Once this data was identified, it was then easy to either protect or remove it, as needed. And once the initial scan was conducted, Cloud Compliance began to maintain always-on privacy protection, scanning any new data changed in the repository or added to it.

To perform the same work manually would've been a considerable undertaking. Using Cloud Compliance, standards changed completely. Based on the initial trial, the company estimated that it was able to cut the time it normally spent on keeping data in check by 80%. This translated into a significant reduction in resources and enables the team to focus on other aspects of IT security.

With Cloud Compliance now fully implemented, the company can look forward to demonstrating and complying with the GDPR. With cloud requirements for cost controls and data protection fulfilled, the company is confidently moving ahead with use of Cloud Compliance for its production environments as well.

Beyond Data Classification

How do you keep track of your sensitive private data in the cloud? Regulations like GDPR are only growing in force, and many companies are already paying the price for not taking these data privacy laws seriously. What happens when data classification isn't enough?

This Cloud Compliance case study showed how one company turned to NetApp to solve the data privacy challenge. With Cloud Compliance, they found a way to automatically manage sensitive private data, respond to GDPR cloud requirements, and extend data privacy scanning capabilities across repositories.

To start protecting your sensitive private data, try Cloud Compliance for free on 1 TB of your data.

Try Out Cloud Compliance Now