anjuna®

CASE STUDY

Securing Data For An Entire City With Confidential Computing

Background

A major European telecommunications provider can trace its lineage back to the mid-1800s; it has grown to provide over 50% of mobile data in its home country, selling services under its name and various subsidiary brands. Citizens, enterprises, and the federal government rely on this provider for fixed-network and mobile communications, with a significant portion of its business dedicated to developing and maintaining the required infrastructure and accompanying IT platforms.

> *In the data economy, nothing is more important than ensuring the confidentiality and integrity of the data and simultaneously making it available for our data consumers to analyze. Anjuna made that all possible without changing a single line of code.*
>
> - CSO, Major Telecom Provider

Challenge:

A Telecom provider must ensure data confidentiality in a large-scale multi-party computation (MPC) project between data producers and consumers.

Key Result:

With no modification to the codebase, the Telecom provider rapidly deployed Anjuna® Confidential Computing software to secure data on AWS.

Challenges

The Telecom company undertook a unique and revolutionary project: to create a Smart City. The City would be interconnected to make it more efficient, ecological, and socially inclusive in a secure MPC environment between data producers and consumers. Multiple data producers needed to share proprietary data with a trusted third-party ML application that would provide insights to numerous data consumers and keep the shared data confidential. The Telecom provider needed to ensure data privacy from producer to producer, consumer to consumer, and producer to consumer to create a trusted relationship. Privacy for the data producers remained a chief concern because, in most cases, the producers expose raw code when generating it in real-time. Inherently, the lack of protection around data-in-use meant a break in the chain of trust between the data producers and the consumers.

Environment

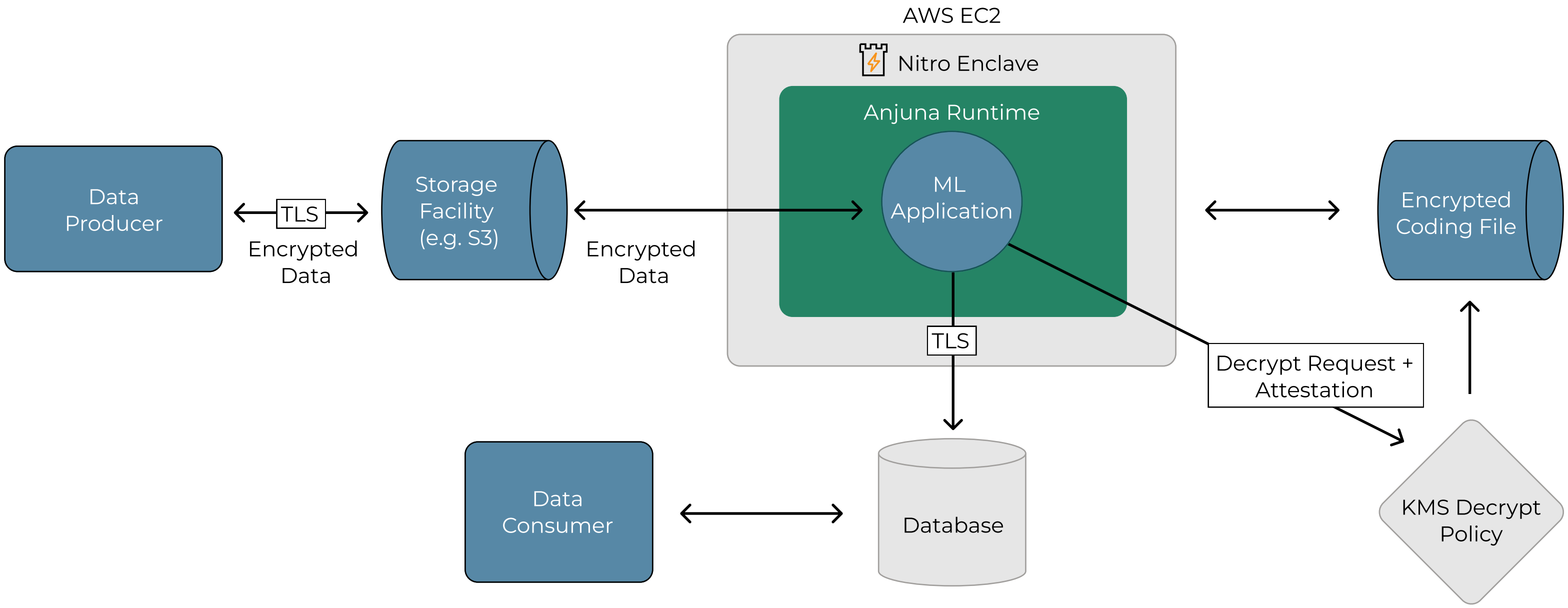
AWS is the cloud of choice for the underpinnings of the Smart City. A proprietary machine learning (ML) application functioned as the focal point for all the data generated and consumed within the City. The Telecom provider leveraged the in-built AWS Key Management Service (KMS) to ensure seamless integration with the rest of the AWS cloud. The architecture is flexible by design and ready to scale as needed, yet the quintessential matter of guaranteeing privacy and maintaining confidentiality remains.

Solution

The Telecom provider learned that with Anjuna, Confidential Computing could address the project challenges using a single binary. Anjuna's Confidential Computing software unlocked the ability to migrate the proprietary ML application into AWS Nitro Enclaves to protect data in real-time by default. Elegant in its simplicity, Anjuna achieved end-to-end data protection for the entire project without modifying the existing codebase. Anjuna ensured data protection in three states (in use, at rest, and in transit), ML applications processing the data are in confidential compute, and code is validated via attestation. Through attestation, data producers can validate that the ML application is legitimate and protected by Confidential Computing before providing their sensitive data.

Results

Anjuna protected producer data and code from unauthorized viewers, making the process seamless while eliminating the development time required to gain the benefits of Nitro Enclaves on AWS. Now, the Telecom company has established a trusted relationship between the data producers and consumers. The data producers know that their privacy and integrity are guaranteed, and the data consumers are now free to process and analyze the data using their tool of choice.



About Anjuna

Anjuna Security makes the public cloud secure for business. Confidential Computing software from Anjuna Security effortlessly enables enterprises to safely run even their most sensitive workloads in the public cloud. Unlike complex perimeter security solutions easily breached by insiders and malicious code, Anjuna leverages the strongest hardware-based secure computing technologies available to make the public cloud the safest computing resource available anywhere. Anjuna is based in Palo Alto, California.

anjuna.io | info@anjuna.io | 650-501-0240