anjuna®

CASE STUDY

Advanced Data Security And Privacy In A Multi-Party Computation Environment

Background

A national bank headquartered on the east coast of the United States can trace its roots back to the turn of the century. Since its inception, it has become one of the leading financial institutions in the country, with a customer base of nearly 10% of the US population. It has extended operations in every corner of the globe. It is responsible for transacting millions of dollars daily, with total assets of over $1 trillion across commercial, wealth management, and investment banking.

> *Anjuna took the guesswork out of strengthening our data security and allowed us to add secure enclaves into our environment quickly. Our customer data remains protected from other banks, cloud admins, and insiders, and we still can cooperate with other institutions to identify fraudulent activities.*
>
> - CISO, National Bank

Challenges:

A financial institution wants a secure way to share fraud prevention data without jointly exposing client PII to other parties.

Key Result:

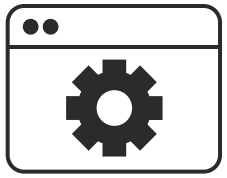
Anjuna software makes multi-party computation safe, secure, and easy to implement. PII data from each provider is protected, and all parties benefit from the computation results.

Challenges

As banking has become predominately digital, the financial institution built a platform to better identify and defend against criminals defrauding their clientele using credit card data. To ensure the highest possible accuracy in detecting fraudulent charges, the bank wants to work with other financial institutions in a multi-party computation (MPC) environment to cast as broad a net as possible. Yet the bank cannot risk exposing its clients' personally identifiable information (PII) to the other institutions on the platform or any unauthorized insiders or third parties in the cloud.

Environment

The bank first built a proprietary MPC application with the underpinnings of a SQL database and housed it on an Azure instance. The bank also leveraged HashiCorp Vault for key management, offering a tried-and-true level of protection against outside attack vectors. To secure personal data while in use, the company explored the capabilities of Intel SGX secure enclaves to protect the MPC application and HashiCorp Vault further.



MUTLI-PARTY COMPUTE PLATFORM

HASHICORP VAULT KEY MANAGEMENT

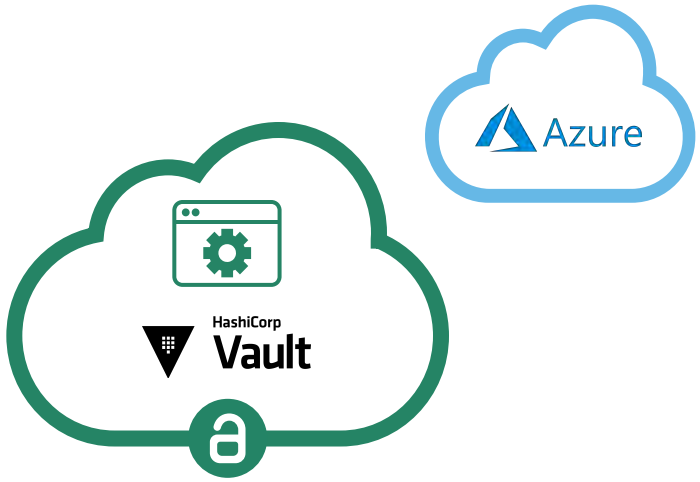
AZURE WITH INTEL SGX

Solution

Seeking to harden the security of PII in the cloud, the bank turned to Anjuna to bring secure, enclave-grade protection on Azure leveraging Intel SGX. The institution used Anjuna® Confidential Computing software to add a layer of airtight security around the proprietary MPC application and reinforce Vault's already best-in-class key management. Anjuna made securing the bank’s MPC solution and HashiCorp Vault fast and easy with no changes to the code of either application and with minimal performance impact on the applications.

Results

With the advanced protection of Anjuna Confidential Computing software in place on Azure, the bank enlisted other banking institutions to join in its initiative to prevent fraud. All parties now safely contribute transaction data from their respective customer bases without the risk of accidentally exposing PII. Furthermore, anyone with access to the public cloud, even with root access, cannot steal customer information. The bank and associated financial institutions are one step closer to stopping fraud wherever it occurs.



About Anjuna

Anjuna Security makes the public cloud secure for business. 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.io | info@anjuna.io | 650-501-0240