CASE STUDY

Enclave-Level Protection For Multi-Party Computation (MPC) Digital Asset Custody

Background

With offices in the UK, Portugal, and Rio de Janeiro, Parfin is on a mission to enable the widespread and secure institutional adoption of digital asset technologies and help create a more efficient and fair financial system. Since 2019, Parfin employs multi-party computation (MPC) in its digital asset custody system to help blend the world of traditional finance with leading-edge technologies to bring forth new opportunities and substantial efficiency gains in the digital age.

> *"Anjuna provided the level of security we envisioned for our Parfin MPC Custody system. Now, we can ensure our customers' distributed key shares are protected by an additional layer of secure enclaves that wasn't possible without Anjuna."*
>
> - Alex Buelau, CTO and Co-founder, Parfin

Challenges:

Parfin uses advanced MPC technology to protect customers' digital assets, but Parfin wanted to go further and provide additional layers of security against potential unauthorized access of the cloud provider and insiders.

Key Result:

Anjuna provided enclave-level security to safeguard key components of Parfin's MPC solution against unauthorized access.

Challenges

Already a highly security-conscious organization, Parfin is SOC2 certified and provides several layers of security including MFA, encryption at rest and in-transit, zero-trust microservice architecture, firewalls, and private networks as part of its security architecture, with sensitive data encrypted in HSMs. Looking to add another layer of security, Parfin explored AWS Nitro Enclaves to secure key components of its MPC solution. However, a typical in-house implementation to run their MPC custody application in a secure enclave meant a lengthy, costly, and complex process to re-architect its application. Parfin wanted to increase security measures to offer its customers peace of mind without impacting the performance of its SaaS service.

Environment

Being cloud-native, Parfin makes extensive use of AWS and Azure. The company leverages MPC technology as part of the foundation for securing digital key shares that represent distributed versions of cryptographic private keys. At the same time, AWS Nitro Enclaves were worth exploring for the additional security benefits of secure enclaves to protect cryptographic distributed keys data while in use.

Solution

Parfin required a solution to harden the protection for customers' distributed cryptographic key shares provided by its MPC custody solution. Anjuna® Confidential Computing software extends the security of AWS Nitro enclaves by providing an isolated environment for Parfin's MPC Custody application in minutes. The ability to secure all MPC key shares and its customers' digital assets data with Anjuna software allowed for secure joint computation from various participants, maintaining privacy across distributed channels. Anjuna enabled secure enclave protection of the Parfin MPC custody solutions without recoding or refactoring the applications.

Results

Using Anjuna, Parfin gained the hardened security of AWS Nitro Enclaves with the click of a button. Parfin avoided the pitfalls of do-it-yourself (DIY) implementation altogether saving months of time and development expenses. The solution went live without issues within days and Anjuna enabled Parfin to be self-sufficient during the entire implementation process. Parfin now holds an unparalleled security advantage in the crypto market where its customers can fully trust that the custody of their keys is theirs and theirs alone.

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