anjuna®

World-Class Data Protection, Securing Customer Keys In The Cloud

Background

Paradigm is the leading institutional liquidity network for crypto derivatives traders. It provides a single point of access to multi-dealer block liquidity for crypto futures and options across the largest derivatives exchanges globally.

Paradigm's mission is simple: provide on-demand liquidity for traders, anytime and anywhere, without compromising on trading preferences, execution costs, and immediacy. Its customers execute derivative transactions on the biggest crypto exchanges and require both speed and security.

PARADIGM

Industry
Cryptocurrency, FinTech

Use Case
Secure customer and API accounts against breaches

Benefits
- Ironclad security as a competitive differentiator
- Enhanced ability to attract large institutional customers

No Recoding

Instantly protect applications at runtime with zero modifications to the codebase

Rapid Time-to-Value

Paradigm quickly implemented Anjuna to secure its platform

Seamless Integration

Anjuna offers native integration with AWS

Challenges

One of Paradigm's primary growth initiatives is to attract large cryptocurrency exchanges as customers. To do that, Paradigm must satisfy the exchanges' stringent requirements for protecting the API keys that Paradigm's platform uses to settle transactions at the exchanges' APIs. Additionally, any security enhancements must not add latency to customers' transactions.

With security and transaction latency top of mind, Paradigm sought to optimize its platform by:
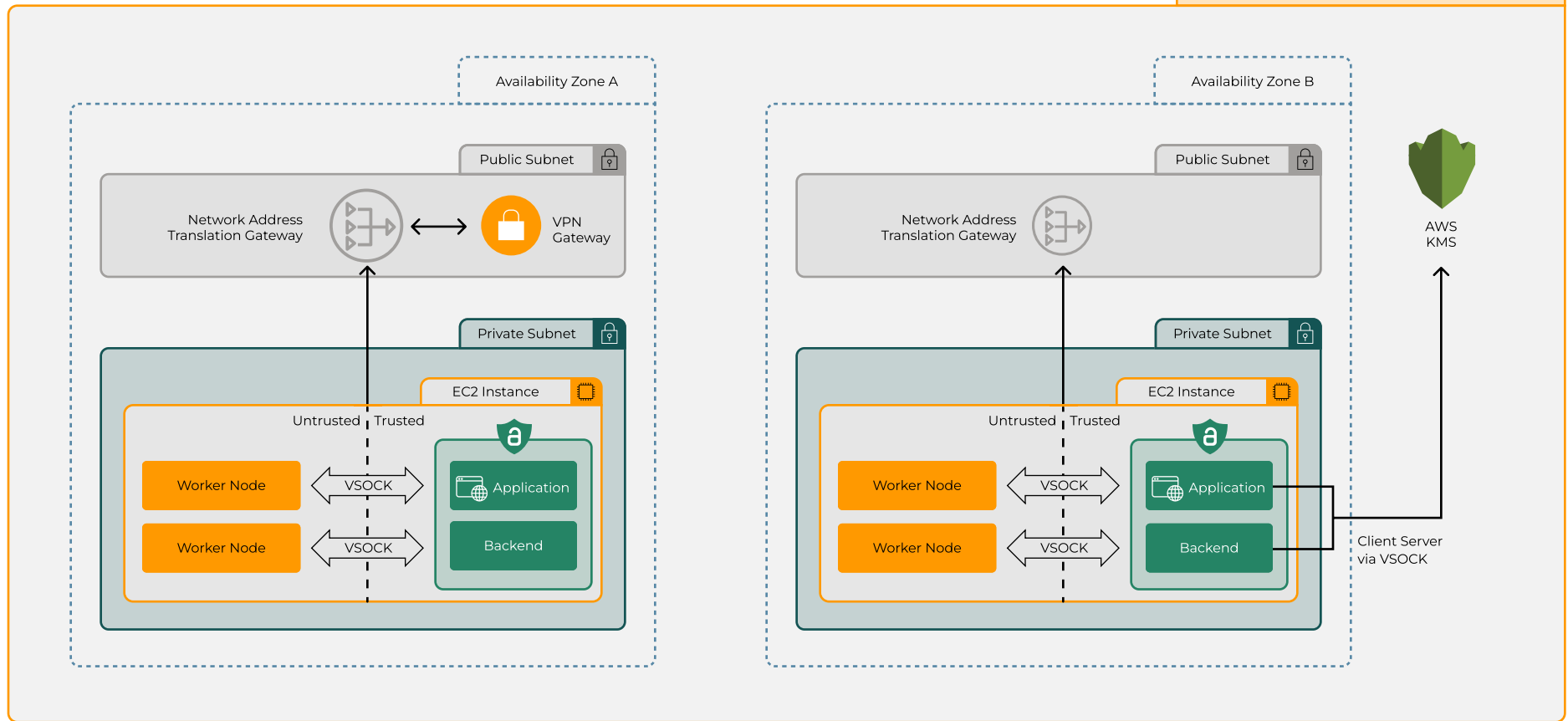
- Deploying Confidential Computing to eliminate any chance that an infrastructure breach could allow attackers or insiders to exfiltrate API keys from memory
- Minimizing transaction latency by reducing the number of calls and network hops to AWS KMS, which Paradigm's platform uses to encrypt and decrypt API keys

Since Paradigm's platform runs on Amazon and uses its EKS and KMS services, Paradigm planned to leverage AWS Nitro Enclaves for runtime protection of its core application and database, which handles and stores encrypted API keys. To accelerate the shift to the new secure architecture and avoid any additional development cost, Paradigm looked for a Confidential Computing platform that natively works with AWS Nitro Enclaves and eliminates the need to re-engineer its applications.

Solution

Paradigm chose the Anjuna Confidential Computing Platform. Anjuna seamlessly integrates with AWS Nitro Enclaves and does not require applications to be re-engineered in order to take advantage of them. Apps run unmodified in Anjuna's Confidential Runtime while being protected by AWS Nitro Enclaves, providing quick time to value.

Using Nitro Enclaves afforded Paradigm a secondary benefit. Instead of frequently calling the KMS to decrypt API keys (high latency), Paradigm could safely retrieve data keys from the KMS to subsequently decrypt API keys locally (low latency) within the secure environment of Nitro Enclaves.

PARADIGM

AWS EKS Cluster

Availability Zone A

Public Subnet

Network Address Translation Gateway ←→ VPN Gateway

Private Subnet

EC2 Instance

Untrusted | Trusted

Worker Node ←VSOCK→ Application

Worker Node ←VSOCK→ Backend

Availability Zone B

Public Subnet

Network Address Translation Gateway

Private Subnet

EC2 Instance

Untrusted | Trusted

Worker Node ←VSOCK→ Application

Worker Node ←VSOCK→ Backend

AWS KMS

Client Server via VSOCK

Sometimes it feels like you need a Ph.D. to navigate the deeply technical and complex world of configuring and using secure enclaves. Anjuna makes it as simple as counting to 10.

• **Jameel Al-Aziz, Software Architect, Paradigm**

Results

Paradigm now offers the highest level of security to its customers. By providing an easy way to implement Confidential Computing on AWS without having to re-architect its platform, Anjuna helped Paradigm realize several outcomes:

- Current and future applications can easily leverage AWS Nitro Enclaves without engineering efforts, shortening time to value for new, highly secured digital offerings
- Paradigm can attract large institutional customers that demand security for API keys, offering a differentiated high trust service that allows customers to maintain complete confidentiality and privacy of their keys which are now encrypted end to end and inaccessible even to Paradigm
- Paradigm can increase customer satisfaction and build more efficient markets by eliminating settlement latency, previously 4 seconds (average) to 60 seconds (max)

With Anjuna, Paradigm increased security and performance, enabling Paradigm to position itself as the premier, security-first platform for discerning cryptocurrency traders and investors.

> *Anjuna has empowered us to be confident that we're offering our customers leading, enterprise-class data security. We can sleep comfortably knowing that our customers' credentials are as safe and secure as they can possibly be.*
>
> **• Jameel Al-Aziz, Software Architect, Paradigm**

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