

Customer Story

타인에이아이, 안랩과 함께 핀테크 최적화 AWS 환경 구축



TainAI

웹사이트

www.oreurak.kr

산업

핀테크

운영환경

AWS 포함 멀티 클라우드

솔루션

- AhnLab Cloud
- AhnLab CPP
- 보안관제서비스

도입효과

- AWS 환경으로의 성공적인 이전
- 마이데이터 인증 심사 항목을 준수하는 견고한 보안 체계 확립
- 멀티 클라우드 기반 재해복구센터 구축

타인에이아이 소개

타인에이아이(TainAI)는 주식 포트폴리오 서비스 '오르락(oreurak)'을 제공하는 핀테크 스타트업입니다. 오르락은 공동인증서 연동 한 번으로 여러 증권사에 있는 주식을 모아볼 수 있는 주식 포트폴리오를 만들 수 있으며, 종목, 섹터, 국가, 계좌 별 포트폴리오도 자동으로 관리할 수 있습니다.

타인에이아이는 다른 주식 투자자와 투자 정보 의견을 교류할 수 있는 기능을 추가하여 더 많은 고객을 유치하고, 증권사 제휴를 통해 주식매매 기능까지 통합하여 소셜 증권 플랫폼으로 도약할 계획입니다.

도전과제

타인에이아이는 타 CSP(Cloud Service Provider)의 클라우드 환경에서 운영 중이던 서비스를 아마존웹서비스(Amazon Web Services: AWS)로 이전하였습니다. 이 과정에서, 마이데이터 인증 심사 요구 항목에 맞춰 클라우드 인프라를 설계하고 구축해야 했습니다. 또한, 비상 사태 발생 시 서비스가 마비되는 것을 방지하기 위해 구축하는 재해복구센터(Disaster Recovery Center)를 AWS와 타사 클라우드 서비스를 혼용하는 멀티 클라우드 기반으로 조성하고자 했습니다.

솔루션

우선, 차세대 MSP 서비스 '안랩 클라우드(AhnLab Cloud)'를 통해 안랩 전문가들이 마이

데이터 인증 심사 항목과 타인에이아이의 현황을 교차 분석하였습니다. 이후, 타인에이아이가 운영하는 서비스의 특징과 요구사항을 도출하고, 개선 혹은 변경이 필요한 대상을 선정하여 AWS 클라우드 환경을 구축했습니다.

또, 타인에이아이가 AWS와 타 CSP의 서비스를 함께 운영하는 멀티 클라우드 환경임을 고려하여 두 클라우드 간 가상사설망(Virtual Private Network: VPN)을 구성하고, 데이터 싱크(Sync)를 설정하여 두 환경이 효과적으로 연동되도록 하였습니다. 추가적으로, 하이브리드 클라우드와 같이 다양한 환경에 걸쳐 탁월한 가시성을 제공하는 클라우드 워크로드 보안 플랫폼 'AhnLab CPP'를 도입해 클라우드 서비스 전체의 보안을 강화하고, 안랩의 전문성이 축적된 보안관제서비스를 함께 활용하여 운영의 효율성까지 더했습니다.

“ AWS로의 이전, 재해복구센터 구축 등 타인에이아이의 장기적인 비즈니스 기반이 될 주요 과제들을 안랩 클라우드를 통해 효과적으로 해결할 수 있었습니다. 앞으로도 안정적인 클라우드 환경을 바탕으로 유연하고 경쟁력 있는 주식 포트폴리오 서비스를 제공할 계획입니다.

- 타인에이아이 이수완 대표 ”

도입 효과

타인에이아이는 AWS 이전 초기부터 안랩 클라우드와 함께 보안을 충분히 고려하여, 마이데이터 인증 심사 항목을 준수하는 클라우드 인프라를 구성했습니다. 또한, 멀티 클라우드 기반의 재해복구센터를 효과적으로 구축하여, 장기적인 관점에서 재해 상황에 대비하고 비즈니스에 회복력(resilience)을 더했습니다.

아울러, 안랩의 탁월한 기술력과 노하우가 집약된 클라우드 보안 솔루션과 보안관제서비스를 도입해 사이버 위협을 상시적으로 모니터링하고 탐지 및 대응 역량을 최적화했습니다. 이를 통해, 정보자산을 효율적으로 보호하는 동시에 비즈니스에 집중할 수 있는 체계를 마련했습니다.

안랩 클라우드 소개

안랩 클라우드(AhnLab Cloud)는 기존 구축과 운영에 중점을 둔 MSP(Managed Service Provider) 서비스에 안랩의 독보적인 보안 역량을 더한 '차세대 MSP' 서비스입니다. 안랩 클라우드는 클라우드 설계부터 구축과 운영까지 모든 단계에서 보안에 최적화된 클라우드 관리 역량을 '원스톱'으로 제공해 고객이 마주한 어려움들을 해결합니다. 컨설팅 단계서부터 안랩의 클라우드 보안 프레임워크를 기반으로 구축 방안을 도출하고 보안 컴플라이언스를 반영해 최적화된 서비스 아키텍처를 수립합니다. 또한, 클라우드 보안 침해의 주요 원인인 설정 오류 등 운영 실수로 인한 사고도 사전에 예방해 고객의 비즈니스에 안정성을 더합니다.