

Customer Story

에어스메디컬, 안랩 클라우드로 디지털 의료 기술 혁신



AIRS MEDICAL

웹사이트

airs-medical.com

산업

의료 & 헬스케어

운영환경

Amazon Web Services

솔루션

- AhnLab Cloud
- 보안관제서비스

도입효과

- 조직에 최적화된 안정적 AWS 환경 조성
- 의료 데이터에 대한 강력한 보안 확보
- 컴플라이언스를 준수한 보안 체계 확립

에어스메디컬 소개

에어스메디컬(AIRS Medical)은 헬스케어 시장의 패러다임을 바꾸는 의료 AI 솔루션을 개발해 공급하는 스타트업입니다. 에어스메디컬의 'SwiftMR'은 딥러닝을 활용하여 저품질 MR 영상을 고품질로 복원해줌으로써 MRI 촬영시간을 최대 50%까지 단축해주는 의료기기 소프트웨어입니다. 의료기관에서 별도 초기투자 없이 소프트웨어 구독만으로 간편하게 MRI 장비 성능을 업그레이드할 수 있도록 SaaS(Software-as-a-Service) 형태로 제공됩니다.

도전과제

아마존웹서비스(Amazon Web Services: AWS)를 도입하여 운영 중인 에어스메디컬은 의료 데이터를 외부 환경에 안전하게 보관하기 위한 보안 요구사항을 충족해야 했습니다. 이 과정에서, 비즈니스에 가해지는 영향을 최소화하기 위해 기존 구축되어 있는 인프라를 변경하지 않고 CC(Common Criteria) 인증을 받은 보안 솔루션 운영이 필요했습니다.

에어스메디컬은 의료 정보와 같은 민감 데이터를 보호하고 유출을 방지하기 위해 보안 솔루션을 원활하게 운영하여, 웹을 통한 침입 등 침해를 방어하고 혹여라도 보안 이슈가 발생할 경우 즉각 대응할 수 있는 체계를 갖춰야 했습니다.

솔루션

안랩은 차세대 MSP 서비스 '안랩 클라우드(AhnLab Cloud)'의 일환으로 컨설팅을 진행

하여 의료 및 헬스케어 서비스 기업 맞춤형 클라우드 컴플라이언스를 검토하고 에어스메디컬의 현황을 분석했습니다. 그리고, 분석 결과를 토대로 에어스메디컬 조직 구조와 업무 현황에 적합한 접근 통제 및 권한 부여 작업을 진행했습니다.

또한, 내·외부에서 발생할 수 있는 위협에 효과적으로 대응하기 위해 방화벽 관리 서비스 ‘AWS Firewall Manager’와 지능형 위협 탐지 서비스 ‘Amazon GuardDuty’ 등 AWS의 보안 서비스들을 추가로 구성하였습니다. 아울러, 쿠버네티스 기반 애플리케이션 배포, 조정 및 관리 자동화 등을 지원하는 AWS EKS(Elastic Kubernetes Service)의 보안 설정도 강화했습니다.

이 밖에, CC 인증이 완료된 웹 애플리케이션 방화벽(Web Application Firewall: WAF) 솔루션을 이중화 구성하고, 안랩의 전문성과 노하우가 축적된 보안관제서비스와 연계하여 운영 중인 AWS 클라우드 환경 전반의 보안성을 높였습니다.

“

안랩 클라우드를 통해 의료 서비스 분야 클라우드 규제 준수와 보안 강화를 원스톱으로 신속하게 해결할 수 있었습니다. 앞으로도 안정적인 클라우드 환경 조성에 박차를 가해 고객이 안심할 수 있는 서비스를 제공할 것입니다.

- 에어스메디컬 이진구 대표

”

도입 효과

에어스메디컬은 안랩 클라우드 서비스에 따라 조직의 현황에 부합하는 보안 체계를 재구성하고 WAF 솔루션 및 안랩의 보안관제서비스를 도입해 침해 위협 모니터링, 탐지 이벤트 최적화를 바탕으로 강력한 침해 대응 역량을 확보했습니다. 또한, 직무 담당자 별 접근 권한을 차등 부여하고, 각 사용자의 활동을 모니터링함으로써 내·외부 보안을 강화하고 장기적으로 안정적인 비즈니스를 운영할 수 있는 견고한 클라우드 환경을 조성했습니다.

안랩 클라우드 소개

안랩 클라우드는 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.