AKAMAI 고객 사례

KKLab

Akamai의 제로 트러스트 솔루션을 도입해 내부 및 외부 네트워크의 보안 기능과 유연성을 결합하는 벤처 스튜디오

100
매일 자동으로 차단되는 악성 이메일 건수

30분 안에 개념 증명(PoC) 설정 완료

유연성을 유지하면서 보안 강화

2019년 혁신적인 연구 기업인 KKLab으로 거듭난 KKBOX의 R&D팀은 2015년에 정보 보안을 더욱 면밀하게 살펴보기 시작했습니다. R&D팀은 다양한 실험을 진행했고 외부 전문가 팀을 고용해 해커 침입 훈련 및 침투 테스트를 실시해 유출 가능성이 있고 개선될 수 있는 시스템을 발견했습니다. R&D팀은 멀티팩터 인증을 구현하기로 결정했고, 이와 함께 표적 공격을 막기 위해 Akamai Secure Internet Access Enterprise, 애플리케이션 시스템 접속 보안을 위해 Akamai Enterprise Application Access를 도입했습니다. 이 2가지 클라우드 기반 정보 보안 서비스를 도입함으로써 제로 트러스트 보안을 구축했습니다.

제로 트러스트 아키텍처로의 전환을 통해 기존 VPN의 취약점 보완

KKLab의 AVP 헝이 첸(Hung-Yi Chen)은 KKBOX 그룹은 항상 기술 지향적이었다고 말했습니다. 헝이 첸은 2005년에 학업을 마치고 KKBOX 그룹에 입사했으며 15년간 R&D 기술에 주력해 왔습니다. 그룹이 성장하면서 흥미롭고 까다로운 신기술을 많이 도입하도록 지원했습니다. 2010년 사이트 안정성 엔지니어링팀을 만들었고 CI/CD를 도입했으며 하이브리드 클라우드 아키텍처를 배포했습니다. 이후 클라우드 기반 기술 서비스 제공업체인 KKLab에 합류했습니다. KKLab은 클라우드 및 인공지능을 연구해 기업의 기술 전환을 지원합니다.

KKLab은 KKBOX, KKTV, KKStream, KKTIX, theFARM 등 그룹 내 다양한 기업들에게 기술 서비스를 지원합니다. 또한 인공지능 및 머신러닝 툴 체인, 빅데이터 고속 컴퓨팅 플랫폼, 멀티 하이브리드 클라우드 구축, 컨설팅 서비스 등에 집중하면서 외부 기업들과 협력하고 있습니다. 디지털 지원을 확장해 하이테크 제조, 유통 물류, 미디어 및 엔터테인먼트, 금융 및 보험 등 여러 분야의 기업들에게 서비스를 제공합니다.

KKLab
대만 타이페이
www.kklab.com

업종
미디어

도전과제
Multi-Factor Authentication, 애플리케이션 시스템 접속 보안, 표적 공격 방어 강화 등을 지원하는 제로 트러스트 보안으로 전환

솔루션
- Secure Internet Access Enterprise
- Enterprise Application Access

KKLab은 기술 서비스를 제공하면서 정보 보안을 핵심 목표로 삼고 있습니다. 특히, 써드파티 정보 보안 테스트 기능을 도입했으며, 해킹 침입 훈련을 이용해 시스템의 잠재적인 보안 취약점을 밝혀냈습니다. 많은 직원들은 KKLab의 정보 보안 수준이 높고 테스트를 쉽게 견뎌낼 수 있다고 확신했습니다. 그러나 데이터베이스 공격 테스트를 통해 상당수의 계정과 비밀번호가 해커에 의해 노출되어 위험해질 수 있다는 사실이 밝혀졌습니다. KKLab 팀은 기존의 정보 보안 프레임워크와 VPN을 통해 인트라넷 리소스에 접속하는 개념이 실제로 상당히 위험하다는 것을 깨달았습니다. 해커가 내부 계정 비밀번호를 입수하면 VPN을 따라 인트라넷에 들어가서 마음대로 정보를 탈취할 수 있고 그룹은 큰 운영 리스크에 노출될 수 있습니다.

이러한 리스크를 방지하기 위해 KKLab은 2단계 보안 강화 조치를 적용했습니다. 우선 Multi-Factor Authentication을 도입했습니다. 모든 직원들은 VPN에 접속하기 전에 계정 비밀번호와 일회용 비밀번호 코드를 동시에 입력해야 합니다. 아울러 KKLab은 제로 트러스트 아키텍처를 적극적으로 계획하고 있습니다. 제로 트러스트 아키텍처는 모든 방문자가 실제로 정상 사용자인지 지속적으로 확인하고 검증합니다. KKLab의 궁극적인 목표는 제로 트러스트 기반의 보다 유연하고 안전한 근무 환경을 조성하는 것입니다.

Secure Internet Access Enterprise와 Enterprise Application Access로 보호망을 구축해 모든 의심스러운 접속 차단

엔터테인먼트 미디어 및 스트리밍 기술 서비스에 역점을 두고 있는 KKBOX 그룹이 유연성을 활용하고 악성 행동을 즉시 차단하기를 기대한다고 첸 부사장은 말합니다. 직원들의 창의성을 저해하는 과도한 통제 조치를 원하지 않기 때문에 KKLab은 제로 트러스트 모델 도입을 권장합니다. 솔루션은 배포 및 유지 관리가 용이해야 하며 사용자의 워크플로우에 미치는 영향을 최소화해야 합니다. 이런 요구사항에 대응하기 위해 KKLab은 Akamai의 솔루션을 사용하기로 결정했습니다.

첸은 "Akamai Secure Internet Access Enterprise는 인트라넷으로부터의 접속을 필터링 및 분석하고 악성 IP 주소 또는 도메인이 있는지 정확하게 판단합니다. 그 열쇠는 빅데이터 데이터베이스에 있습니다."라고 언급합니다. 또한 첸 부사장은 Akamai의 시장 점유율이 높다고 덧붙였습니다. KKLab이 Akamai를 선택한 첫 번째 이유는 대량의 악성 행동 데이터를 수집하는 CDN 및 DDoS 차단 서비스를 중심으로 기반이 구축되었기 때문입니다. 이러한 강력한 리소스는 Secure Internet Access Enterprise의 효과적인 운영을 뒷받침하는 중요한 기반입니다.

두번째 이유는 시장에서 Secure Internet Access Enterprise와 유사한 솔루션을 살펴보면 배포 요구사항이 다릅니다. 모든 엔드포인트 디바이스에 에이전트를 설치해야 하며, 기업 백본 네트워크에 커넥터를 설치해야 하는 경우도 있습니다. Akamai는 동시 접속을 지원합니다. Akamai Connector는 경량 가상 머신 이미지이며, 몇 가지 네트워크 설정만 조정하면 됩니다. KKLab은 2018년에 개념 증명(PoC)을 30분 안에 완료했습니다. Secure Internet Access Enterprise가 풍부한 인텔리전스 데이터베이스와 Akamai Connector를 통해 요구사항에 부합한다는 것을 확인한 이후 Akamai와 협력하기로 결정했습니다.

> Akamai Secure Internet Access Enterprise는 인트라넷으로부터의 접속을 필터링 및 분석하고 악성 IP 주소 또는 도메인이 있는지 정확하게 판단합니다. 그 열쇠는 빅데이터 데이터베이스에 있습니다.
>
> **헝이 첸(Hung-Yi Chen)**
> KKLab AVP

KKLab은 내부 및 외부 접속을 필터링하는 것 외에도, 모든 위치에서 인트라넷 리소스에 접속하는 직원의 행동을 제어하기 위해 2020년 Enterprise Application Access를 도입했습니다. KKLab은 Docker 이미지를 사용해 Akamai Connector를 배포했습니다. 지금까지 KKLab은 Enterprise Application Access를 통해 100여 개의 내부 애플리케이션 시스템에 대한 접속을 제공했습니다. 많은 파트너들이 인트라넷 시스템에 접속하기 위해 보다 복잡한 VPN 채널을 사용했었지만, 이제는 IT 유지관리 리스크를 줄이고 동료들의 추가적인 유지관리 부담을 덜어주는 Enterprise Application Access 모델을 사용할 수 있습니다.

KKLab은 Akamai를 배치한 후 단순한 고객사 이상의 기업으로 성장했습니다. KKLab은 기업 고객 서비스 분야에서 풍부한 경험을 보유하고 있으며, 리포팅에 보다 세부적인 정보를 추가하는 등 고객들에게 유용한 여러 가지 사용 사례와 권장사항을 제공했습니다. 예를 들어 특정 기간 동안 트로이목마 또는 피싱과 같은 이벤트의 통계를 확인하는 것 외에도 이런 이벤트를 트리거한 사용자 및 디바이스를 파악하고자 했습니다. 또한 보고서에 텍스트와 숫자 외에도 원형 차트, 막대 그래프, 선 그래프 등의 데이터 시각화를 추가하는 것을 제안했습니다. Akamai는 이러한 제안에 신속하게 대응하면서 보고서를 조정했고 글로벌 사용자들에게 더 큰 혜택을 제공할 수 있었습니다.

현재 KKBOX 그룹은 Akamai의 제로 트러스트 솔루션을 통해 피싱 행동, 악성 광고, 악성 프로그램이 깔린 사이트로 사용자를 연결하려는 이메일을 매일 평균 100개씩 자동으로 차단합니다. KKLab은 모든 의심스러운 접속 행동을 쉽게 이해하고 피해가 발생하기 전에 문제를 예방할 수 있습니다. 또한 아키텍처 또는 사용자 행동의 문제를 검토하면서 KKBOX 그룹의 정보 보안을 지속적으로 개선할 수 있습니다. KKLab은 미래를 내다보면서 여러 기업들이 혜택을 얻을 수 있도록 제로 트러스트 여정 경험을 위한 모델을 구축하고 이를 그룹 외부의 기업들에게 서비스로 제공할 계획입니다.

iThome이 게시한 원본 문서, 2020 년 12월 7일.

KKLab Keke Experimental Co., Ltd.는 2019년에 설립되었습니다. 선구적인 기술을 개발하고, 산업 발전을 가속하며, 기업의 디지털 전환을 지원합니다. 또한 'AI 인공 지능 및 머신 러닝, 클라우드 플랫폼 구축 및 운영, 웹사이트 신뢰성 엔지니어링(SRE)' 및 기타 원스톱 서비스를 제공합니다. KKLab은 새로운 비즈니스 기회 개발을 지원하기 위해 혁신적인 서비스 및 IP 개발 가속화팀을 운영하고 있습니다. 현재 서비스 범위는 미디어, 엔터테인먼트, 통신, 의료, 가소화 등 다양한 업계에 걸쳐 있습니다. KKLab은 지속적으로 기술을 개선하고 업계 발전에 기여하고 있으며, 고객과 업계를 위해 더 많은 가치를 창출하기 위해 끊임없이 노력하고 있습니다. www.kklab.com

©2023 Akamai Technologies | 지원 | 2023년 1월 발행