Akamai 고객 사례

Fortune 100대 음료 리테일 기업, API 및 데이터 보안 강화

주요 API 취약점을 식별하고 이전의 사기, 도용, 도난으로 인한 피해를 복구해 고객 데이터 보호

API(Application Programming Interface)를 통해 리테일 기업은 운영을 간소화하면서 고객을 위한 엔드투엔드 개인 맞춤형 경험을 구축할 수 있습니다. 재고 데이터, 주문 제출, 위치 데이터, 결제, 리워드 프로그램 등 소비자에게 음료를 제공하는 모든 변수는 API를 통해 전달됩니다. API는 리테일 기업, 파트너, 고객으로 구성된 생태계를 연결해 쇼핑 경험에 혁신을 가져왔습니다. 하지만 민감한 데이터에 지속적으로 접근하기 때문에 리스크 요소도 존재합니다.

소비자들은 새로운 디지털 리테일 경험을 즐기면서도 자신의 개인정보가 얼마나 잘 보호되는지에 대해 우려하는 경우가 많습니다. API는 점점 더 사이버 범죄자들이 선호하는 공격 기법이 되고 있습니다. 이러한 이유로 Fortune 100대 리테일 음료 기업 중 한 곳은 API 보안 체계의 취약점을 해결하기 위해 Noname Security(현재 Akamai 자회사)를 찾았습니다.

API 사용 증가에 따른 도전 과제

초기 대화에서 이 회사는 글로벌 규모에서 의미 있는 API 거버넌스 및 보안을 달성하지 못하는 상황에 대해 우려를 표명했습니다. 증거를 수집하기 위해 공개적으로 문서화된 버그 현상금을 의뢰하고 약 1억 명 사용자의 이름, 주소, 이메일, 전화번호가 유출될 수 있는 큰 취약점을 발견했습니다. 다행히도 이 문제는 현상금 프로그램을 통해 아무런 피해 없이 해결되었습니다.

Retail Beverage Company

위치

미국

업계

리테일, 여행, 관광

솔루션

Akamai API Security

주요 효과

- 하루 10억 건 이상의 API 호출 보호
- 초당 5000건의 요청 보호
- 200개 이상의 문제 식별 및 해결

Akamai

또한 프로덕션 API 가시성 및 모니터링이 부적절해 리스크를 적절히 평가할 수 없었고, Apigee 데이터는 데이터 종류, 사용자 행동, 기준선, 취약점 포렌식 등 상황에 맞는 세부 정보를 제공하지 못했습니다. 이러한 API 취약점으로 인해 사기, 남용, 도난이 이어졌습니다. 그 결과 이 리테일 기업의 운영 비용은 커졌습니다.

API 보안 체계 강화

Noname API Security Platform(현재 Akamai API Security의 일부)은 고객의 API를 인벤토리화하고 행동 분석, 실시간 공격 탐지, 취약점 관리, API별 AppDev 테스트를 제공할 수 있었습니다. 그 결과 고객은 기존 컨트롤에서 놓쳤던 API 공격을 탐지하고 해결할 수 있었습니다. AppSec(Application Security) 팀은 효율성을 높이고 더욱 효율적으로 리스크가 높은 문제의 우선순위를 정할 수 있었습니다.

또한 Akamai는 운영 지연 시간 없이 엔진당 최대 5만 개의 API를 지원합니다. 이 고객은 Akamai 플랫폼을 중심으로 글로벌 API 보안 프로그램을 개발했습니다. 이제 맥락에 맞는 API 세부 정보를 통해 API 인벤토리에 대한 완벽한 가시성을 확보하고 있습니다. 또한 기존 툴로는 얻을 수 없었던 실행 가능한 인텔리전스를 확보했습니다. 이를 통해 효율적인 API 취약점 관리와 실시간 위협 탐지를 위한 비용 효율적인 기능을 사용할 수 있게 되었습니다.

©2024 Akamai Technologies | 지원 | | 2024년 8월 발행