Akamai 고객 사례

API와 리테일 운영을 안전하게 보호한 Fortune 500대 패션 선도 기업

편리하고 개인 맞춤형 리테일 경험을 제공하는 API를 보호하는 동시에 고객 데이터가 유출되지 않도록 보호한 기업

모든 API 발견 | 취약점 식별 | 보안 체계 강화

API는 리테일 업계가 기존의 오프라인 매장에서 이커머스 플랫폼으로 전환하는 과정에서 핵심적인 역할을 담당했습니다. 모든 디지털 상호 작용의 배후에는 API가 존재하며, 이를 통해 리테일 기업은 다음과 같은 일을 할 수 있습니다.

- 다양한 시스템, 애플리케이션, 서비스를 원활하게 연결합니다
- 온라인 스토어를 백엔드 재고 관리 시스템, 결제 게이트웨이, 배송 공급업체, 고객 관계 관리 툴과 통합합니다
- 신속한 데이터 교환을 촉진하여 온라인 리테일을 개인 맞춤화하고 편리하게 만듭니다

데이터 보호를 최우선 과제로 삼는 API 보안은 온라인 비즈니스 운영의 신뢰, 무결성, 기밀성을 보장하는 데 중요한 역할을 합니다.

API는 민감한 데이터에 지속적으로 근접해 있기 때문에 취약점을 악용하려는 사이버 범죄자에게 매력적인 표적이 됩니다. API 유출이 성공하면 개인 정보, 결제 카드 데이터, 구매 내역과 같은 고객 정보가 노출될 수 있습니다. 이전부터 Salt Security에 만족하지 못했던 Fortune 500대 패션 리테일 기업은 이러한 이유로 Noname Security(현재 Akamai가 인수한 기업)에 도움을 요청했습니다.

Fashion Retailer

위치
미국

업계
리테일

솔루션
Akamai API Security

Akamai

API 보안에 대한 프로그래밍 접근 방식 구축

해당 Fortune 500대 리테일 기업은 웹 애플리케이션 방화벽과 API 게이트웨이를 넘어 API 보안 리스크를 방어하는 완벽한 엔드투엔드 워크플로우를 구축하고자 했습니다. 이를 위해서는 API 거버넌스를 위한 강력한 제어 기능을 갖춘 견고한 API 보안 전략이 필요했습니다. 또한 궁극적으로 정상적인 사용자와 악성 봇을 구분해 시스템, 데이터, 사용자 경험을 보호하기 위해 봇 방어에 주력했습니다.

프로젝트의 규모를 고려해 해당 리테일 기업과 Akamai는 단계적 접근 방식에 동의했습니다. 1단계에서는 모든 API를 찾고, 민감한 데이터를 분류하고, 탐지 및 대응을 구축하고, Splunk와 통합하는 작업을 수행했습니다. 2단계는 보안 코드를 신속히 생성하기 위해 시프트 레프트 API 보안 테스트 접근 방식으로 전환하는 것이었습니다.

배포를 가속해 가치 실현 시간 단축

1단계가 까다로운 작업이었음에도 불구하고 Akamai 팀은 120일 만에 Noname의 API 검색 및 런타임 보호 모듈을 배포하는 동시에 Splunk 통합 작업을 실행할 수 있었습니다. API 검색은 API 확산을 관리하는 데 중요한 역할을 합니다. 여기에는 기업 내의 모든 API를 체계적으로 식별하고 카탈로그화하는 작업이 포함됩니다. 개발자는 중앙 집중식 API 리포지토리를 유지함으로써 새로운 개발 작업을 시작하기 전에 기존 API를 쉽게 검색하고 발견할 수 있습니다. 이를 통해 중복을 제거하고 재사용을 촉진해 시간과 노력을 절약할 수 있습니다.

Akamai는 자동화된 머신 러닝 기반 탐지 기능을 사용해 데이터 유출, 데이터 변조, 데이터 정책 위반, 의심스러운 행동, API 보안 공격 등 API 취약점을 탐지합니다. 해당 Fortune 500대 리테일 기업은 API의 보안과 무결성을 크게 개선하고, 민감한 데이터를 보호하고, 사용자와 파트너의 신뢰를 유지할 수 있습니다.