AKAMAI 제품 설명서

Brand Protector

피싱 사이트, 가짜 스토어, 브랜드 사칭을 탐지하고 방해해 최종 사용자의 피해와 비즈니스 손실을 예방하는 솔루션!

보안팀은 오랫동안 성을 보호하는 데 주력하며 악의적이고 은밀한 공격으로부터 기업의 디지털 자산을 보호하고 있습니다. 그러나 모든 공격이 기업의 정문을 노리는 것은 아닙니다. 공격자는 웹 전반에서 글로벌 브랜드와 고객의 오랜 관계를 활용해 디지털 유사 제품으로 브랜드를 사칭하고 귀중한 인증정보를 넘기거나 직접 결제하도록 유인합니다.

따라서 기업의 가장 소중한 자산인 평판을 자체 디지털 도메인 외부에서도 보호하는 것이 어려운 과제로 떠올랐습니다. Akamai Brand Protector는 수요와 수익성을 떨어뜨리는 가짜 상품에 대응하고 고객의 민감한 데이터와 계정 정보를 보호함으로써 매출 하락과 리스크 증가로부터 기업을 보호합니다.

Akamai Brand Protector는 가짜 웹사이트, 피싱, 사칭, 상표 불법 복제 등 표적 공격을 탐지하고 방어하는 솔루션입니다.

인지도 높은 브랜드는 기업 안팎에서 측정 가능한 가치를 창출합니다. 브랜드 가치가 높아지면 고객 이탈이 줄어들고 구매 전환율 및 파이프라인이 증가합니다. 브랜드의 영향력이 커지면 내부 보상도 높아져 직원 이직률 및 고용 비용이 감소합니다.

Brand Protector는 인텔리전스, 탐지, 가시성, 방어라는 4단계 접근 방식을 통해 사칭 문제를 간단하고 효율적으로 해결하도록 설계되었습니다.

인텔리전스

피싱 및 기타 브랜드 사칭 웹사이트를 탐지해야 하는 도전 과제는 인텔리전스 및 데이터 수집 단계에서 시작됩니다.

Brand Protector는 세계 최대의 엣지 플랫폼인 Akamai Intelligent Edge Platform을 기반으로 합니다. 이 플랫폼은 인터넷 전반에 걸쳐 독점적인 가시성을 확보하고 있고 전 세계 트래픽의 약 30%를 차지하며 매일 300TB가 넘는 데이터를 분석합니다. 이런 세밀한 인텔리전스는 써드파티의 데이터 피드로 한층 강화되어 공격자의 활동을 종합적으로 파악할 수 있습니다.

Brand Protector는 Akamai만의 독보적인 입지와 독점적인 보안 데이터 로그를 사용해 다른 시장 솔루션보다 빠르고 효율적으로 사기 웹사이트를 탐지하는 인텔리전스를 수집합니다.

기업이 누릴 수 있는 혜택

신뢰할 수 있는 공격 탐지
Akamai의 글로벌 네트워크와 추가 피드는 브랜드 사칭을 탐지하는 장점을 제공합니다.

고객별 가시성
브랜드, 제품, 조건에 맞는 전용 인텔리전스 컬렉션을 제공합니다.

정확성 및 속도
알고리즘의 빠른 탐지 기능이 오탐률을 최소화하면서 첫번째 방문 시 알림을 전달합니다.

유용한 인사이트
리스크 점수를 산정해 포괄적인 데이터를 유용한 인사이트로 제공하고 심각도와 도달 범위를 한 눈에 볼 수 있게 요약합니다.

사용 편의성
실시간 인사이트를 확보하고 증가하는 공격 기법에 대한 문제 해결을 몇 분 안에 시작할 수 있습니다.

통합 차단
자체 차단 서비스 또는 Brand Protector 포털 내의 통합된 차단 서비스를 활용해 생산성을 유지합니다.

Akamai

탐지

매주 5만여 개의 피싱 웹사이트가 새로 생성됩니다. Akamai Brand Protector는 내부 및 외부 소스에서 매일 수십억 건의 디지털 활동을 조사해 공격 캠페인이 시작되기 전에 기업 브랜드와 브랜드 구성요소의 악용 사례를 발견합니다.

가시성

다양한 소스에서 인텔리전스를 수신하면 데이터 신호가 일련의 휴리스틱 및 AI 탐지기를 통해 실행됩니다. 대량의 데이터와 증거가 수집되지만, Akamai의 간소화된 사용자 인터페이스를 통해 고객에 대한 실시간 사칭 위협을 한 눈에 파악할 수 있습니다.

고객별 트래픽, 탐지, 위협 데이터는 Akamai 고객 포털 내에서 유용한 인사이트로 축약되고 위협 점수, 신뢰 점수, 심각도 등급을 제공하며, 탐지별로 영향을 받는 사용자 수를 정량화합니다. 알림 증거가 구성되며, 스크린샷, 탐지 지표, 도메인 세부 정보를 제공합니다.

방어

통합 차단 서비스는 브랜드 사기를 예방하는 역할을 합니다. 이 단계에서는 수집된 증거를 사용해 방어 조치를 요청할 수 있는 자동 옵션이 사용자에게 제공됩니다. 사용자는 포털에서 상태를 보고 추적할 수 있습니다.

 | 지원 | 2023년 1월 발행