

Brand Protector 제품 설명서

피싱 사이트, 가짜 스토어, 브랜드 사칭을 탐지하고 차단해 고객 피해를 막고 대규모 사기 및 남용 공격의 리스크를 줄이세요.

인지도 높은 브랜드는 기업 안팎에서 측정 가능한 가치를 창출합니다. 기업은 브랜드 구성요소를 보호해 손실, 생산성 저하, 부정적인 고객 후기를 최소화하면서 고객 충성도를 유지하고 더 높일 수 있습니다. 보안 관점에서 브랜드 사칭 관리는 킬 체인을 차단해 인증정보 수집 및 계정 도용을 방지하는 역할을 합니다.

모든 공격이 기업의 정문으로 들어오는 것은 아닙니다. 공격자는 웹 전반에서 디지털 유사 브랜드를 사칭해 고객의 민감한 데이터, 인증정보, 직접 결제 내역을 훔칩니다. 브랜드 사칭 및 피싱 캠페인은 점점 더 어려운 도전 과제가 되고 있습니다. 반복적으로 멈췄다 다시 활동하고 위치를 변경해 탐지 및 방어에 많은 리소스가 소비되게 만드는 수명이 짧은 캠페인 기법 때문입니다.

Akamai Brand Protector는 퍼스트 파티 및 써드 파티 데이터 피드 모두를 결합한 최대 규모의 위협 인텔리전스 데이터베이스 중 하나를 활용해 탐지 속도를 높이고 정확도를 개선합니다. Brand Protector의 통합 방어 기능은 사기 및 남용 공격을 조기에 방어하는 데 효과적이고 필수적인 툴입니다.

Akamai Brand Protector는 사이트, 소셜 미디어, 앱 마켓플레이스 전반에서 피싱, 사칭, 브랜드 도용 등의 표적 공격을 탐지하고 방어합니다. 특히 Brand Protector를 사용하면 신뢰 관계를 보호할 수 있습니다.

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

Brand Protector는 인텔리전스, 탐지, 가시성, 방어라는 4단계 접근 방식을 통해 사기성 사칭 문제를 해결합니다.

기업이 누릴 수 있는 이점

-  **신뢰할 수 있는 공격 탐지**
독점적인 글로벌 네트워크와 추가 피드는 브랜드 사칭을 탐지하는 데 있어 독보적인 이점을 제공합니다.
-  **정확성 및 속도**
신속한 알고리즘 탐지를 통해 공격 캠페인이 시작되기 전에 알리를 전달하고 오탐률을 최소화할 수 있습니다.
-  **유용한 인사이트**
공격의 심각도와 범위를 한눈에 파악할 수 있는 리스크 점수 책정을 통해 포괄적인 데이터를 유용한 정보로 제공합니다.
-  **고객별 가시성**
웹사이트, 소셜 미디어, 앱 마켓플레이스 전반에서 브랜드, 제품, 관련 구성요소에 대한 전용 인텔리전스를 수집합니다.
-  **사용 편의성**
실시간으로 인사이트를 확보하고 증가하는 공격 기법에 대한 문제 해결을 몇 분 안에 시작할 수 있습니다.
-  **차단 및 방어**
생산성을 유지하려면 Brand Protector 내의 통합 차단 서비스를 활용하거나, 브라우저 알림을 통해 트래픽을 차단하세요.

인텔리전스

피싱 및 브랜드 사칭 공격 탐지와 관련된 도전 과제는 인텔리전스 및 데이터 수집 단계에서 시작됩니다.

Akamai가 구축한 최대 규모의 글로벌 엣지 및 클라우드 플랫폼은 전 세계 웹 트래픽에 대한 독점적인 뷰를 통해 매일 788TB 이상의 데이터를 분석합니다. Brand Protector의 인텔리전스는 써드파티 데이터 피드로 한층 강화되어 공격자의 활동을 종합적으로 파악할 수 있습니다. 또한, Brand Protector 탐지 클라우드에서 분석할 URL과 도메인을 직접 추가할 수 있습니다.

탐지

Brand Protector의 탐지 성능과 속도는 Akamai의 독자적인 인텔리전스 피드와 분석 알고리즘을 결합해 탐지 신뢰도를 높이고 오탐률은 낮춥니다.

브랜드 공격은 악의적이고 수명이 짧은 웹사이트를 자동화합니다. 대부분의 기술은 이러한 공격 자산이 고객에게 영향을 미치기 전에 탐지하고 방어할 수 있을 만큼 빠르지 않습니다. Akamai의 접근 방식은 새로 고친 목록이나 지연된 피드에 의존하지 않고 실시간 트래픽을 추적해 브랜드 남용을 탐지한다는 점에서 다릅니다. Brand Protector를 사용하면 캠페인이 고객에게 도달하기 전인 첫 번째 HTTP/HTTPS 요청이 발생할 때 보안팀에서 피싱 사이트를 탐지할 수 있습니다.

가시성

보안팀은 고객 중심의 엔지니어링 및 설계를 통해 단일 대시보드 보기에서 광범위한 보안 인사이트를 얻을 수 있습니다.

인텔리전스를 수신한 후 데이터 신호는 일련의 휴리스틱 및 인공 지능 탐지기를 통해 실행됩니다. 압도적인 양의 데이터와 증거가 수집되지만, Akamai의 간소화된 사용자 인터페이스는 사칭을 통해 고객에게 가해지는 활성 위협을 즉각적으로 파악하도록 지원합니다.

고객별 트래픽, 탐지, 위협 데이터는 선별되어 Akamai 고객 포털 내에서 유용한 인사이트로 제공됩니다. 분석 결과는 요약된 위협 점수에 따라 순위가 매겨집니다. 알림을 클릭하면 신뢰 점수, 심각도 등급, 영향을 받는 사용자 수, 공격 이벤트 일정 등의 위협 분석 데이터를 확인할 수 있습니다.

탐지된 사항마다 증거가 뒷받침됩니다. 단일 탐지 화면에서 코드, 스크린샷, 탐지 지표, 도메인 세부 정보를 볼 수 있습니다.

방어

통합 차단 서비스는 브랜드 사기를 예방하는 역할을 합니다.

보안팀은 Brand Protector를 통해 탐지 화면에서 바로 악성 사이트에 대한 차단 실행을 요청할 수 있습니다. Akamai 써드파티 파트너에게 전송되는 Brand Protector에 대한 차단 요청은 사용 편의성을 위해 탐지 증거와 추가 세부 정보를 자동으로 첨부합니다. 포털에서 방어 상태를 추적하고 확인할 수 있습니다.

브랜드에 맞게 구축

구역 보호

Brand Protector는 Akamai 엣지 보안 포트폴리오의 일부로서 보안팀의 시야를 초기 킬 체인 보호로 확장할 수 있습니다. 고객이 피싱 피해자가 되는 데 사용될 수 있는 브랜드 도메인의 순열을 선제적으로 검색합니다.

소셜 미디어 모니터링

소셜 미디어에서 브랜드 사칭이 증가함에 따라 새롭게 강화된 소셜 미디어 모니터링 기능은 온라인 사기를 탐지하고 무력화해 다양한 플랫폼에서 브랜드와 고객을 보호합니다.

악성 앱 탐지

앱 마켓플레이스 모니터링은 공식 및 비공식 앱 저장소를 스캔해 브랜드 아이덴티티를 오용하는 사기성 애플리케이션을 탐지하는 새로운 기능으로 디지털 환경 전반에서 포괄적인 방어 기능을 제공합니다.

