AKAMAI 제품 설명서

# Content Protector

**갈수록 정교해지는 스크레이퍼 공격으로부터 매출을 보호하세요**

콘텐츠 스크레이핑으로 공격자는 돈을 벌고 기업은 손실을 입습니다. 콘텐츠를 공개적으로 공유하는 것은 전략적 선택이지만, 소비자의 참여와 유해한 스크레이핑 활동을 구분하는 것이 중요합니다. 경쟁업체와 공격자는 스크레이핑된 데이터를 악용해 기업의 가격 전략을 방해하고 고객에게 피해를 줄 수 있습니다. Akamai Content Protector는 스크레이퍼 공격의 고유한 툴링과 기법에 적합한 탐지 기능을 사용해 스크레이퍼를 즉시 탐지하고 중단시킵니다. 속도 혹은 성능 저하 없이 비즈니스와 매출을 보호하세요.

스크레이핑 공격은 온라인 비즈니스의 지속적인 도전 과제입니다. 스크레이퍼는 시작과 끝이 분명한 일반적인 사이버 위협과 달리 사이트에 지속적으로 접속할 수 있기 때문에, 이를 해결하지 못할 경우 다음과 같은 심각한 결과로 이어질 수 있습니다.

- **웹사이트 성능 저하:** 지속적인 스크레이핑 활동으로 인해 사이트 속도가 느려져 사용자 불만이 증가하고 전환율이 감소할 수 있습니다.
- **경쟁력 약화:** 경쟁업체는 스크레이핑을 통해 대상 기업의 가격을 모니터링하고 그보다 가격을 낮춰 매출에 영향을 줄 수 있습니다.
- **브랜드 평판 리스크:** 위조업체는 스크레이핑된 콘텐츠를 오용해 기업의 브랜드명으로 위조 제품을 판매할 수 있습니다.

스크레이퍼는 이미 수년간 존재해 왔습니다. 그런데 최근 들어 상황이 악화된 이유는 무엇일까요? 최근 스크레이퍼를 보다 빨리 퇴치해야 할 필요성이 커졌습니다. 2020년에 시작된 팬데믹과 이에 따른 공급망 붕괴로 인해 스크레이핑을 통해 얻을 수 있는 금전적 효과가 커졌습니다. 일상적인 필수품부터 고급 상품 및 여행 서비스까지, 수요가 높은 품목이 정교한 스크레이핑 공격의 주요 표적이 되었습니다.

잠재적인 수익이 늘어나면서 봇 운영자들은 툴링(원격 측정)을 전문적으로 다루고 이를 다른 봇 운영자들이 만든 툴과 연계해, 스크레이핑 공격에 특화된 고도로 전문화된 봇을 제작하며 혁신에 뛰어들기 시작했습니다. 이로 인해 스크레이퍼가 더 위험해지고 탐지하기는 더 어려워졌습니다. 설상가상으로 스크레이핑은 플러그인과 같은 다른 방법을 통해서도 발생할 수 있기 때문에 스크레이퍼를 막으려면 봇 관리 이상의 조치가 필요합니다.

하지만 모든 스크레이퍼를 차단할 수는 없습니다. 검색 봇은 공개 검색에 표시할 새로운 콘텐츠를 찾고, 일부 소비자 쇼핑 봇은 비교 사이트에서 기업의 제품을 강조 표시하며, 파트너는 최신 제품 정보를 효율적으로 수집해 고객과 공유할 수 있습니다.

## 기업이 누릴 수 있는 혜택

**전환율 증가**
사이트와 앱의 속도를 떨어뜨리는 봇을 제거해 더 많은 고객 유치 및 매출 증대

**비용 절감**
봇 트래픽에 지출되는 비용 제거

**스캘퍼 차단**
스크레이퍼가 인기 있는 제품의 재고가 입고되는 시점을 파악하기 위해 기업의 사이트를 핑하는 것을 방지함으로써 봇 운영자가 인벤토리 사재기 공격 체인의 다음 단계로 나아가지 못하도록 차단

**경쟁업체 견제**
경쟁업체가 기업의 가격을 낮추고 매출을 감소시키는 데 일조하는 자동화된 스크레이핑 차단

**불법 복제 방어**
불법 복제 업체가 콘텐츠를 수집해 전달받을 목적으로 이용하는 무자비한 스크레이핑 차단

**마케팅 효과 개선**
사이트 애널리틱스에서 봇 트래픽을 제거해 실제 사용자에 맞게 최적화

Akamai

Akamai Content Protector는 스크레이퍼를 탐지하고 차단하도록 설계된 탐지 기능을 갖추고 있습니다. Akamai 네트워크의 가시성, 봇 관리 분야의 글로벌 강점, 최첨단 탐지 기능의 지속적인 개발을 적극 활용합니다. Content Protector는 위협의 변화에 따라 보안을 업데이트하고 위협 인텔리전스 연구원 및 데이터 과학자의 인사이트를 자동으로 통합함으로써 스크레이퍼에 대한 맞춤형 탐지 기술을 지속적으로 선도합니다.

스크레이퍼를 차단하면 사이트 성능 및 전환율을 개선하고 경쟁업체의 영향을 줄이는 등 기업의 디지털 입지를 최대한 활용하는 데 집중할 수 있습니다.

## 핵심 기능

- **탐지:** 클라이언트측 및 서버측에서 수집된 데이터를 평가하는 ML 기반의 탐지 방법.
  - » **프로토콜 수준 평가:** 프로토콜 핑거프린팅은 클라이언트가 다음 OSI 모델의 다른 계층에서 서버와의 연결을 설정하는 방법을 평가합니다. TCP, TLS, HTTP - 협상된 매개 변수가 가장 일반적인 웹 브라우저 및 모바일 애플리케이션에서 예상되는 매개 변수와 일치하는지 확인합니다.
  - » **애플리케이션 수준 평가:** 클라이언트가 자바스크립트로 작성된 비즈니스 로직을 실행할 수 있는지 평가합니다. 클라이언트가 자바스크립트를 실행하면 Content Protector가 디바이스 및 브라우저의 특성과 사용자 기본 설정(핑거프린트)을 수집합니다. 이러한 다양한 데이터 포인트를 프로토콜 수준 데이터와 비교하고 교차 점검해 일관성을 확인합니다.
  - » **사용자 상호 작용:** 행동 지표는 터치스크린, 키보드, 마우스 같은 표준 주변기기를 통해 클라이언트와 인간의 상호작용을 평가합니다. 상호 작용이 부족하거나 비정상적일 경우 일반적으로 봇 트래픽과 관련이 있습니다.
  - » **사용자 행동:** 웹사이트에서 사용자의 여정을 분석합니다. 봇넷은 일반적으로 특정 콘텐츠를 노리기 때문에 정상적인 트래픽과 상당히 다른 행동을 보입니다.
  - » **헤드리스 브라우저 탐지:** 클라이언트 측에서 실행되는 자바스크립트로, 스텔스 모드에서 실행 중일 때도 헤드리스 브라우저에 의해 남겨진 지표를 찾습니다.
- **리스크 분류:** 평가 중에 발견된 비정상을 기반으로 트래픽을 저, 중, 고 리스크로 분류해 결정적이고 실행 가능한 정보를 제공합니다.
- **대응 방법:** 간단하게 모니터링 및 차단할 수도 있고, 서버 중단 또는 여러 다양한 종류의 챌린지 액션을 활용하는 타피트(Tarpit) 같은 보다 세밀한 방법을 사용할 수 있습니다. 크립토 챌린지는 오탐률 측면에서 CAPTCHA 챌린지보다 일반적으로 사용자 친화적입니다.

### Content Protector를 뒷받침하는 Akamai 생태계

Akamai는 빠르고 안전하며 스마트한 인터넷 환경을 제공합니다. Akamai가 제공하는 포괄적인 솔루션은 전 세계적으로 촘촘하게 구축된 Akamai Connected Cloud를 기반으로 설계되었습니다. 모든 솔루션은 Akamai 통합 포털인 Akamai Control Center를 통해 고객사별로 탁월한 가시성과 관리 역량을 제공합니다. Akamai의 Professional Services는 고객사가 전략적 변화에 맞추어 혁신을 주도해 나갈 수 있도록 지원합니다.

## 데모를 신청하거나 Akamai 영업 팀에 문의하세요.