AKAMAI 제품 설명서

Bot Manager

"누구를 신뢰할 것인가"만큼 중요한 질문은 "누가 나를 신뢰하는가" 입니다. 온라인 트랜젝션의 반대편에 있는 소비자, 파트너, 봇이 말하는 것을 신뢰할 수 있어야 합니다. 봇은 사이트 트래픽의 최대 70%를 차지하는데 안타깝게도 봇은 정상 사용자인 척 가장해 지적 재산을 훔치고 운영을 방해합니다. Akamai Bot Manager는 봇에 대한 가시성과 제어를 제공해 비즈니스를 보호하고 온라인 관계의 신뢰를 지킬 수 있도록 지원합니다.

소비자, 파트너, 공급업체, 써드파티와의 상호작용을 자동화하고 온라인 효율성을 높이기 위해 정상 봇을 사용하는 기업들이 점차 증가하고 있습니다. 이러한 봇이 사이트 성능과 고객 경험에 미치는 영향을 반드시 관리해야 합니다.

공격자들과 범죄자들이 자동화하는 것도 증가하고 있는데 다음과 같은 목적을 위해 봇넷을 확장하고 있습니다.

- 고객이 구매하기 전에 재고 확보
- 크리덴셜 스터핑 공격 개시
- 로열티 포인트 및 기프트 카드 탈취
- 비즈니스 로직의 취약점 악용
- 비즈니스 공격으로 사이트 속도 저하 및 비용 증가

봇 운영자가 기업과 고객을 악용하기 위해 최선을 다하고 있는 상황에서 온라인 상호작용에 대한 신뢰를 유지할 수 있는 방법은 무엇일까요? 또한 다른 사람들에게 신뢰성을 어떻게 보여줄 수 있을까요?

Bot Manager는 탁월한 탐지 및 방어 기능을 통해 자동화된 작업을 더욱 효과적이고 안전하게 실행할 수 있게 해주며 사용자 및 전체 생태계에 대한 신뢰를 제고합니다.

Akamai와 함께 시작하는 신뢰할 수 있는 봇 관리

Akamai는 글로벌 기술 역량을 보유한 신뢰할 수 있는 기업입니다. 전 세계 500대 기업 중 50% 이상을 위해 서비스를 지원하고 131개 이상의 국가에 4167여 개의 네트워크 거점(PoP)을 보유하고 있으며 연 매출이 36억 달러를 넘습니다. 이 모든 강점을 Bot Manager에 담았습니다. 혁신을 거듭해 시간이 지나도 성능이 저하되지 않고 봇 트렌드 및 회피 기법보다 앞서 나갑니다.

기업이 누릴 수 있는 혜택

신뢰 강화: 자사와 파트너 및 고객
어떤 상호 작용이 정상인지 파악하고, 사용자 불편을 줄이고, 사기 활동로부터 사용자를 보호함으로써 소비자, 파트너, 기업의 신뢰를 높일 수 있습니다.

문제 해결의 부담 경감
감염된 계정 확인, 도난된 계정 교체, 사용자 불만 해결, 기타 봇 공격 여파로 인한 경제적 및 리소스 관련 부담이 줄어듭니다.

운영 개선
효율성을 높이고, 비즈니스 및 재정적 리스크를 줄이고, IT 지출을 관리하고, 파트너 봇을 전략적으로 관리할 수 있습니다.

데이터를 기반으로 보다 현명한 의사 결정
상세한 애널리틱스 및 리포팅 기능을 활용해 고객 여정, 보안 체계, 리스크 허용 범위, IT 운영에 대한 창의적이고 효과적인 의사 결정을 내릴 수 있습니다.

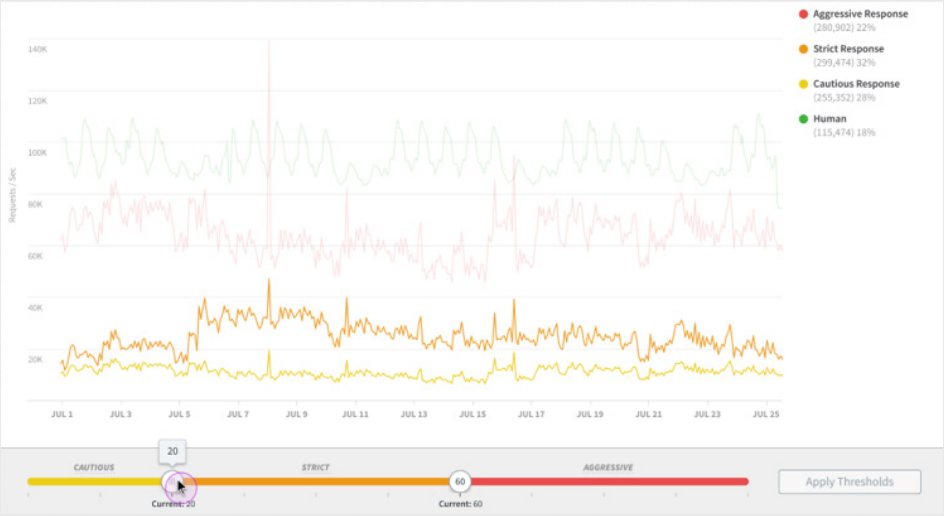
 | 지원 | | 2023 년 10 월 발행

Bot Manager는 특허받은 여러 가지 기술을 사용해 봇과 처음 접촉하는 지점에서 봇을 탐지하고 방어하며 봇이 사이트에 먼저 접속하도록 허용하지 않습니다. 또한 위협 변화에 맞춰 지속적으로 보안 상태를 업데이트합니다. Akamai 위협 인텔리전스 연구원들의 인사이트는 Bot Manager의 탐지 및 분석에 자동으로 통합됩니다. 따라서 특별한 업그레이드나 개선을 요청할 필요가 없습니다.

Bot Manager는 웹, 네이티브 모바일 앱, API를 통한 엔드포인트를 비롯해 상호 작용이 발생하는 모든 곳에서 기업을 보호합니다. 요청이 한 도메인에서 다른 도메인으로 넘어가는 경우에도 사용자를 보호합니다. 여러 브랜드 또는 비즈니스를 운영하는 경우에도 Bot Manager가 상호 작용 전반에 걸쳐 최초의 요청을 따르기 때문에 보안에 틈이 발생하지 않습니다.

Bot Manager AI 프레임워크

Bot Manager는 Akamai Connected Cloud에서 인라인으로 작동하는 AI(Artificial Intelligence) 프레임워크에서 시작됩니다. Bot Manager는 트래픽 패턴, 트래픽 종류, 트래픽 규모에 대한 정확한 정보를 제공하며 사용자가 애플리케이션에 처음 연결되는 엣지에서 트래픽을 확인할 수 있습니다. Akamai는 네트워크 전반에서 매일 평균 370억 건의 봇 요청을 모니터링하고 있습니다.



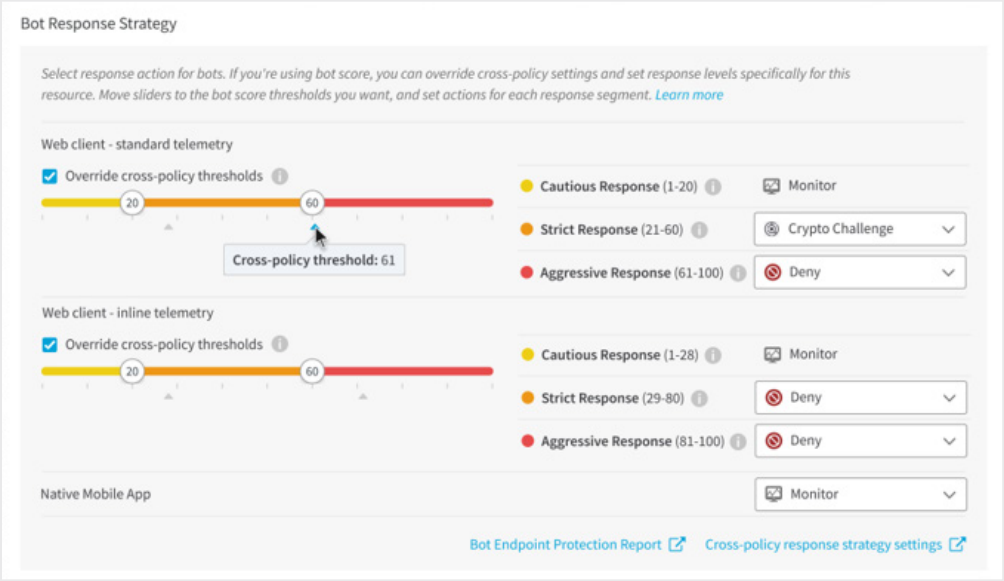
AI, 머신 러닝, 위협 인텔리전스

다양한 종류의 '정상 트래픽' 데이터를 대규모로 수집하면 ML(Machine Learning) 알고리즘의 정확도를 더욱 높일 수 있습니다. Akamai 네트워크는 매일 13억 대의 디바이스에서 발생하는 트래픽을 관측하고 최대 트래픽은 164Tbps를 기록했습니다. 이런 데이터 가시성을 기반으로 알고리즘은 더 빨리 더 많이 학습할 수 있습니다. Akamai 팀은 400여 명의 위협 연구원으로 구성되어 있고 공격 패턴, 기술 혁신, 새로운 회피 기법 등 트렌드를 지속적으로 추적하고 탐지 역량을 강화합니다. Akamai 위협 연구원들은 매일 662TB의 새로운 공격 데이터를 분석하고 있으며, 이는 2021년의 290TB보다 증가한 수치입니다.

Akamai의 강력한 AI 및 ML 기술과 함께 고객별 모델을 위한 기능을 제공합니다. 이러한 딥 러닝 모델은 대규모 브랜드 웹사이트를 표적으로 한 가장 정교한 공격을 연구합니다. 그런 다음 학습한 내용을 고급 알고리즘에 적용해 다른 방법으로는 며칠 또는 몇 주가 걸리는 새로운 공격에 대한 방어를 단 몇 분 만에 구축합니다.

봇 점수 - 탐지된 모든 봇 평가

봇 점수는 모든 탐지 트리거를 종합적으로 연결하고 정교한 봇을 탐지해 각 요청에 대해 더 정확한 평가를 제공합니다. 따라서 추가 지연 시간 발생 없이 시스템의 전체 탐지 효과가 최적화됩니다. 아울러 봇 점수는 점수 범위에 따라 대응 전략을 정의할 수 있도록 지원합니다.



혁신적인 챌린지

Bot Manager의 봇 점수 기능을 최첨단 챌린지와 결합하면 미리 정의된 임계값과 대응 작업을 통해 자동으로 조치할 수 있습니다. 사람에게는 보이지 않는 Akamai의 챌린지를 사용해 정상 사용자와 봇을 구별하는 수고를 덜 수 있습니다. 크립토 챌린지는 푸는데 최소한의 시간이 걸리는 암호화 퍼즐에서 봇이 CPU 사이클을 소비하도록 만듭니다. 이를 통해 정교한 봇 공격의 크롤링 속도를 늦추고 공격자의 비용을 증가하게 만듭니다. 틈새형 챌린지는 고객이 쿠키 저장 및 자바스크립트 실행을 지원한다는 것을 증명하도록 요구합니다. 그렇지 않은 경우 Bot Manager가 시간 페널티를 적용하고 고객이 선택한 방어 조치를 실행합니다.

네트워크에 영향을 주는 공격 방어

Akamai는 세계에서 가장 규모가 크고 잘 알려진 기업들을 보호합니다. 이러한 기업들은 자주 최첨단 봇 운영자의 표적이 됩니다. 한 고객에서 새로운 봇이 탐지되면 해당 봇에 대한 데이터가 알려진 봇 라이브러리와 모든 고객을 위한 고유한 "캐터펄트 알고리즘"에 몇 분 내에 추가됩니다. 이런 네트워크 효과는 고객이 봇을 효과적으로 관리할 수 있도록 하고 특정 봇이 다른 사람들을 공격하지 못하도록 사전에 차단하는 역할을 합니다.

빠르고 간편한 배포

Bot Manager의 인라인 아키텍처를 통해 빠르고 원활하게 배포할 수 있습니다. 솔루션을 활성화한 순간부터 지연 시간 없이 실시간으로 봇을 탐지하며, 사이트 또는 네트워크 성능에 영향을 미치지 않습니다. Bot Manager는 Akamai 네트워크의 막대한 용량을 활용해 고객의 성장에 맞춰 확장할 수 있습니다. Akamai 네트워크의 트래픽은 매일 100Tbps를 상회하며 2022년 12월 14일에는 역대 최고치인 261.21Tbps를 기록했습니다.

핵심 기능

알려진 봇 디렉터리 — Bot Manager는 알려진 봇에 자동으로 대응하며 1750개의 알려진 봇으로 구성된 디렉터리를 지속적으로 업데이트합니다.

정교한 동적 봇 탐지 — Bot Manager는 다양한 AI, 머신 러닝 모델, 기술을 사용해 첫 번째 상호작용에서 알려지지 않은 봇을 정확하게 탐지합니다. 여기에는 행동 분석, 브라우저 핑거프린팅(Fingerprinting), 자동 브라우저 탐지, 비정상 HTTP 탐지, 높은 요청률 등이 포함됩니다. Bot Manager의 동적 코드 및 텔레메트리 난독화는 리버스 엔지니어링을 방어해 시간이 지나도 Bot Manager의 효과를 유지합니다.

점수 모델 — 봇 점수 모델은 Bot Manager Premier에서 탐지하는 모든 요청을 평가합니다. 그리고 해당 요청이 봇에서 보낸 요청일 확률을 계산해 0점(확실히 사람)에서 100점(확실히 봇) 사이의 점수를 매깁니다.

브라우저 사칭 탐지 - 봇 운영자는 탐지를 피하기 위해 종종 특정 브라우저를 사칭하려 합니다. Akamai의 브라우저 사칭 탐지 기능은 정기적인 튜닝 없이도 매우 정확하게 작동하도록 개발되었기 때문에 다른 탐지 방법보다 오탐률이 낮습니다.

엔드포인트 당 사용자 지정 설정 — 봇 점수 기능을 활용하면 각 엔드포인트에 맞춰 적절하게 전략적으로 대응할 수 있습니다. 예를 들어 검색 페이지에는 35점 이하의 봇에 주의(주시/모니터링) 대응을 적용하면서 로그인 페이지에 도달하는 요청에는 임계값을 20까지 낮출 수 있습니다.

대응 조정 시뮬레이터 — 기업의 리스크 허용 범위와 엔드포인트에 따라 전략적 대응을 미세조정할 수 있습니다. 봇 점수 기능을 활용해 미세조정 사항을 실제로 적용하기 전에 시뮬레이션하고 과거 트래픽에 기반해 임계값 변경이 어떤 영향을 주는지 시각화할 수 있습니다.

자동 조정 — 봇의 변화에 맞춰 대응하기 때문에 사람이 직접 개입해 미세조정할 필요가 줄어듭니다. Bot Manager는 사이트의 정상 트래픽 패턴을 학습하고 고유한 패턴에 따라 탐지를 자동으로 조정해 요청이 잘못 분류되는 일을 방지합니다.

섬세한 대응 조치 — 대체 콘텐츠 제공, 챌린지 서비스, 속도 저하 등 '차단 및 허용' 이외의 다양한 조치를 통해 봇 방어를 강화합니다.

세분화된 리포팅 및 분석 — Bot Manager의 실시간 히스토리 리포팅 기능을 통해 신뢰할 수 있는 데이터를 기반으로 의사 결정을 내릴 수 있습니다. 개별 봇이나 기타 봇 트래픽 세그먼트에 대한 전반적인 트렌드와 상세 분석 정보에 대한 가시성을 확보할 수 있습니다. 또한 봇 트래픽을 동종 업계 내의 다른 기업 및 모든 Akamai 고객들과 비교할 수 있습니다.

Managed Security Service(옵션) — 내부팀에 부담을 주지 않으면서 Bot Manager를 최적화합니다. Akamai 전담 전문가가 선제적 권장 사항을 모니터링 및 제공할 뿐만 아니라 발견된 보안 이벤트를 긴급 지원합니다.

리스크 인식 봇 관리

- **봇 대응을 기업의 리스크 허용 범위에 맞춰 기업의 목표 지원**
- **장기적인 목표와 개별 이벤트(예: 반짝 세일)에 맞게 점수 임계값 수정**
- **엔드포인트에 따른 전략적 대응 매칭(예: 고가치 엔드포인트에서는 낮은 리스크 점수에도 적극적인 조치 적용)**

자세한 내용을 알아보려면 Akamai 담당자에게 문의하시거나 Akamai.com에 방문하시기 바랍니다.