



성공적인 봇 관리를 위한 10가지 고려 사항

e-Book



목차

서론	03
1. 정교한 전문성	04
2. 인텔리전스	05
3. 안정적인 보호	06
4. 오탐률 및 미탐률	07
5. 유연한 조치	08
6. 배포	09
7. 가시성 및 보고	10
8. API 보호	11
9. 사이트 vs 페이지	12
10. 매니지드 서비스	13

서론

봇 문제가 얼마나 까다로워졌는지 궁금하지 않으신가요? 테일러 스위프트(Taylor Swift) 티켓이나 신상 에어 조던 한 켄레를 구매해 보세요. 이는 단지 잘 알려진 이벤트들일 뿐입니다. 봇은 업계 전반에 점점 더 널리 퍼지고 있으며 그 폐해가 심각해지고 있습니다.

더 큰 문제는 봇 관리 환경이 달라지고 있다는 점입니다. 실제로 봇 관리 환경은 항상 변화해 왔습니다. 봇 관리는 종종 군비 경쟁 또는 고양이와 쥐의 게임에 비유됩니다. 기업이 방어 체계를 구축하면 봇 제작자가 이를 우회하는 방법을 지속적으로 찾아냅니다. 하지만 지금은 봇만 진화하고 있지 않습니다. 봇을 둘러싼 환경도 진화하고 있습니다. 예를 들어 기업은 더 이상 개별 행위자나 기업화된 그룹만 상대하지 않습니다. 이제 Airbnb처럼 봇을 일주일 단위로 대여하는 것이 가능해졌습니다. 마찬가지로 솔루션은 봇을 단순히 정상 봇과 악성 봇으로 구분할 수 없습니다. 지금은 애매모호한 영역이 너무 많습니다.

봇과 봇을 둘러싼 환경이 이렇게 진화하면서 봇 관리 소프트웨어를 선택하기가 그 어느 때보다 어려워졌습니다. 이제 과거의 봇에 효과적이었을 뿐만 아니라 현재와 미래의 봇에도 효과적인 것이 무엇인지 판단해야 합니다.

이 가이드는 봇 관리 소프트웨어를 선택할 때 구매자가 고려해야 할 몇 가지 주요 사항을 간략하게 설명합니다. 가이드의 정보를 활용해 현명한 구매 결정에 도움을 얻으시기 바랍니다.

1 정교한 전문성

봇 관리 솔루션은 기본적으로 봇을 탐지합니다. 즉, 요청자가 사람이 아니라는 자동화 징후와 기타 지표를 찾습니다. 하지만 봇이 진화하고 정교해짐에 따라 봇도 더욱 전문화되었습니다. 이제 봇은 사이트에서 콘텐츠를 스크레이핑하거나, 대규모 이벤트 기간 동안 인벤토리를 비축하거나, 고객 계정을 탈취하기 위한 크리덴셜 스테핑 등 다양한 용도에 맞게 설계됩니다. 그리고 한 종류의 특수 봇을 탐지하되 다른 봇은 탐지하지 못하는 경우가 많습니다. 따라서 벤더사가 기본적인 범용 봇뿐만 아니라 기업이 직면한 특정 봇을 차단할 수 있는지 확인해야 합니다.

고려 사항

- 벤더사가 비즈니스 사용 사례에 기반한 전문화된 봇 탐지 기능을 갖추고 있나요?
- 벤더사가 특정 봇 문제에 대한 전문성을 입증할 수 있나요?
- 벤더사의 다른 고객 중 얼마나 많은 고객이 동일한 문제에 직면하고 있나요? 벤더사가 다른 고객들로부터 배운 교훈을 활용할 수 있나요?
- 벤더사가 보고서, 서비스, 기타 기능을 제공해 전문화된 악성 봇과 싸울 때 지원할 수 있나요?



2 인텔리전스

봇 관리 솔루션의 성능은 모니터링하는 봇의 특징을 인식할 수 있는 능력에 의해 결정됩니다. 일부 벤더사는 99.9%의 봇을 탐지한다고 주장하지만, 그 효과를 객관적으로 측정하기는 불가능합니다. 봇은 항상 변화하기 때문에 어제 탐지한 봇이 오늘은 탐지를 회피하는 방법을 배웠을 수도 있습니다. 봇 관리 툴을 평가할 때 더욱 좋은 기준이 될 수 있는 것은 벤더사가 봇 탐지 기능을 알려주는 방식입니다. 일반적으로 의심스러운 봇뿐만 아니라 가장 정교한 봇을 탐지할 수 있는 솔루션과 가장 큰 데이터 세트를 활용하는 솔루션이 필요합니다. 많은 AI(Artificial Intelligence) 및 ML(Machine Learning) 툴이 오픈 소스이므로 솔루션의 AI 및 ML을 평가할 때 데이터의 양, 데이터의 청결도, 솔루션이 알고리즘에 데이터를 공급하는 속도가 과소평가되고 있다는 점을 유념해야 합니다. 인사이트에는 도메인 전반의 모든 로그인에 대한 신뢰 지표와 리스크 점수가 포함되어야 합니다. 또한 효과적인 솔루션은 최신 방법을 사용해 봇 탐지에 대한 다각적인 접근 방식을 취해야 합니다.

고려 사항

- 벤더사가 봇 탐지 기능에 대한 정보를 어떻게 제공하는지 자세히 확인하세요. 공격자에게 매력적인 대규모 고객을 보유한 벤더사는 평가할 리스크 및 신뢰 신호, 더 많은 디바이스 이상 탐지 등의 기능을 구축하는 데 기반이 되는 경험과 포괄적인 데이터 세트를 더 많이 보유하고 있을 것입니다. 투명성이 부족한 벤더사는 경계해야 합니다.
- 벤더사가 솔루션을 지원하기 위해 AI 및 ML을 사용하나요? 해당 모델은 얼마나 정교한가요? 벤더사가 해당 모델에 얼마나 많은 데이터를 제공하는지도 중요합니다. 공격자는 AI를 사용하고 있기 때문에 여러분도 AI를 사용해야 합니다.
- 하지만 AI만으로는 충분하지 않습니다. 새로운 공격 기술을 지속적으로 찾고 해커 커뮤니티를 모니터링해 항상 한 발 앞서 나갈 수 있도록 지원하는 보안 연구원과 위협 인텔리전스 애널리스트 같은 자격을 갖춘 전문가 팀을 벤더사가 보유하고 있나요?

3 안정적인 보호

정교한 봇을 차단해도 영구적으로 사라지지 않습니다. 탐지를 피하기 위해 계속 변화하면서 집요하게 다시 찾아옵니다. 많은 봇 관리 솔루션은 초기에 봇(또는 적어도 일부)을 탐지할 수 있지만 봇이 변하면 효과가 떨어집니다. Akamai는 봇이 몇 시간 만에 변화하는 것을 목격했습니다. 기존의 개발 주기는 너무 느려 이를 따라잡기 어렵습니다. 선택한 솔루션이 시간이 지남에 따라 학습하고 진화하도록 해야 하며, 가급적 머신 러닝을 자동으로 사용해야 합니다. 여기에는 방어를 회피하는데 사용할 정보를 얻으려는 공격자의 접근을 어렵게 만드는 선제적 방어 기능이 포함되어야 합니다.

고려 사항

- 최첨단 봇 탐지 기술(예: 사용자 행동 분석 및 고객별 학습 모델)을 갖춘 솔루션을 찾아야 합니다. 이러한 솔루션은 봇의 형태가 변화하고 진화하더라도 오랫동안 효과를 유지합니다.
- 공격자가 방어를 우회할 수 있는 봇을 리버스 엔지니어링하기 어렵게 만드는 자바스크립트 난독화 같은 방어 기법이 솔루션에 포함되어 있는지 확인하세요.
- 해당 솔루션을 이미 배포한 다른 고객의 사례나 이용 후기 등을 요청해 이 솔루션이 장기적으로 효과가 있는지 확인해야 합니다.



4 오탐률 및 미탐률

봇 관리 솔루션이 봇을 차단했다고 표시할 때 시스템이 실제로 정상적인 사용자를 차단하지 않았는지 어떻게 알 수 있을까요? 오탐률을 대수롭지 않게 생각하는 벤더사들이 많습니다. 탐지된 모든 봇에 점수를 매기는 솔루션이 없는 경우 애매모호한 봇을 탐지하지 못해 '예 또는 아니오'의 이분법적인 결정을 내릴 수 있습니다. 또한 이러한 벤더사들은 오탐률이 높음에도 그저 많은 '봇'을 차단했음을 고객에게 보여주려 하는데, 이는 봇뿐만 아니라 유효한 트래픽, 즉 사람이나 기업에 가치 있는 '정상' 봇도 차단하고 있음을 의미합니다. 반면, 오탐률이 낮다는 말은 벤더사가 인간 사용자를 차단하지 않기 위해 전체 솔루션의 효율성을 낮춰야 했다라는 것을 깨닫기 전까지는 좋게 들리지만, 결국 허용해서는 안 되는 봇을 통과시키는 결과를 초래할 수 있습니다. 비즈니스에 지장을 주지 않으면서 악성 봇을 차단하되 보안 수준을 낮춰서는 안 됩니다. 파트너로 선택한 벤더사가 정확성과 오탐률 및 미탐률의 영향에 대해 신경을 쓰고 있는지 확인해야 합니다.

고려 사항

- 벤더사가 오탐률 또는 미탐률에 대한 조정을 고객에게 말기나요, 아니면 고객과 협력하기 위해 기능과 서비스에 투자하나요?
- 솔루션이 사이트 전반의 트래픽 패턴을 학습하고 자동 조정해 고객사의 부담을 줄이나요?
- 벤더사가 다른 챌린지 조치 대신 CAPTCHA 사용을 제안하나요? CAPTCHA 제안 여부는 중요한 근거가 됩니다. 사용자는 CAPTCHA를 싫어하지만, 벤더사 입장에서는 CAPTCHA 기능을 추가하면 룰을 조정하는 것보다 쉽게 오탐률을 최소화할 수 있습니다.
- 솔루션이 봇에서 발생한 요청이라고 판단했을 때 그 이유에 대한 가시성을 확인할 수 있는지 파악해야 합니다. 요청에 대한 정밀한 가시성을 통해 취해진 조치를 확인할 수 있는 기능과 설정 변경 사항을 프로덕션에 적용하기 전에 시각화할 수 있는 기능이 있는지 살펴보세요.



5 유연한 조치

정상 봇은 통과시키고 악성 봇만 차단하면 된다고 생각하기 쉽습니다. 하지만 환경은 그보다 훨씬 더 복잡해졌습니다. 많은 봇 운영자들은 대부분의 기업이 합법적인 사용자를 차단하는 리스크를 감수하기보다 악성 봇을 허용하는 리스크를 감수한다는 사실을 알고 있기 때문에, 리스크 신호를 충분히 낮춰 봇을 애매모호한 영역에 배치하는 방법을 배웠습니다. 솔루션은 정교한 조치를 제공해야 하며, 이를 통해 차단을 넘어 암호화 챌린지와 강화된 MFA 같은 챌린지 조치를 포함해야 합니다. 또한 정상 봇 같은 다른 종류의 상황에 대응하는 방법도 포함되어야 합니다. 트래픽이 많은 시간대에는 파트너 봇의 속도를 늦추고, 트래픽이 적은 시간대에는 봇을 즉시 통과시킬 수 있어야 합니다. 또한 동일한 카테고리의 봇에 대해 서로 다른 작업을 선택할 수 있어야 합니다. 예를 들어, 리테일러의 경우 인기 있는 쿠폰 봇은 사이트를 확인하도록 허용하고 거래하고 싶지 않은 봇은 차단할 수 있습니다. 특히 위치, 시간대 또는 계절에 따라 달라지는 봇의 경우, 비즈니스와 IT에 미치는 영향에 따라 다양한 종류의 봇에 서로 다른 조치를 적용할 수 있는 유연성이 필요합니다. 또한 단순히 모든 봇을 차단하는 솔루션이 아니라(그렇게 함으로써 회피 기법을 바꾸도록 가르치는 솔루션), 공격자가 공격하기 어렵고 비용이 더 많이 들도록 장애물을 만드는 솔루션이 필요합니다.

고려 사항

- 다양한 종류의 봇에 대해 개별적인 카테고리를 생성하는 기능이 있는지 아니면 좋은 봇과 악성 봇 두 가지로만 분류하는지 확인해야 합니다. 검색 엔진이나 금융 애그리게이터 같은 동일한 카테고리의 봇에 대해 다른 조치를 생성할 수도 있나요?
- 어떤 종류의 조건부 조치를 지원하나요? Slow(속도 늦추기)와 Serve Alternate Content(대체 콘텐츠 제공) 같이 트래픽 관리에 도움이 되는 고급 기능을 지원하나요? 암호화 챌린지 같은 조치를 포함하나요?
- 솔루션이 다양한 종류의 봇을 얼마나 탄력적으로 관리할 수 있나요? 단순한 톨인가요, 아니면 시간대별, 트래픽 비율별 또는 URL 별로 조치를 적용할 수 있나요?
- 솔루션이 리소스 집약적인 문제를 삽입해 봇 운영자에게 더 많은 비용을 발생시키며 403 오류 이상으로 요청량이 많은 증폭 공격을 느리게 할 수 있나요?



6 배포

봇 관리 솔루션의 경우 솔루션을 실행하는 데 걸리는 시간과 솔루션을 얼마나 빠르게 수정할 수 있는지가 핵심 고려 사항입니다. 구매자는 기존 애플리케이션을 수정해야 하거나 애플리케이션 성능에 영향을 미치는 솔루션은 주의해야 합니다. 배포 지연은 많은 비용을 초래할 수 있으며, 깜짝 세일처럼 비즈니스 이벤트에 따라 애플리케이션을 변경해야 하는 경우 더 많은 리소스가 필요할 수 있습니다.

고려 사항

- 솔루션이 기존 애플리케이션의 성능에 영향을 주지 않고 실시간으로 작동하나요?
- 기존 애플리케이션을 변경해야 하나요?
- 증폭 공격 또는 반짝 세일 같은 예상치 못한 이벤트에 대응하기 위해 확장 또는 축소할 수 있나요?



7 가시성 및 리포팅

모든 봇 관리 솔루션은 봇 트래픽에 대한 전반적인 수준의 통계자료를 제공하지만 더욱 상세한 정보가 필요합니다. 인프라 계획이나 관리팀에 보고하는 경우 상위 수준의 통계자료는 봇 트래픽을 분석하는 데 필요한 세부 정보는 제공하지 않습니다. 게다가 솔루션이 올바른 조치를 취했다고 확신할 수 있는 증거 역시 제공하지 않습니다. 기업의 사용자를 차단할 수 있는 솔루션이라면 상세한 통계자료가 반드시 필요합니다. 비즈니스를 지원하고 리스크 임계값 변경이 성능에 미치는 영향을 더 잘 이해하려면 상세한 보고가 필요합니다.

고려 사항

- 비즈니스를 지원하고 신속하게 인사이트를 도출하는 데 필요한 상세한 리포팅을 제공하는 솔루션이 필요합니다. 다양한 점수 세그먼트와 어떤 봇이 어떤 엔드포인트를 공격하고 있는지, 또한 어떤 조치가 취해졌는지에 대해 보고할 수 있나요?
- 트래픽이 급증하는 상황을 조사하고 요청을 개별적으로 자세히 살펴볼 수 있나요? 요청의 세부 내용을 확인해야 어떤 조치를 취해야 할지 결정할 수 있는 경우가 있습니다.
- 여러분의 봇 트래픽이 업계의 다른 봇 트래픽과 어떻게 비교되는지 보여줄 수 있나요?
- 이러한 리포팅 기능은 다른 보안 솔루션에서 제공하는 리포팅 기능과 어떻게 연결되나요? 트래픽을 전체적으로 분석할 수 있나요, 아니면 별도의 보기가 있나요?



8 API 보호

벤더사나 솔루션에 상관없이 현재의 정교한 봇 탐지 기술들은 하나같이 자바스크립트 코드 삽입과 클라이언트 응답 분석에 의존합니다. API 기반 클라이언트가 자바스크립트에 응답하지 않을 경우에는 API를 어떻게 해야 할까요? 모바일 앱이나 기타 써드파티 지원을 위해 API를 노출해야 한다면 웹 페이지를 보호하는 것과 동일한 방식으로 API를 보호할 수 있는 솔루션이 필요합니다. 그렇지 않으면 웹 페이지에 발생한 봇과 봇 문제가 API로 옮겨가게 됩니다.

고려 사항

- 벤더사가 어떤 API 보안 기능을 제공하나요? 혹시 할당량 관리와 전송률 제한 (Rate Limiting)이 전부인가요?
- 벤더사의 가장 정교한 봇 탐지 기술을 기업의 모바일 앱에 통합할 수 있는 모바일 기능을 찾아야 합니다.
- 평판 기반의 접근 방식은 다른 능동적 탐지만큼 효과적이지는 않지만, SDK와 같은 모바일 기능에 접속할 수 없는 써드파티를 지원하는 API를 보호하는 좋은 방법이 될 수 있습니다.



9 사이트 vs 페이지

웹사이트가 여러 페이지로 구성되어 있다면 웹사이트의 여러 부분에 영향을 끼치는 봇 문제로 인해 어려움을 겪을 수 있습니다. 가격 스크레이핑은 제품 페이지에 큰 영향을 미칠 수 있습니다. 콘텐츠 스크레이핑은 부가가치가 높은 디지털 콘텐츠를 훼손할 수 있습니다. 한편 로그인 페이지에 대한 인증정보 도용 공격은 여전히 발생하고 있습니다. 하지만, 일부 봇 관리 솔루션은 이렇게 많은 문제들 중 하나만 해결하도록 설계되어 있습니다. 전체 사이트가 봇의 영향을 받든 또는 특정 페이지만 영향을 받든 상관 없이 언제나 모든 봇 문제를 해결할 수 있는 관리 솔루션을 찾아야 합니다.

고려 사항

- 솔루션이 집중적으로 다루는 부분이 개별 페이지인지 또는 전체 웹사이트인지 확인해야 합니다. 개별 페이지 앞단에 구축되는지 또는 전체 페이지 앞단에 구축되는지 확인해야 합니다.
- 솔루션이 인증정보 도용, 웹 스크레이핑, 콘텐츠 애그리게이션 등 기업이 직면한 모든 봇 문제를 효과적으로 해결할 수 있나요?





10 매니지드 서비스

봇이 사용자와 기업에 미치는 영향을 제어하려면 봇 관리가 필요합니다. 그러나 봇을 관리한다는 것은 그리 쉬운 일이 아닙니다. 기업 내 전문가를 보유하고 있다 하더라도 추가적인 도움이 필요한 경우가 발생합니다. 봇 문제를 이해하는 전문가가 있어야 합니다. 게다가 이러한 직책을 맡을 인력을 확보하기가 점점 더 어려워지고 있습니다. 일부 인력이 퇴사하면 어떻게 될까요? HTTP 요청을 확인한 후 트래픽을 차단하는 시그니처를 생성하는 작업은 누구나 할 수 있습니다. 하지만 문제를 해결하지 못합니다. 봇을 사용해 봇 문제를 재현한 후 해당 문제를 해결할 수 있는 전략을 설계·구축할 수 있는 전문가가 필요합니다.

고려 사항

- 솔루션을 최대한 활용하는 데 필요한 봇 관련 전문 지식을 내부적으로 보유하고 있나요?
- 봇 관리 솔루션 벤더사가 전문 서비스를 제공하나요, 아니면 제품만 판매하나요?
- 긴급 상황 발생 시 언제든지 선제적인 모니터링 및 추가 전문가 리소스에 접속할 수 있나요?





사후 대응이 아닌 선제적 대응

봇이 문제가 되기 전에, 그리고 다음 변화의 물결로 인해 기존 방어 체계가 이전 방어 체계의 모방에 불과해지기 전에 봇 관리에 투자해야 합니다. 선택 가능한 솔루션을 조사할 때 이러한 점을 고려해야 합니다. Akamai Bot Manager는 기업이 필요로 하는 확신을 제공하는 데 도움을 드릴 수 있습니다. 자세한 내용을 알아보려면 모의 공격에 대한 맞춤형 데모를 요청하세요.

자세히 보기



Akamai는 어디에서 구축하고 제공하든지 생성하는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 인력, 시스템, 데이터를 보호합니다. Akamai 플랫폼은 글로벌 위협에 대한 가시성을 바탕으로 제로 트러스트 지원, 랜섬웨어 차단, 앱 및 API 보안 또는 DDoS 공격 차단을 목표로 보안 체계를 조정하고 발전시켜 지속적으로 안심하고 혁신하며 확장하고 가능성을 현실로 구현할 수 있습니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 대해 자세히 알아보려면 akamai.com와 akamai.com/blog를 확인하거나 [Twitter](#)와 [LinkedIn](#)에서 Akamai Technologies를 팔로우하시기 바랍니다. 2023년 09월 발행