ボット管理に関する 10 の考慮事項

eブック

目次

はじめに

ボットの問題がどれほど難しくなっているか気になりませんか。テイラー・スウィフトのチケットや新しいエア・ジョーダンを手に入れようとしてみてください。これらは注目のセールスイベントに過ぎませんが、ボットは、さまざまな業界にますます蔓延し、悪質化の度合いを深めています。

答えを求める人にとってさらに悪いのは、ボット管理が根底から変わってしまったことです。実のところ、ボット管理は常に変化し続けてきました。ボット管理は、軍拡競争や猫とネズミの追いかけっこと表現されることが多いように、防御策を講じる企業側とそれを回避する方法を探し続けるボット作成者側のいたちごっこです。しかし今、進化しているのはボット自体にとどまりません。ボットを取り巻く環境も同様に進化しています。たとえば、企業が対峙しているのはもはや個々のアクターにとどまらず、さらには組織化されたグループにもとどまりません。今や、Airbnb を利用するのと同じように、ボットを 1 週間レンタルすることさえできるようになっているのです。同様に、ボットを善玉と悪玉に仕分けるだけのソリューションでは不十分です。グレーゾーンが広すぎるのです。

ボットとそれを取り巻く環境のこのような進化により、ボット管理ソフトウェアの選択がこれまで以上に難題になっています。過去のボットに対して何が効果的だったのか把握するだけでなく、現在そして未来のボットに対して何が効果的なのか予想することも必要です。

このガイドでは、ボット管理ソフトウェアを選択する購入者にとって重要な考慮事項をいくつか説明します。ガイドの情報を参考にノイズを選別し、十分な情報に基づいて購入の決定を下してください。

1 高度な専門知識

ボット管理ソリューションの役割は、ボットを検知することと定義されています。つまり、ボット管理ソリューションは、自動化の兆候や、リクエスト元が人間ではないことを示すその他のサインを探します。しかし、ボットは進化し高度化するにつれ、より専門的にもなりました。現在では、サイトからのコンテンツのスクレイピング、人気セールスイベント中の在庫の買い占め、顧客アカウントを乗っ取るための Credential Stuffing など、絞り込んだ目的に合わせて設計されています。また、1　種類の専門化されたボットを検知できるソリューションが他のボットは検知できないこともよくあります。基本の汎用的なボットだけでなく、貴社が直面している特定のボットをそのベンダーが阻止できるかどうかを見極める必要があります。

検討事項

- そのベンダーは、ビジネスユースケースに基づくボットに特化した検知機能を備えていますか。
- そのベンダーは、貴社が直面している具体的なボットの問題に関して専門知識を示すことができますか。
- そのベンダーに、貴社と同じ問題に直面している顧客はどれくらいいますか。ベンダーがこれらの顧客から学んだことが、貴社に活かされるでしょうか。
- そのプロバイダーは、専門化された敵対的ボットとの戦いをさらにサポートするレポート、サービス、その他の機能を提供していますか。

2 インテリジェンス

ボット管理ソリューションは、監視対象のボットの特性を認識する能力があって初めて、優れたソリューションと言えます。99.9%のボットを検知できると主張するベンダーもありますが、有効性を客観的に測定することは不可能です。ボットは常に変化しています。貴社が昨日検知できたボットが、今日は検知を回避する方法を身につけてしまった可能性もあります。ボット管理ツールを評価する際は、ベンダーが自社のボット検知機能にどのように情報を供給しているかが良い基準になります。必要なのは、最も高度なボット（通常の疑わしいボットだけでなく）を検知でき、最大規模のデータセットからデータを取得できるソリューションです。多くの人工知能（AI）と機械学習（ML）ツールがオープンソースであることに注意が必要です。つまり、データの量、データのクリーンさ、アルゴリズムにデータをフィードする速度は、ソリューションの AI／ML を評価する際に過小評価されています。複数の領域にわたるすべてのログインの信頼指標とリスクスコアが知見に含まれる必要があります。さらに、効果的なソリューションでは、最新の方法を使用して、ボット検知に多方面からアプローチを取る必要があります。

検討事項

- ボット検知機能にどのように情報を供給しているのか、ベンダーに詳しく尋ねてください。攻撃者にとって魅力的な大規模顧客を抱えるベンダーは、評価するリスクシグナルや信頼シグナルの種類、より多くのデバイスの異常検知など、能力を構築するためのより多くの体験や包括的なデータセットを持つことになります。透明性の欠如は、警告となるべきです。

- そのベンダーはソリューションをサポートするために AI／ML を使用していますか。それらのモデルのレベルはどれぐらい高いのでしょうか。また、次の点も重要です。そのベンダーはこれらのモデルにどれくらいの量のデータを供給していますか。攻撃者が AI を使用しているのは間違いないので、貴社も活用すべきです。

- しかし、AI だけでは不十分です。そのベンダーは、セキュリティリサーチャーや脅威インテリジェンスアナリストなどの資格を持つ専門家のチームを擁していますか。こうしたチームは常に斬新な攻撃手法を探し、ハッカーコミュニティを監視して、常に一歩先を行くようにしていますか。

3 耐障害性に優れた保護

ボットをブロックしても、消えてなくなるわけではありません。ボットは、検知を逃れようと常に変異しながら、何度でも戻ってきます。ボット管理ソリューションの多くは、当初はボットを検知することができますが（少なくとも一部は検知可能）、ボットが変異し始めると検知できなくなります。Akamai　はボットが数時間で変異するのを見てきました。従来の開発サイクルでは遅すぎて対応できないのです。選択したソリューションが、できれば機械学習を自動的に使用して、時間とともに学習し、進化することを確認してください。これには、防御を回避するための情報を狙う攻撃者をより困難にする、先制的な防御も含まれている必要があります。

検討事項

- 最先端のボット検知テクノロジー（ユーザーふるまい分析や顧客固有の学習モデルなど）が採用されたソリューションを探してください。こうしたソリューションは、ボットが変異しても比較的長期間効力を持続します。
- そのソリューションに JavaScript の難読化などの防御戦術が含まれているかどうかを確認します。このような戦術により、防御をすり抜けるボットのリバースエンジニアリングが困難になります。
- 長期間効力を持続するかどうかを確認するために、そのソリューションを展開済みの他の顧客から裏付けや参考情報を入手します。

4 フォールス・ポジティブ（誤検知）とフォールス・ネガティブ（検知漏れ）

ボット管理ソリューションがボットを阻止したと示したとき、そのシステムが阻止したのが正規ユーザーでないことがどうしたら分かるのでしょうか。多くのベンダーは、誤検知を大雑把に扱います。すべての検知に対してボットをスコアリングするソリューションがない場合、グレーボットを検知できず、「はい」「いいえ」の二者択一になる可能性があります。これらのベンダーは、誤検知率の高さにもかかわらず、どれだけ多くの「ボット」を阻止したのかを顧客に見せたがります。これは、ボットだけでなく、企業にとって価値のある人間や「良性」のボットも阻止していることを意味します。一方、検知漏れ率が低いというのは素晴らしいことのように聞こえますが、実際のところ検知漏れ率の低さは、ベンダーが人間のユーザーをブロックしないようにするためにソリューション全体の有効性を下げざるを得ず、その結果、本来は通すべきではないボットを通してしまったということです。ビジネスの妨げにならないように悪性ボットを阻止することも、保護レベルも下げないことも重要です。提携しているベンダーが、精度や誤検知、検知漏れの影響を気にかけていることに確信が持てなくてはなりません。

検討事項

- そのベンダーは、誤検知や検知漏れの調整をお客様任せにしていないでしょうか。それとも、お客様と協働するための機能やサービスに投資しているでしょうか。
- そのソリューションは、サイト間のトラフィックパターンから学習し、チームの負担を軽減するように自動調整していますか。
- そのベンダーは、他のチャレンジアクションの代わりに CAPTCHA を使用することを推奨していませんか。これは決定的な証拠となることがよくあります。ユーザーは CAPTCHA を好みませんが、ベンダーにとっては、誤検知を最小限に抑えるためにルールを調整するよりも CAPTCHA を採用する方が簡単です。
- ボットからリクエストがあった際に、なぜソリューションがそのリクエストにフラグ付けしたか可視化されますか。それとも、ブラックボックスですか。リクエストを細かく可視化して実行されたアクションを検証し、本番環境で稼働する前に設定の変更を可視化する機能を見つけてください。

5 柔軟なアクション

悪性ボットを阻止し、良性ボットを通すことだけを心配すればよいというのは魅力的な考えです。しかし、環境はそれよりもはるかに複雑になっています。ボットオペレーターの多くは、正規のユーザーを阻止するリスクよりも悪性ボットを侵入させるリスクの方が組織にとって高いことを知っています。そのため、ボットをグレーゾーンに置くことでリスクシグナルを十分に下げる方法を学んでいます。一連の高度なアクションを提供するソリューションを選択する必要があります。それにより、ボットの阻止や許可にとどまらず、暗号化チャレンジやステップアップ MFA などのチャレンジアクションを含めることができるようになります。また、そのソリューションには、良性ボットなど、他の種類の状況に対処するためのアクションも含まれている必要があります。トラフィックの多い時間帯にパートナーボットを減速させ、ピーク時以外はそれらのボットを即座に通過させたいといったことも考えられます。また、同じ既知のカテゴリーのボットに対して異なるアクションを選択することもできます。たとえば小売企業の場合、より人気の高いクーポンボットにはサイトをチェックさせ、相手をしたくないボットは阻止することも可能です。ビジネスや IT 部門への影響に基づいて、さまざまなタイプのボットに異なるアクションを取ることのできる柔軟性が必要です。特に、そうした影響が場所や時間帯、季節によって異なる場合は、柔軟性が重要です。それ以上に、単にすべてのボットを阻止してボットに回避戦術を変えるよう教えてしまうのではなく、障害物を作り、攻撃者にとってより難しく、より高くつくようにするソリューションが必要です。

検討事項

- そのソリューションは、ボットのタイプに応じてさまざまなカテゴリーを作成できますか。あるいは、良性のボットと悪性のボットを区別するだけですか。また、検索エンジンや金融アグリゲーターなど、同じカテゴリーのボットに対して異なるアクションを作成できますか。
- そのソリューションは、どのようなタイプの条件付きアクションを取ることができますか。トラフィックを向上させる低速の代替コンテンツの提供など、高度なアクションを取ることができますか。暗号化チャレンジのようなアクションも含まれていますか。
- そのソリューションは、検知されたさまざまなボットをどのくらい柔軟に管理できますか。攻撃に対して攻撃し返すだけですか。それとも、時間、トラフィックのパーセンテージ、URL に基づいて、きわめて正確にアクションを取ることができますか。
- そのソリューションは、ボットオペレーターのコストを上げ、ハード 403 以上に大量リクエスト攻撃をスローダウンさせる、リソース集約型の問題を組み入れることができますか。

6 導入

どのようなボット管理ソリューションでも、ソリューションの立ち上げにかかる時間と変更の迅速さが重要な考慮事項となります。購入者は、既存のアプリケーションへの変更を要求するソリューションやアプリケーションのパフォーマンスに影響を与えるソリューションに用心する必要があります。導入が遅れるとコストがかさみます。また、フラッシュセールのようにビジネスイベントに応じてアプリケーションを変更する必要があると、より多くのリソースが必要になります。

検討事項

- そのソリューションは、既存のアプリケーションのパフォーマンスに影響を与えることなく、リアルタイムで動作しますか。
- 既存のアプリケーションに変更を加える必要はありますか。
- ボリューム型攻撃のような不測の事態や、フラッシュセールのような想定外のイベントに対応するように、スケールアップまたはスケールダウンできますか。

7 可視化とレポート

ボット管理ソリューションはどれも、ボットトラフィックの高レベルの統計情報を表示できますが、それ以上の機能が必要です。高レベルの統計情報は、インフラ計画や管理職への報告には適していますが、ボットトラフィックの分析に必要なきめ細かさはありません。さらに、高レベルの統計データでは、そのソリューションが適切なアクションを取ると信頼できるエビデンスが得られません。ユーザーをブロックできるソリューションの場合、ブラックボックスにしたくはありません。ビジネスをサポートし、リスクしきい値の変更がパフォーマンスに与える影響についての理解を促進する、詳細なレポートが必要になります。

検討事項

- そのソリューションには、特定のボット、ボットネット、ボットの特性について詳しく知ることのできるレポート機能が備わっていますか。異なる複数のスコアセグメントや、攻撃しているボットと攻撃されたエンドポイント、実行されたアクションについてレポートできるソリューションですか。
- トラフィックの急増について調べたり、個々のリクエストを見たりすることはできますか。リクエストの詳細を見れば、対応策が分かることもあります。
- そのソリューションは、ボットトラフィックを同業他社と比較して表示できますか。
- レポート機能は、他のセキュリティソリューションのレポート機能と連携していますか。トラフィックを総合的に分析できますか、それとも個別のビューがありますか。

8 API の保護

ベンダーやソリューションにかかわらず、現行の最先端のボット検知テクノロジーは、JavaScript コードを挿入してクライアントの応答を分析しています。それでは、API ベースのクライアントが JavaScript に応答しない場合は、API をどのようにすればよいのでしょうか。API を公開してモバイルアプリなどのサードパーティー製品に対応させる必要がある場合は、Web ページの保護と同様の方法で API を保護できるソリューションが必要です。そうしないと、ボット（およびボット問題）によって、Web ページから API に簡単に移行されてしまいます。

検討事項

- そのベンダーは、API に対してどのような保護を提供していますか。クォータ管理やレート制限のみですか。
- そのベンダーの最先端のボット検知機能をモバイルアプリに組み込むことのできるモバイル機能を探します。
- 必ずしも他のアクティブな検知機能と同様に効果的とは限りませんが、レピュテーションベースのアプローチでも、SDK のようなモバイル機能にアクセスできないサードパーティー製品をサポートする API を保護することができます。

9 「サイト」対「ページ」

Web　サイトが複数のページで構成されている場合は、複数のボット問題が発生する可能性があり、それぞれがサイトのさまざまな部分に影響を及ぼします。価格スクレイピングは、商品ページに大きな影響を与える可能性があります。コンテンツのスクレイピングは、付加価値の高いデジタルコンテンツを損なう可能性があります。一方、ログインページに対する Credential Abuse 攻撃は依然として発生しています。しかし、ボット管理ソリューションの中には、1 つの問題にしか対応しないものもあります。貴社の管理ソリューションがすべてのボット問題に対応できるかどうか、また、それらがサイト全体に影響を及ぼすものであるか、あるいは特定のページにのみ影響を及ぼすものであるかを確認する必要があります。

検討事項

- そのソリューションは、個々のページとWebサイト全体のどちらを重視していますか。また、どのように展開しますか。個々のページの外側か、Web サイト全体のどちらですか。
- そのソリューションは、すべてのボット問題、つまり、Credential Abuse、Web スクレイピング、コンテンツアグリゲーションに対応できますか。

10 マネージドサービス

貴社や貴社のビジネスへの影響を軽減するためにボットを管理する必要がありますが、ボット管理は簡単ではありません。社内で詳しい人ですらサポートを必要とすることがあります。つまり、ボット問題を理解しているエキスパートが必要だということです。さらに、これらのポジションの人材確保はますます困難になっています。人材の一部が退職した場合はどうなるでしょう。HTTP リクエストを見てトラフィックをブロックするシグネチャーを作成することは誰にでもできますが、それでは問題は解決しません。必要なのは、ボットのことを本質的な問題に結びつけ、その問題を解決するための戦略を策定し、実施できる人材です。

検討事項

- あらゆるソリューションを最大限に活用するために必要な、ボット専門の担当者は社内にいますか。
- ボット管理ベンダーは、プロフェッショナルサービスを提供してくれますか。または、製品を販売するだけですか。
- 緊急事態が発生した場合に、予防的モニタリングや補助的な専門家リソースにいつでもアクセスできますか。

事後ではなく、事前に対応する

ボットが問題になる前に、また、次の進化の波によって既存の防御が以前の防御の弱体版のようなものになる前に、ボット管理に投資することで、より効果的に対処できます。オプションを調べる際は、これらの点を考慮してください。Akamai Bot Manager は、お客様が必要とする保証を提供するお手伝いをします。詳細については、パーソナライズされた攻撃シミュレーションのウォークスルーをリクエストしてください。

詳細を見る