AKAMAI 製品概要

Bot Manager

自分が誰を信頼し、そして、誰に信頼されているのか。どちらも等しく重要なことです。オンライン取引では、信頼できる存在であるという相手側（消費者、パートナー、ボット）の主張を信じる必要があります。しかし残念ながら、正当なユーザーになりすまして知的財産を盗もうとしたり、業務に悪影響を与えようとするボットが多く、このようなボットがサイトトラフィックの 70% を占めることもあります。Akamai Bot Manager は、ボットを可視化し、制御できるようにすることで、お客様のビジネスを保護します。これは、オンラインでの信頼関係を守ることにもつながります。

オンライン業務の効率を高めるため、たとえば、消費者、パートナー、サプライヤー、サードパーティーとのやり取りの自動化などを目的として良性ボットを利用する企業が増えています。このようなボットがサイトのパフォーマンスや顧客体験に及ぼす影響を管理する必要があります。

一方、詐欺師や攻撃者側も自動化を進めています。彼らはボットネットを拡大し、以下のような目的に利用しています。

- 顧客が購入する前に在庫を買い占める
- Credential Stuffing 攻撃を開始する
- ロイヤルティポイントやギフトカードを盗む
- ビジネスロジックの脆弱性を悪用する
- サイトの速度を低下させ、コストを増大させるために企業を攻撃する

ボット運用者が企業やその顧客に悪影響を与えようと暗躍している状況で、どうすればオンライン取引の信頼性を確保できるでしょうか？また、信頼できることを他者に実証するためには、どうすればよいのでしょうか？

Bot Manager の比類ない検知機能と緩和機能を活用すれば、自動化をより効果的かつ安全に実行できるようになり、自社およびそのエコシステム全体の信頼を強化できます。

信頼は Akamai のボット管理から始まる

Akamai が信頼を得ているのは、技術的にも企業としてもグローバルな強みがあるからです。当社は、Global 500 企業の 50% 以上にサービスを提供しています。また、131 か国以上に 4,167 か所を超えるアクセスポイントを有し、年間収益は 36 億ドルを超えています。このような強みはすべて Bot Manager にも活かされ、年月が経過しても機能が低下することなく、また、常に新たなボットの傾向や回避手法に先制できるよう、開発が継続されています。

ビジネス上のメリット

信頼関係の強化：あらゆる当事者
正当なインタラクションの特徴を把握し、ユーザーのフリクションを軽減し、不正行為からユーザーを守ることによって、消費者、パートナー、お客様自身の間の信頼を強化します

修復の負担の軽減
侵害アカウントのチェック、盗まれたアカウントの回復、ユーザーからの苦情への対応など、ボット攻撃による経済的損失やリソースへの悪影響を軽減できます

運用管理の向上
効率を強化し、ビジネスリスクと経済的リスクを軽減し、IT 支出を管理し、パートナーボットを戦略的に管理できます

データに基づく的確な意思決定
詳細な分析とレポートは、カスタマージャーニー、セキュリティ対策、リスク許容度、IT 運用に関して、創造的かつ効果的な選択を行うために役立ちます

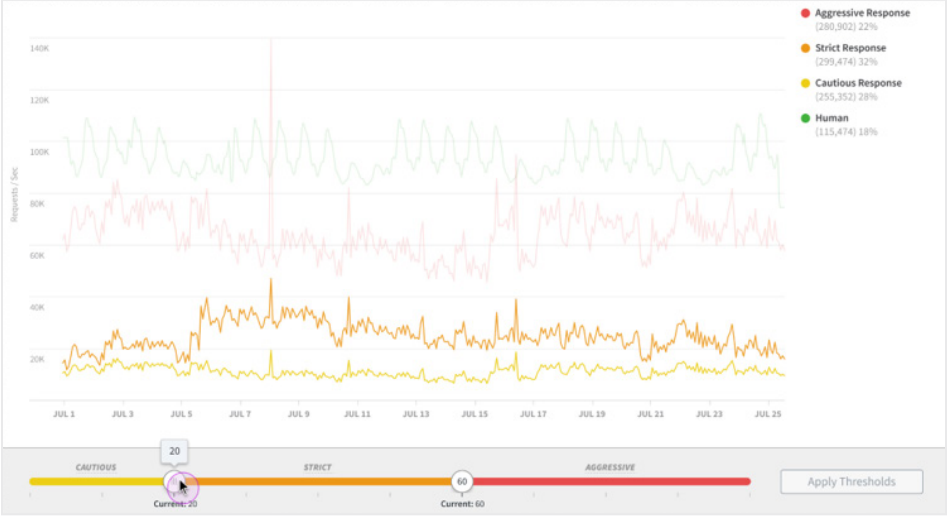
©2023 Akamai Technologies | サポート | 公開日：2023 年 10 月

Bot Manager は、特許取得済みテクノロジーを使用して、最初の接触ポイントでボットを検知し緩和します。ボットがお客様のサイトに直接到達することはありません。また、脅威が進化してもお客様を確実に保護できるよう、Akamai は絶えず保護をアップデートしています。Bot Manager の検出と分析には、Akamai の脅威インテリジェンスリサーチャーからの知見が自動的に取り込まれるため、お客様からアップグレードや機能拡張をお求めいただく必要はありません。

Bot Manager は、エンドポイントの Web、ネイティブ・モバイル・アプリ、API など、他者とのやり取りがあるすべての場所でお客様を保護します。また、ドメイン間でリクエストが転送されるときにもお客様を保護します。複数のブランドや事業を有する場合も、Bot Manager は最初のリクエストをインタラクションの最後まで追跡するため、防御の隙間が生じることはありません。

Bot Manager の AI フレームワーク

Bot Manager の機能は、Akamai Connected Cloud 上でインラインに動作する人工知能（AI）フレームワークから始まります。これにより、Bot Manager はユーザーが最初にアプリケーションに接続するエッジでトラフィックを把握できます。そのため、トラフィックパターン、トラフィックタイプ、トラフィックボリュームに関して、クリーンなデータを提供できます。Akamai は、ネットワーク全体で 1 日あたり平均 370 億件のボットリクエストを認識しています。



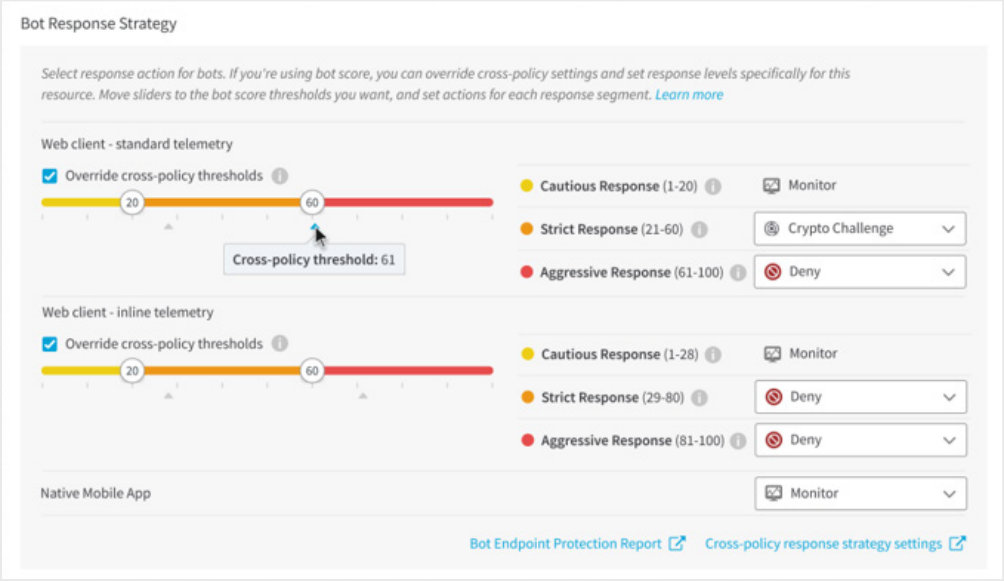
AI、機械学習、脅威インテリジェンス

広範なデータタイプについて膨大な「クリーントラフィック」データを収集することで、Akamai の機械学習（ML）アルゴリズムが鍛えられ、正確性が向上します。Akamai ネットワークでは、毎日 13 億台のデバイス（重複を除く）からのトラフィックが処理され、1 日あたり最高 164 Tbps というトラフィック量が記録されています。このような莫大なデータ可視性によって、Akamai のアルゴリズムはより速く、より大量に学習できます。また、400 人を超える Akamai の脅威リサーチャーチームが、攻撃パターン、テクノロジーイノベーション、新たな回避手段の傾向を常に追跡し、Akamai の検知能力を高めています。Akamai の脅威リサーチャーは毎日 662 TB もの新たな攻撃データを分析しています。これは、2021 年の 290 TB から大幅に向上しています。

Akamai の堅牢な AI／ML 技術に加えて、顧客固有のモデルにも対応できるようになりました。ディープ・ラーニング・モデルが、標的になりやすい有名ブランドの Web サイトに対する巧妙な攻撃を学習します。この学習内容を高度なアルゴリズムに組み込み、新しい攻撃に対する緩和策を、他の方法では数日や数週間かかるところを、このモデルは数分で実装します。

Bot Score — 検知したすべてのボットを評価

Bot Score は、あらゆる検知トリガーを総合的に組み合わせて、レイテンシーを増大させることなく、巧妙なボットを特定して、各リクエストをより正確に評価し、全体的な検知の有効性を最適化します。また、スコア範囲に基づいて、応答戦略を定義することもできます。



画期的なチャレンジ

Bot Manager の Bot Score 機能と最先端のチャレンジを組み合わせることで、事前定義済みのしきい値と応答アクションを用いて、自動でアクションを実行できます。人間には見えないチャレンジを使用することで、正当な人間のユーザーとボットを見分ける作業を軽減できます。クリプトチャレンジでは、最小時間で解ける暗号パズルでボットに CPU サイクルを消費させ、巧妙なボット攻撃を低速化して攻撃者のコストを増大させます。Interstitial Challenge では、クライアントに対して、cookie の保存と JavaScript の実行に対応していることを証明するよう求めます。対応していない場合、Bot Manager は、時間のペナルティに加えて、緩和策として選択されている応答アクションを実行します。

ネットワーク効果による攻撃防御

Akamai が防御しているお客様のなかには、注目度の高い世界最大規模の企業も含まれており、最も巧妙なボット運用者に頻繁に狙われています。あるお客様で新しいボットが検知されると、数分以内にそのボットに関するデータが既知のボットライブラリと Akamai 独自の「カタパルトアルゴリズム」の両方に追加され、全てのお客様に役立てられます。このようなネットワーク効果は、お客様がボットを効果的に管理できるようにするだけでなく、Akamai がこれらのボットに事前に対処して、他のお客様への攻撃を完全に阻止するためにも役立ちます。

迅速かつシンプルな展開

Bot Manager はそのインラインアーキテクチャにより、迅速かつシームレスに展開できます。起動した瞬間から正確に動作し、リアルタイムでボットを検知します。レイテンシーが生じることはなく、またサイトやネットワークのパフォーマンスに影響を与えることもありません。また、Bot Manager は、Akamai ネットワークの比類のないキャパシティを活用することで、お客様のニーズに応じたスケーリングも可能です。では、

Akamai ネットワークにはどの程度のキャパシティがあるのでしょうか。Akamai ネットワークの日々のトラフィックはピーク時に 100 Tbps を超え、2022 年 12 月 14 日には 261.21 Tbps という最大値を記録しています。

主な機能

既知のボットディレクトリ — Bot Manager は既知のボットに対して自動で適切に対応します。現在ディレクトリには 1,750 の既知のボットがあり、継続的に更新されています。

高度かつ動的なボット検知 — Bot Manager は、最初のインタラクションから未知のボットを正確に検知するために、多様な AI／ML モデルやテクノロジーを活用しています。たとえば、ユーザーのふるまい分析、ブラウザーフィンガープリンティング、ブラウザー自動検知、HTTP 異常検知、高リクエスト率などが活用されています。Bot Manager は、コードやテレメトリの動的な難読化により、リバースエンジニアリングを防止します。これにより、Bot Manager の有効性を長期にわたって高く維持できます。

スコアリングモデル — Bot Score モデルは、Bot Manager Premier が検知したすべてのリクエストを評価します。そして、それがボットからのリクエストである可能性を計算し、0（確実に人間）～100（確実にボット）のスコアを割り出します。

ブラウザー偽装検知 — ボット運用者は、特定のブラウザーを偽装することで、検知を回避しようとします。Akamai のブラウザー偽装検知では、定期的なチューニングを行うことなく、高い精度で偽装を検知し、他の検知方法よりもフォールス・ネガティブ（検知漏れ）を抑制できます。

エンドポイントごとのカスタム設定 — Bot Score では、エンドポイントごとに異なる応答戦略を設定できます。たとえば、検索ページへのリクエストについては、スコアが 35 以下のボットに対して Cautious（監視）を適用し、ログインページへのリクエストについては、しきい値を 20 に引き下げることができます。

応答調整シミュレーター — エンドポイントや組織のリスク許容度に基づいて、応答戦略を調整できます。応答戦略を調整したら、実際に実行する前にシミュレートできます。これにより、過去のトラフィックに基づいて、しきい値の変更が及ぼす影響を視覚化できます。

自動調整 — 調整における人間の介入を軽減して、ボットの進化に対応できます。Bot Manager は、サイト（または複数のサイト）の通常のトラフィックパターンを学習して、独自のパターンに基づいて検知を自動調整し、リクエストの誤分類を回避します。

応答アクションの微調整 — ブロックと許可だけでなく、代替コンテンツの提供、チャレンジの提供、低速化などのアクションを使用してボットの緩和効果を高めます。

詳細なレポートと分析 — Bot Manager のリアルタイムレポートと履歴レポートを活用することで、信頼できるデータに基づいた意思決定が可能となります。個々のボットや、ボットトラフィックのその他のセグメントに関して、全体的な傾向と詳細分析が可視化されます。また、自社のボットトラフィックを業界内の他社や Akamai のすべてのお客様と比較することもできます。

Managed Security Service（オプション） — 社内チームに負担をかけずに Bot Manager を最適化できます。専任の Akamai エキスパートが監視し、事前対応策を提案するとともに、セキュリティイベントの際には緊急サポートを提供します。

リスク認識型ボット管理

- **企業のリスク許容度に基づいてボット応答戦略を調整して、企業目標をサポート**
- **長期目標や個々のイベント（フラッシュセールなど）に合わせてスコアのしきい値を変更**
- **エンドポイントごとに応答戦略を設定（価値の高いエンドポイントについては、リスクスコアが低くても Aggressive（積極的）を適用するなど）**

詳細については、Akamai の担当者にお問い合わせください。
また、Akamai.com でも詳細をご覧いただけます。