CEQUENCE

Cequence Bot Management

ボット検知・緩和・不正防止

いまや良性・悪性を問わず、ボットはWebトラフィックの約半分を占めています。悪性ボットはかつて主にWebサイトやアプリを標的にしていましたが、現在はアプリを回避してAPIを直接狙うケースが増えています。アクセス容易性・柔軟性・普及の高さゆえに、APIは脅威アクターの最優先ターゲットになりました。適切に実装されたAPIであっても、大規模なアカウント乗っ取り（ATO）やショッピングボットの一環として、ビジネスロジックの悪用を受け得ます。偽アカウントの大量作成やコンテンツスクレイピングも、アプリケーションとそのAPIに対して常態化しています。組織には、アプリケーションとAPIに対する自動化攻撃を検知・阻止でき、導入が容易で即効性のあるソリューションが必要です。

Cequence Bot Management のポイント

- CAPTCHA不要 — ネットワークベースのアプローチで、エージェント／JavaScript／SDKの組み込みは不要
- ネイティブ緩和 — WAFなどのサードパーティ基盤に依存せず、攻撃の特定とブロックを実行
- 多彩な緩和オプション — ブロック、レート制限、ヘッダー挿入、デセプション（欺瞞）
- 柔軟な導入モデル — オンプレミス／SaaS／ハイブリッドに対応
- API不正防止 — 組織固有のユースケースに合わせた粒度の細かいポリシーをカスタマイズ可能

Cequence Bot Management 概要

Cequenceは、組織のWeb／モバイル／APIアプリケーションをあらゆるボット攻撃から保護し、データ流出、窃取、不正を防ぎます。MLベースの分析エンジンが、アプリケーションおよびAPIの各トランザクションが正当か悪性かをリアルタイムに判定。ネイティブな緩和機能で攻撃を遮断し、ダウンタイムやブランド毀損、売上分析の歪み、インフラコスト増といった悪影響を排除します。

主な機能

アプリ改修不要・顧客フリクションなし

Cequenceのネットワークベースのアプローチは、エージェントやアプリ改修（JavaScriptの挿入やモバイルSDK統合など）を不要にします。これにより、CAPTCHAなどのボット対策が招く顧客フリクションを解消し、計測できるアプリに限定せず、すべてのアプリケーションとAPIをカバーします。ネットワークベースの保護なら、アプリ計測に伴う開発・テスト作業も不要になり、時間とコストを削減できます。

多くの組織はボット問題を認識していないだけで、ボットは攻撃を大規模に自動化するための手段にすぎません。Cequenceは次のような攻撃を検知し、緩和します。

多くの組織はボット問題を認識していないだけで、ボットは攻撃を大規模に自動化するための手段にすぎません。Cequenceは次のような攻撃を検知し、緩和します。

アカウント乗っ取り（ATO）

BOLA（Broken Object Level Authorization）の悪用

フラッシュセール／話題化セール／スニーカードロップの買い占め

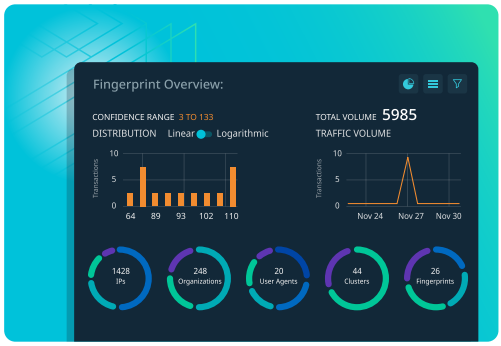
機密データの露出

ギフトカード／ロイヤルティプログラムの悪用

偽アカウント作成

継続的な行動ベースの脅威検知

MLベースの分析エンジンがWeb／モバイル／APIトラフィック全体の「行動の意図」を解析し、IPアドレスだけに頼らず、ふるまいに基づいて正当か悪性かを判定します。解析結果から「行動指紋」を形成し、回避策を講じる高度な攻撃であっても継続的に追跡。クライアント側やアプリ側の組み込みを必要としないため、幅広いアプリケーション／API保護を短期間で実現します。



AI／MLを活用したボット防御

CequenceはUAPプラットフォーム全体でAIとMLを活用し、検知から緩和までを支援します。MLモデルは、エンドポイントや脅威の高精度な分類、機密データの検出、行動指紋の生成などを実現。さらに、悪性アクティビティを検知すると、緩和ルールやポリシーを自律的に作成し、自動適用または人手による確認後に適用できます。エンタープライズにおける正当な生成AI／エージェント型AIの活用を保護しつつ、AIボットによる不要なスクレイピングや、攻撃者がAIを用いて仕掛ける高度な攻撃からも防御します。

迅速な価値実現

アプリの改修は不要。SaaS／オンプレミス／ハイブリッドなど柔軟な展開オプションにより、短期間で効果を発揮します。

ビジネスに合わせた不正防止

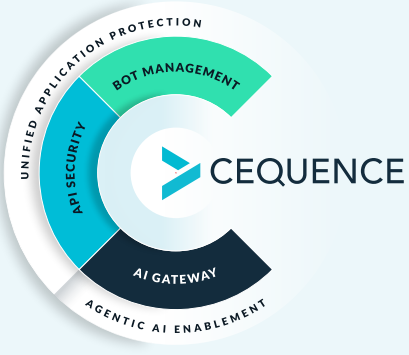
Cequence Bot Managementは不正防止機能を備え、業務・業種固有のユースケース向けに、カスタマイズ可能で粒度の細かいポリシーをサポートします。APIに流入するトラフィックを監視し、これらのポリシーに合致する不正行為をリアルタイムに特定・遮断。各不正キャンペーンの詳細分析に必要な情報も提供します。新しいポリシーの作成や、用意されたポリシーの調整はノーコードで実施可能です。

Cequence AI Gateway との連携

Cequence AI Gatewayは、社内／社外／SaaSアプリケーションへのエージェント型AIアクセスを、コード不要で数分で有効化します。Bot Managementは、悪性エージェントからエンタープライズのアプリケーションとAPIを堅牢に保護します。

Bot Managementは、Cequence Unified Application Protection（UAP）プラットフォームの一部です

Cequence Unified Application Protection（UAP）プラットフォームは、ディスカバリー／コンプライアンス／プロテクションを統合し、組織のアプリケーションとAPIを攻撃・ビジネスロジックの悪用・不正から守ります。数日～数週間ではなく“数分”で価値を実証でき、アプリの計測や改修を必要としない柔軟なデプロイモデルを提供します。最大規模で要求水準の高い民間・公共機関から信頼され、Cequenceは1日100億件超のAPIインタラクションと40億のユーザーアカウントを保護しています。



CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai