

Brand Protector 製品概要

フィッシングサイト、偽装ストア、ブランドなりすましを検知して阻止し、顧客への被害を防ぎ、大規模な詐欺や悪用攻撃のリスクを低減します。

認知度の高いブランドは、社内外で注目に値する価値を生み出します。ブランド要素を保護することで、組織は損失、生産性の低下、マイナスの顧客レビューを最小限に抑えながら、顧客ロイヤルティを維持し、向上させることができます。セキュリティの観点から見ると、ブランドなりすましを制御することで、即座にキルチェーンを断ち切り、認証情報の収集やアカウントの悪用を防止できます。

しかし、すべての攻撃が企業の正面玄関から行われるわけではありません。Web 上のあらゆる場所で、攻撃者はデジタルの偽装によってブランドになりすまし、顧客の機微な情報、認証情報、および直接支払われる金銭を盗もうとします。ブランドなりすましとフィッシングは、短期間で有効になったり無効になったりしながら場所を移動する短期的なキャンペーンであり、検知と緩和に多大なリソースを要するため、ますます大きな課題となっています。

Akamai Brand Protector は、ファーストパーティとサードパーティの両方のデータフィードを組み合わせた最大規模の脅威インテリジェンスデータベースを活用して、検知速度と精度を向上させます。総合的な緩和機能を備えている Brand Protector は、詐欺や悪用攻撃を早期に回避するために効果的で不可欠なツールです。

Akamai Brand Protector は、サイト、ソーシャルメディア、アプリストアでのフィッシング、なりすまし、ブランドの悪用などの標的型攻撃を検知して緩和します。そして何よりも、信頼関係を守ることができます。

毎週 50,000 件を超える新しいフィッシング Web サイトが作成されています。Akamai Brand Protector は、内外のソース全体で毎日数兆件のデジタルアクティビティを検査し、多くの場合、攻撃キャンペーンが実行される前に企業のブランドやブランド要素が悪用されるケースを高速かつ効率的に検知します。

インテリジェンス、検知、可視性、緩和の 4 ステップのアプローチを通じて、なりすましの問題に対応します。

ビジネス上のメリット

-  **信頼できる攻撃検知**
Akamai 独自のグローバルネットワークと追加フィードには、ブランドなりすましの検知という独自のメリットがあります
-  **正確性とスピード**
Akamai の高速検知アルゴリズムは、攻撃キャンペーンが開始される前にアラートを発し、誤検知を最小限に抑えることができます
-  **実用的な知見**
攻撃の重大度とリーチを一目で分かるように要約したリスクスコアリングにより、実用的な知見として総合的なデータを提供します
-  **顧客ごとの可視性**
Web サイト、ソーシャルメディア、アプリストアで、ブランド、製品、関連要素に固有の情報を収集します
-  **使いやすい**
リアルタイムの知見を獲得し、わずか数分で、拡大を続ける攻撃ベクトルに対する修正を実施します
-  **テイクダウンと緩和**
生産性を維持するために、Brand Protector に統合されたテイクダウンサービスを活用したり、ブラウジングアラートでトラフィックを阻止したりすることができます



インテリジェンス

フィッシングやブランドなりすまし攻撃を検知する取り組みは、インテリジェンスとデータ収集の段階から始まります。

世界最大のグローバルエッジおよびクラウドプラットフォームとして、Akamai は世界中の Web トラフィックを独自に掌握し、1 日に 788 TB 以上のデータを分析します。Brand Protector のインテリジェンスは、サードパーティからのデータフィードでさらに深みを増し、攻撃者の行動全体を把握できます。さらに、自組織の URL とドメインを追加し、Brand Protector の検知クラウドで分析することができます。

検知

Brand Protector は、Akamai 独自のインテリジェンスフィードと分析アルゴリズムを組み合わせて検知の信頼性を高め、フォールス・ポジティブ（誤検知）を減らすことで、検知力と検知速度を向上させています。

ブランド攻撃は、自動化された一時的な悪性 Web サイトを使用します。ほとんどのテクノロジーには、顧客に影響が及ぶ前にこの攻撃資産を検知して緩和するのに十分な速度がありません。しかし、Akamai のアプローチは異なります。Akamai はリストの更新や遅れがちなフィードに頼らず、ライブトラフィックを追跡し、ブランドの悪用を検知するからです。Brand Protector を使用すると、セキュリティチームは最初の HTTP / HTTPS リクエストが発生したとき（多くの場合、キャンペーンが顧客に到達する前）にフィッシングサイトを検知できます。

可視性

お客様を第一に考えたエンジニアリングと設計により、チームは単一のダッシュボードでセキュリティに関する広範な知見を得ることができます。

インテリジェンスを受信すると、データ信号がヒューリスティックな人工知能ディテクターで検証されます。膨大な量のデータとエビデンスが収集されますが、Akamai のシンプル化されたユーザーインターフェースにより、なりすましがお客様に及ぼすアクティブな脅威を即座に把握できます。

お客様固有のトラフィック、検知・脅威データを分析し、Akamai カスタマーポータルを通じて実用的な知見を提供します。分析結果は、端的な脅威スコアによってランク付けされます。アラートをクリックすると、信頼度、深刻度、影響を受けるユーザー数、攻撃イベントのタイムラインなど、脅威データの分析結果が表示されます。

検知された内容は、それぞれがエビデンスに基づくものです。コード、スクリーンショット、検知指標、およびドメインの詳細を 1 つの検知画面で確認できます。

緩和策

統合されたサイト閉鎖サービスにより、ブランドを悪用した詐欺行為への対策を完結できます。

お客様のチームは、Brand Protector の検知画面から不正サイトの閉鎖要求を直接送信できます。Akamai のサードパーティパートナーへ送信される Brand Protector へのテイクダウンリクエストは、検知の証拠と追加の詳細情報を自動的に添付するため、使い勝手に優れています。緩和の状況はポータルで追跡および確認できます。

ブランドに合わせた設計

ゾーン保護機能

Akamai のエッジ保護ポートフォリオの 1 つであるこのソリューションは、早期のキルチェーン保護に、セキュリティチームの視野を広げることができます。顧客にフィッシング攻撃を仕掛けるために利用され得るブランドのドメインを、プロアクティブに検索します。

ソーシャルメディア監視機能

ソーシャルメディアでのブランドなりすましが増加するなか、Akamai の強化された新しいソーシャルメディア監視機能は、オンライン詐欺を検知して無効化し、さまざまなプラットフォームでブランドとその顧客を保護します。

不正アプリ検知機能

アプリストアの監視は、公式および非公式のアプリリポジトリをスキャンして、ブランドアイデンティティを悪用する不正なアプリケーションを検知する新機能であり、デジタル環境全体を包括的に保護します。

