Akamai 製品概要

Brand Guardian

デジタルトラストは、現在、最前線のセキュリティ課題となっています。人工知能（AI）がブランドなりすましを産業化したことで、攻撃者は説得力のあるフィッシングサイトやドメイン偽装、詐欺キャンペーンを数分で開始できるようになりました。その結果、詐欺による損失の増加、顧客離れ、ブランドの信頼の低下が生じています。ブランドを監視する従来型のアプローチでは対応できません。組織は、インターネット規模で不正行為を検知して阻止する、インテリジェンスに基づく継続的なソリューションを必要としています。

顧客を保護し、信頼を維持するためには、組織はブランドの悪用を主要なセキュリティ課題として扱い、複数のアタックサーフェスにわたって、継続的な可視化、インテリジェントな優先順位付け、そして迅速な自動応答を実装することが不可欠です。

デジタルブランド保護の実態

不正行為やブランドの悪用は、もはやニッチなセキュリティ課題ではありません。自動化と生成 AI によって加速する、大規模な組織的活動となっているのです。これらのテクノロジーにより、攻撃者の参入障壁が劇的に低下し、説得力のある詐欺、フィッシングコンテンツ、偽のデジタル体験を、かつてないほどの速さと規模で作り出すことができるようになりました。

現在、攻撃者が偽サイトを立ち上げて、本物そっくりなブランディング、言語、顧客フローを完成させるまでにかかる時間は、数分です。大企業では、通常、何千もの活発な類似詐欺やなりすましの派生形に直面していますが、そのほとんどは従来型セキュリティツールが可視化できない範囲で発生しています。

同時に、ユーザーが偽の体験と正規の体験を見分けることは困難です。AI によって生成されたコンテンツ、複製された Web サイト、巧妙なソーシャルエンジニアリングといった戦術により、詐欺的なソーシャルプロファイル、E メール、ログインページが本物のように見えるからです。その結果、顧客は、自分がだまされていることを認識する前に（あるいはまったく気づかずに）、やりとりをし、資格情報を共有し、取引を完了してしまう可能性が高くなります。

これまでのブランド保護モデルは、事後対応で、手動の、部門連携が取れていない、サイロ化されたものでした。最新のブランドセキュリティは、継続的かつ自動化され、中核となるセキュリティ運用に統合されたものでなければなりません。これまでのワークフローは処理が遅く、リソースを大量に消費し、攻撃者がドメイン、ホスティングプロバイダー、アイデンティティを継続的にローテーションする環境には適していません。1つの不正なサイトが特定されて削除される頃には、複数の代替サイトがすでに公開されており、この悪循環が続いています。

ビジネス上のメリット

ブランドの信頼を守る
偽造サイトやなりすましをプロアクティブに排除して、あらゆるデジタルチャネルで安全性、信頼性、真正性（本物であること）を維持します。

顧客の不正被害を低減
高度な AI 主導の攻撃から顧客を保護するために、顧客が関与するよりも前にフィッシングや詐欺のインフラを排除します。

脅威への対応を加速
手作業の作業フローを自動探索と適用に置き換えることで、テイクダウンのスケジュールを短縮します。

顧客離れの抑制
顧客の不満や減少につながるブランド関連の詐欺を防ぎ、顧客維持を支援します。

人員を追加せずに拡張可能
自動化とインテリジェンスを使用して、何千ものルックアライク（類似）ドメインと詐欺の変種を同時に処理します。

リスクの優先順位付け機能の向上
顧客への影響、財務リスク、および評判に基づいてブランドの悪用を順位付けすることで、最も重要な脅威にリソースを集中させます。

経営陣向けの可視性を強化
ブランドリスク、テイクダウンの有効性、トレンド分析に関する明瞭で測定可能な知見を提供し、リーダーの露出に対する理解を深めるために支援します。

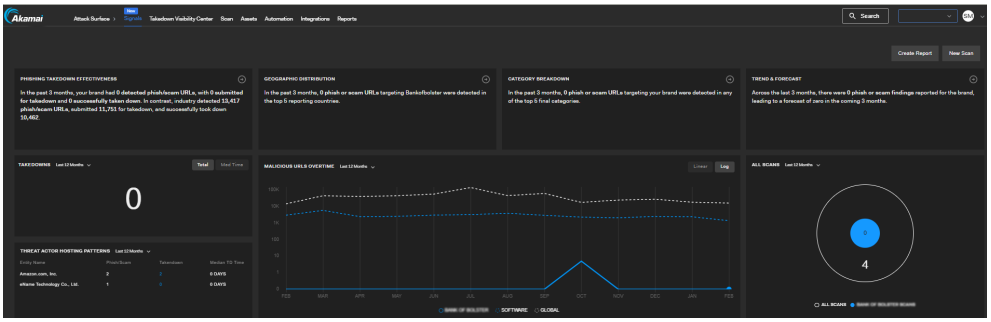
ブランド保護策の統一
セキュリティ、不正行為、法務、信頼と安全、およびマーケティングの各チーム間のサイロ化を解消し、ブランドの悪用を把握するための共通の可視性を提供します。

Akamai

Akamai Brand Guardian の保護支援策

Brand Guardian は、ブランドの悪用を、自動化、インテリジェンス、およびインターネット全体の可視性を必要とする、継続的で大規模なセキュリティ課題として捉えることで、こうした新たな現状に対処します。AI 搭載の検知機能とインターネット規模のインフラの可視化を活用することで、Brand Guardian は、ブランドを標的とした攻撃が発生したその瞬間に、組織がそれらを検知し、優先順位を付け、阻止することを可能にします。

また Brand Guardian は、顧客からの報告や手動での検索に頼るのではなく、ドメイン、Web サイト、ソーシャルメディア、アプリストア、ダーク Web ソースを網羅して、ブランドなりすましをリアルタイムで継続的に探索します。高度な分析により、低リスクのノイズと高インパクトの脅威を区別するためにシグナルを相関させ、チームが顧客と収益を危険にさらすアクティビティの対応に集中できるように支援します。



Signals ダッシュボードは、AI を活用した知見と脅威フィードを搭載しており、フィッシングやなりすましを追跡できます。

自動化された拡張可能な応答

統合されたワークフローにより、レジストラ、ホスティングプロバイダー、およびその他のオンラインプラットフォーム全体での調査、エビデンス収集、テイクダウン処理が高速化されます。実際のブランドの悪用パターンに基づいて訓練された AI モデルが、本物の脅威と正当なブランド使用を区別し、フォールス・ポジティブ（誤検知）を最小限に抑えるため、チームは重要な業務に集中できるようになります。自動化による日常的なテイクダウンでは、経験豊富なセキュリティアナリストが、人間の判断が必要となる複雑なケースに集中的に対応します。

こうした保護策を、ブランド監視の枠を超えて展開します。ブランドの脅威インテリジェンスを Akamai の幅広い DNS ポスチャおよびセキュリティ機能と統合することで、組織は外部リスクに対する統一された可視性を得ることができ、より強力なガバナンス、迅速な対応、そして経営幹部のより明確な説明責任を実現できます。

本製品の主な特長：

- **継続的なブランド悪用の探索**
  ルックアライクドメイン、フィッシングサイト、詐欺的なソーシャルプロファイル、偽アプリ、E メール、新たなデジタルチャネルの出現などのブランドなりすましを自動的に特定します。
- **AI ファーストの脅威検知**
  高度な AI を使用して、フォールス・ポジティブ（誤検知）を最小限に抑えながら、ブランドの悪用をミリ秒単位で検知します。
- **自動化された調査とテイクダウン**
  自動化されたテイクダウンのワークフローにより、レジストラ、ホスティングプロバイダー、プラットフォーム全体でエビデンスの収集と適用が高速化し、削除にかかる時間は大幅に短縮されます。

- **リスクベースの脅威の優先順位付け**
  顧客への危害、不正利用、評判への影響の可能性に基づいて脅威を順位付けし、チームが最も重要度の高いリスクに先に対処できるようにします。
- **広範なマルチチャネルの可視化**
  ドメイン、Web サイト、ソーシャルプラットフォーム、アプリストア、検索エンジン、E メール、ダーク Web ソース全体の監視を、1 つのプラットフォームから行えます。
- **統合されたブランドとセキュリティポスチャ**
  ブランド脅威インテリジェンスを Akamai の幅広いセキュリティおよび DNS ポスチャ機能と統合することで、組織は総合的なセキュリティ戦略の一環としてブランドの悪用を管理できます。

現代の不正行為の規模とスピードに対応する Brand Guardian は、インターネット上のあらゆる場所でブランドを狙う脅威から、組織が顧客を保護し、顧客離れを防ぎ、ブランドへの信頼を維持できるよう支援します。

Akamai チームにブランド評価をご依頼ください。または、akamai.com にアクセスして詳細をご確認ください。

© 2026 Akamai Technologies | サポート |
| 公開日：2026 年 3 月