AKAMAI 製品概要

Account Protector

アカウント不正利用防止機能により、犯罪者を寄せ付けずに信頼を保つ

本物のユーザーか詐欺犯罪者かをどのように判断できますか？お客様は、この 2 つを区別する上で、貴社を頼りにしています。

デジタル取引と新しいデジタル資産の普及が進むにつれ、アカウントの不正利用によるリスクと影響はこれまで以上に重大になっています。デジタルビジネスを拡大し、顧客を保護できるかどうかは、不正行為の戦術が絶えず進化している環境での信頼の維持にかかっています。

アカウント関連の不正使用、例えばアカウント開設の不正（新規アカウント詐欺）やアカウント乗っ取り（ATO）などは、全ての業界の企業にとって大きな問題であり、経済的コストも伴います。侵害されたアカウントや偽のアカウントは、組織に深刻な財務上の影響や評判への影響を及ぼす可能性があります。アカウントが侵害された場合、攻撃者は自由にそのアカウントを悪用し、残高を吸い取ったり、不正取引を行ったり、MFA などのセキュリティ機能を無効化したり、機微な個人情報を盗んだりすることができます。 一方、偽のアカウントは、無料トライアルやクレジットなどのプロモーションを活用したり、SMS ポンピングを実行したり、スパムや不適切なコンテンツをプラットフォームに大量に送り込んだりするために使用できます。これらの攻撃の影響は著しく、企業は顧客の信頼喪失、詐欺による巨額の損害、規制による罰金や評判の低下など、多くのリスクに晒されることになります。

Akamai Account Protector

Account Protector は、アカウントのライフサイクル全体にわたってアカウントの不正使用を防止するために設計された、セキュリティソリューションです。機械学習と、リスク指標および信頼指標の重要なデータセットを使用して、ユーザーリクエストの正当性を判断します。このソリューションはリアルタイムでふるまいを分析し、アカウントの作成やログインなどから発せられる不正行為のわずかな兆候を特定します。不審なふるまいや異常なふるまいが検知された場合、Account Protector はエッジでのブロックや対処、暗号チャレンジやふるまいチャレンジ、代替コンテンツなど、緩和オプションを即座に提供し、シームレスなユーザー体験を維持します。

ビジネス上のメリット

自社とユーザーの信頼性を強化
正当なインタラクションの特徴を把握して、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ります。

自社のビジネスに合わせてカスタマイズした保護策を開発
自動調整されたボット検知機能と、ユーザーとサイトのインタラクションに基づいてユーザー集団プロファイルを理解する機能を活用します。

詳細な知見と可視性
透過的な信号と指標に基づいて自信を持って行動できます。

是正措置による予期せぬ影響を軽減
侵害アカウントの調査、盗まれたアカウントの回復などの対応に伴う経済的損失やリソース不足を軽減できます。

セキュリティとアイデンティティに関する判断をデータに基づいてより適切に実施
詐欺対策ツール、SIEM、その他のセキュリティツールと統合すると Account Protector のリスクおよび信頼のシグナルをこれらのツールで使用できるようになり、ツールの精度と投資効果が高まります。

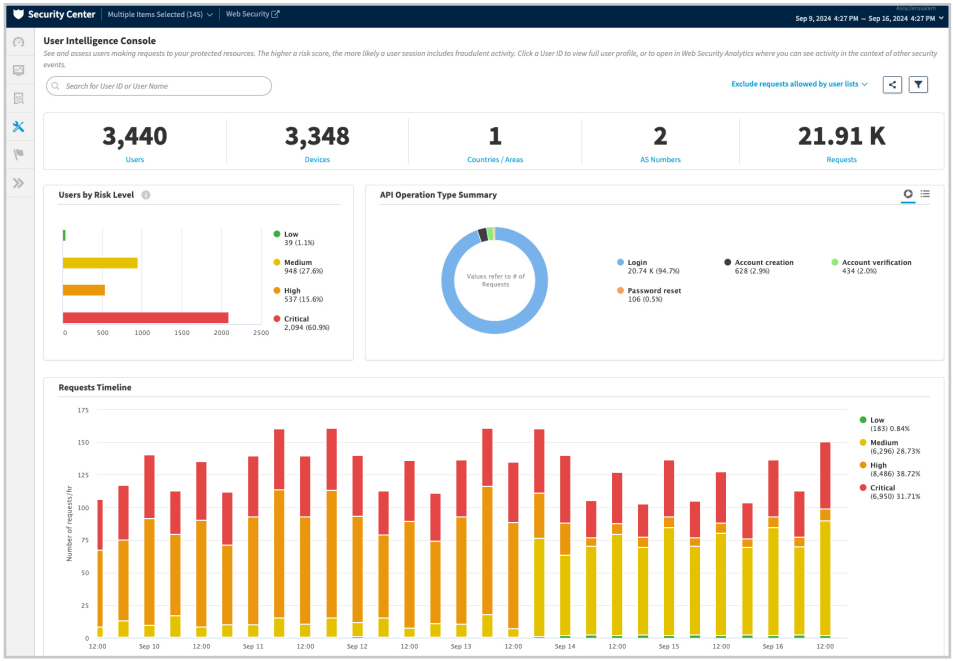
アカウントの不正使用に対する総合的な防御

ユーザーアカウントをライフサイクル全体にわたって悪用から保護し、アカウント開設の不正、アカウント乗っ取り攻撃、それによって促進される他の攻撃スキームに対する高度な保護を提供することができます。

アカウント開設の不正 — プロモーションの活用、SMS ポンピングの実行、窃取されたクレジットカード情報のテスト、インベントリの蓄積などに使用される偽アカウントの作成を緩和します。

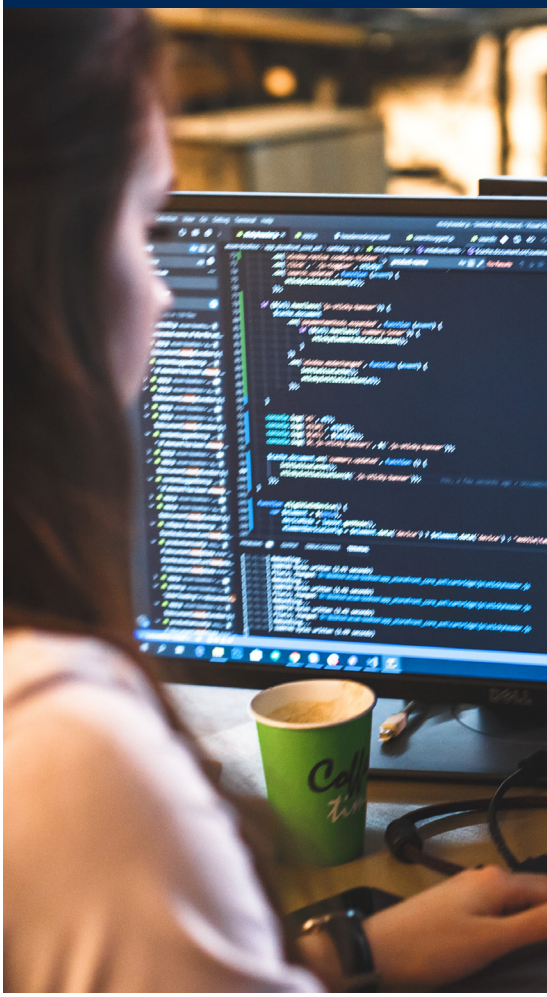
アカウントの乗っ取り — 詐欺犯罪者が正当な顧客アカウントにアクセスして、その価値を抜き取ったり、機微な情報を窃取したり、不正な取引を行ったりすることを防止します。

高度な悪性ボット攻撃 — アカウント解説の不正やアカウント乗っ取りと並行して、Credential Stuffing、インベントリ操作、その他の自動化された攻撃が実行され、価値ある製品、金銭、その他の貴重な資産が盗まれることがよくあります。それらからユーザーアカウントを保護します。



保護、信頼性、ユーザー体験

リスクを分析し、不正使用をリアルタイムで停止します。ライフサイクル全体を通じて継続的にアカウントを監視し、不審なふるまいが発生した場合の兆候を探索します。



主な機能

総合的なアカウントライフサイクル保護 — アカウントの作成からログイン後のアクティビティ（アカウントの更新、パスワードの変更、支払いなど）まで、あらゆる段階でユーザーのリスクを特定し、分析します。

リアルタイムでのユーザーセッションのリスクスコアリング — ユーザーセッション全体でリスクと信頼性を評価し、ユーザーリクエストが正当なユーザーによるものか詐欺犯罪者によるものかを見極めます。

電子メール・アドレス・インテリジェンス — 電子メールアドレスの構文と電子メールの異常使用を分析し、悪性のパターンを検知します。

E メール・ドメイン・インテリジェンス — 使い捨てドメインや電子メールドメインの過剰な使用など、個々の電子メールドメインのアクティビティパターンを評価します。

信頼できるユーザーのグローバル認識 — Akamai のネットワーク全体でユーザーのふるまいを可視化し、ログインの信頼性に関して情報に基づいた判断を行います。

ユーザーのふるまいプロファイル — 以前に観測された場所、ネットワーク、デバイス、IP アドレス、アクティビティ時間に基づいて、ユーザーのふるまいプロファイルを構築し、リピートユーザーを見極めます。

全ユーザープロファイル — 組織のユーザープロファイルを上位集合に集約します。これにより、ふるまいの差異をユーザー全体と比較して、異常検知に役立てられます。

ソースレピュテーション — 世界最大規模のトラフィック攻撃や Web サイトへの大量アクセスなど、Akamai のすべてのお客様でこれまで確認された過去の悪性のアクティビティに基づいて、ソースのレピュテーションを評価します。

指標 — リスク指標、信頼指標、一般的な指標を使用して各リクエストの評価を行い、アカウント不正使用のリスクを評価します。これらの指標は、最終的なユーザーリスクスコアとともに提供され、分析に使用できます。

高度なボット検知機能 — 多様な AI／機械学習モデルやテクニックを活用して、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します。たとえば、ユーザーのふるまい／テレメトリー分析、ブラウザーフィンガープリンティング、ブラウザーの自動検知、HTTP 異常検知、高リクエスト率などが活用されています。

分析とレポート — リアルタイムレポートと履歴レポートの両方を提供します。個々のエンドポイントのアクティビティを分析して、特定のユーザーを調査し、リスクレベルごとにユーザーをレビューして、深い知見を得ます。

高度な応答アクション — アラート、ブロック、遅延、暗号チャレンジやふるまいチャレンジ、代替コンテンツなど、さまざまなアクションを適用して不正行為を阻止できます。さらに組織は、URL、時間帯、ジオロケーション、ネットワーク、トラフィック率に応じて多様なアクションを割り当てられます。

ヘッダーインジェクション — 分析およびリアルタイムの緩和のためにユーザーリスク情報を送信します。 転送されたリクエストに追加のリクエストヘッダーを挿入し、ユーザーのリスクスコア、リスク指標、信頼指標、一般的な指標など、詳細な分析とリアルタイムの緩和に役立つ情報を提供します。

機械学習による自動化 — Akamai プラットフォーム全体でのふるまいパターンや最新のレピュテーションスコアなどを利用して、人間による不正行為とボットの特定に使用する特性とふるまいを自動的に更新します。

SIEM 統合（オプション） — セキュリティの総合的な可視性を高めたい場合は、SIEM ツールにユーザーのリスク情報を統合します。Account Protector から得られた知見を活用して、既存のツールの価値を高めることができます。

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。