行動バイオメトリクス: 生産性を損なわずに不正の阻止を支援

IBM Security Trusteer Pinpoint Detect により不正対策を強化でき、処理時間の短縮も可能

ハイライト

- 機械学習を活用してコグニティブ技術による不正検知と動的な本人確認を実行
- リアルタイム・インテリジェンス・サービスによって不正を検知し誤検知を削減
- ログイン時に顧客本人と不正利用者を区別するために機械学習処理を採用
- 不正のライフサイクル全体で不正を正確に特定して防止するため簡略化されたアプローチを採用

金融機関は、オンライン・バンキング・システムを使用する顧客本人と不正利用者の区別を確実に行えるでしょうか。顧客は、オンライン・バンキングを素早く、簡単に、効率的に操作できることを期待しています。金融機関が、ユーザーが本人であることを信頼性の高い方法で確認できれば、ユーザーがアカウントにアクセスする際の面倒な認証手続きが不要になります。IBM® Security Trusteer® 行動バイオメトリクス機能は、生産性を損なうことなく、不正を阻止できます。

従来型の物理的生体認証では、ユーザーの身体的特性に重点を置き、音声識別、指紋照合、網膜スキャン、顔認識テクノロジーなどの機能を使用します。固有の身体的属性はアカウントの資格情報ほど簡単に盗み取ることができないという理論に基づいて、物理的生体認証が実施されます。このタイプのテクノロジーは効果がありますが、制約もあり、また認証プロセスに余分なステップが追加されることもあります。例えば網膜スキャナーと指紋スキャナーを実装すると、多額のコストがかかる可能性があり、また顔の特徴は時間がたつと変わっていくため、認識テクノロジーの正確さが低下します。しかし行動バイオメトリクスでは、本人であることの証拠を要求するのではなく、*行動*を分析することによって、顧客を識別します。

例えば IBM Security Trusteer Pinpoint™ Detect が提供する行動バイオメトリクス機能は、微細なマウスの動きを識別し、追跡します。そのようにして、複数のセッションにわたって各顧客の行動を継続的に学習し、その行動を分析します。これにより銀行は、認証プロセスを簡素化してシームレスなユーザー・エクスペリエンスをもたらし、その一方で、不正なアクティビティーを検知して抑制する能力を強化できます。

ユーザー本人と不正利用者を正確に区別

金融機関では、お客様に満足していただくことが最優先事項です。金融機関は、顧客の安全を維持すると同時に、認証プロセスが煩雑にならないように、常に努力しています。行動バイオメトリクスは、その目的に適合する非侵襲的な検証方式です。保護層を追加しますが、顧客が余分なステップを実行する必要はありません。毎年、金融機関にとって金融詐欺が絶えずリスクになっていることが報告されています。IBM X-Force® は、「2015 年には、IBM Security Services がモニタリングしていた平均的なクライアント組織で、1 年間におよそ 5300 万回のセキュリティー・イベントが発生しました」と報告しています。[1] 2015 には、「銀行口座へのオンライン・アクセスを通じて金を盗むことを目的としたマルウェア感染が試みられたことに関する通知が、1,966,324 件登録されました。」[2] 銀行によって、設定が面倒な厳格なパスワード規則を追加したり、E メールまたは SMS メッセージを通じてワンタイム確認コードをプッシュしたりしています。このような認証方式も効果はありますが、ログイン・プロセスにかかる時間が長くなり、オンライン・バンキングの利便性が低下して、ユーザー・エクスペリエンスに影響します。Trusteer Pinpoint Detect では、ユーザー・エクスペリエンスに対してシームレスな、追加の保護層を提供します。

行動バイオメトリクスは、顧客からは見えません。ユーザー・エクスペリエンスの妨げになることも、新しいログイン・ステップが追加されることもありません。オンライン・バンキングのやり取りの時間が長くなることも、停止することもありません。代わりに、このソリューションの行動バイオメトリクス機能では、機械学習と自然言語処理を利用した、コグニティブ技術による不正検知と、ログイン時に顧客と既知の不正利用者を識別する動的な身元評価を実行します。マウスの動きを理解して顧客がどのようにオンライン・アカウントとやり取りするかを対応付けて、異常な行動を検知しようとします。

これは金融機関とユーザーに対してどのような意味を持つでしょうか?

顧客本人の行動を既知の不正利用者と区別できれば、不正防止に非常に役立ちます。不正利用者とサイバー犯罪者は、ユーザー情報を盗むことはできますが、顧客の身体的動作を正確に再現することは容易ではありません。そのため、金融機関はお客様のリスクを軽減することができます。行動バイオメトリクスのセキュリティー指標を導入し、利用し、分析することで、エンド・ユーザーにそれほど影響することなく、強力なユーザー本人確認が可能になります。[3]

Trusteer 行動バイオメトリクスは、金融機関がエンド・ユーザーに影響を与えずに、不正を検知し、誤検知を減らし、セキュリティー・アラート・レートを低減できるようにする、基本的に異なるアプローチを提供します。ユーザーの固有のリスク指標と、Trusteer Pinpoint Detect が提供する行動バイオメトリクス機能を組み合わせることで、可視性、グローバルな脅威情報ネットワーク、および意図的な俊敏性という 3 つの中核となる原則に基づいた、不正検知に対する IBM のアプローチの強みが明らかになります。

可視性

Trusteer Pinpoint Detect の中核となるのは、フィッシング攻撃、マルウェア感染、危険にさらされた資格情報、高度な回避手段を検知するためのさまざまな重大不正行為指標を、拡張デバイス、地理位置情報、およびトランザクション・モデルに関連付けて、不正行為をさらに正確に検知できるようにするエンジンです。

グローバルな脅威情報ネットワーク

不正との戦いにおいて、情報収集の深さとスピードが非常に重要です。IBM X-Force のグローバルな脅威情報ネットワークは、何億ものエンドポイントからの情報を分析します。このネットワークは継続的にセキュリティー情報を処理し、X-Force がその情報を使用して動的なデジタル・モデルを作成します。この情報を武器として、Trusteer の脅威分析者は、最先端のアナリティクス・テクノロジーを使用して業界固有ならびに組織固有の脅威を研究および調査します。これにより、金融機関は自動更新を通じて防御をより効果的にすることができますが、組織の該当部分で追加の作業は発生しません。Trusteer Pinpoint Detect は、多数のセッション属性、データ、および不正の指標を含むこの情報を利用して、莫大なデータ・セット内で正確に不正を特定します。

意図的な俊敏性

サイバー犯罪の防止には、時間が極めて重要な要素であるため、Trusteer Pinpoint Detect は、非常に柔軟で迅速な対応プロセスを可能にするアジャイル・アーキテクチャーを備えています。クラウド・ベースのテクノロジーを使用するこのソリューションによって、新たに出現した脅威を迅速に検知して分析し、脅威に対する対策を構築して導入することができます。また、金融機関は自らのニーズと自らが直面している脅威に合わせて特別に調整された、アプリケーション認識型の防御策を利用することもできます。この機能は、検知の正確さをさらに高めることができ、運用コストの削減に役立つように設計されています。

IBM をお勧めする理由

IBM Security プラットフォームは、組織が顧客、データ、アプリケーション、インフラストラクチャーをセキュリティーの脅威から全体的に保護するために役立つセキュリティー情報を提供します。IBM では、ID とアクセス管理、セキュリティー情報とイベント管理、データベース・セキュリティー、アプリケーション開発、リスク管理、次世代の侵入防御策などのためのソリューションを用意しています。世界で最も幅広くセキュリティー関連の調査と開発を行っている組織の 1 つを、IBM が運営しています。

詳細情報

IBM Security Trusteer Pinpoint Detect の詳細については、IBM 担当員または IBM ビジネス・パートナーにお問い合わせいただくか、www.ibm.com/security/jp-ja/trusteer/behavioral-biometrics/ をご覧ください。

さらに、IBM グローバル・ファイナンシングはお客様のビジネスの成長に必要なテクノロジーの取得を支援するため、さまざまな支払いオプションをご用意しています。IBM は IT 製品およびサービスの取得から処分まで、全ライフサイクルの管理を提供します。詳細については、次の Web サイトをご覧ください。**ibm.com**/financing/jp

IBM Security

東京都中央区日本橋箱崎町 19 番 21 号

Produced in Japan
October 2016

Please Recycle

[1] "Reviewing a year of serious data breaches, major attacks and new vulnerabilities," IBM Corp., April 2016. https://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03133usen/SEW03133USEN.PDF

[2] "Kaspersky Security Bulletin 2015: OVERALL STATISTICS FOR 2015," Kaspersky Labs, 2015. https://securelist.com/files/2015/12/KSB_2015_Statistics_FINAL_EN.pdf

[3] "Why adopt behavioral biometrics as part of your multi-modal strategy," Zighra, June 22, 2015. http://www.zighra.com/blog/behavioral-biometrics-and-multi-modal-biometrics

WGS03090-JPJA-00