セキュリティー
ソート・リーダーシップのホワイト・ペーパー

October 2016

コグニティブ技術による不正検知
金融犯罪を阻止する有効な一手に

IBM

目次

概要

戦いにおいては、多くの場合、正当な方が優位に立って敵を圧倒することになる転換点があります。不正利用者と戦う金融サービス・プロバイダーの場合、IBM Trusteer のコグニティブ技術による不正検知を使用することで、その転換点に到達できます。

複雑なデバイス ID、マルウェア検知、トランザクション・モニター、および生体認証システムなどの、不正に対抗する従来型の保護ソリューションはすべて一定レベルの保護を提供し、オンライン・バンキング・システムにログインしてきた「顧客」が申告どおりの人物であることを、金融サービス・プロバイダーが確認できるようにします。

ただし個別の方法では、力の及ぶ範囲は限られており、提供できるのは必要なデータの一部分です。結果として、セキュリティー・アナリストは多くの場合、誤検知を丹念に調べ、データの意味を手動で評価しようとする作業に忙殺されます。多くのセキュリティーの専門家が、不正利用者に「防御が追い付かない」と感じるのも無理はありません。[1]

コグニティブ技術による不正検知は、機械学習によって、これまでにないスピードと規模で非構造化データと構造化データの両方を理解するものです。データの意味を理解し、やり取りがあるたびに学習するため、毎回判断力が高まります。また、エンド・ユーザーに対して透過的であるため、ユーザー・エクスペリエンスを損なうことはありませんが、不正利用者がこれを回避するのは困難です。

さまざまなセキュリティー層にわたってコグニティブ技術による不正検知を使用することで、金融サービス・プロバイダーは、これまでになく正確かつ迅速に不正を検知でき、同時により良いユーザー・エクスペリエンスを維持できます。

このホワイト・ペーパーでは、不正との戦いをさらに支援し、常に進化し続ける脅威に対して金融サービス・プロバイダーが優位に立てるようにするために IBM® Trusteer® ソリューションが提供する、行動バイオメトリクス、行動分析、および適応型インテリジェンスという 3 つの主要なコグニティブ技術による不正検知機能について説明します。これらの機能は、完全に統合されており、IBM Research ラボで開発された特許取得済みの認識テクノロジーを組み込んでいます。

行動バイオメトリクスによる継続的で透過的な検知の実現

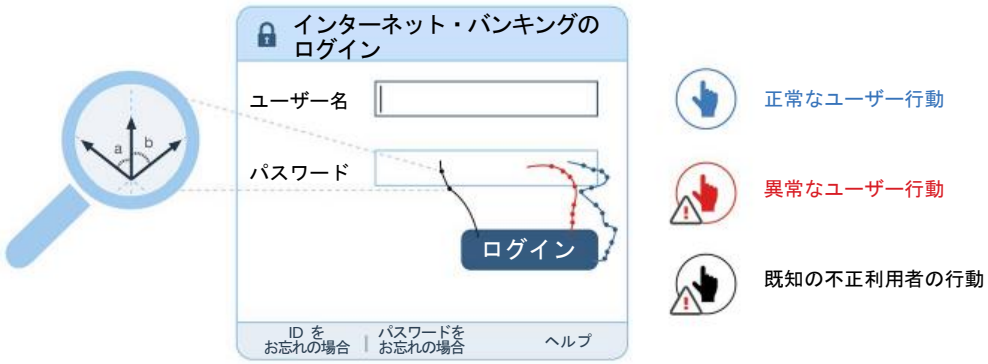
不正検知の基本的な目的は、不正利用者がユーザー本人になりすましたときに、リアルタイムでそれを発見できるようにすることです。ただし、そのためには、アカウント・ユーザーの「正常な」デジタル行動を異常な行動と区別できなければなりません。

IBM Security Trusteer Pinpoint™ Detect は、行動バイオメトリクス機能を組み込んで、コンテキストを意識した動的な身元分析を行うようになりました。この分析によってユーザー・エクスペリエンスを維持しながら検知の精度を高めることができます。

IBM Research ラボと共同で構築されたこのソリューションの行動バイオメトリクス機能は、機械学習を行って、ログイン以降のアプリケーション・フロー全体でのマウスの動きのパターンに基づいてモデルを作成します。

ユーザーのマウスは、どのような角度でログイン・ボックスに近づきますか? ユーザーは通常どの方向にマウスを動かしますか? マウスの軌跡、速度、曲率、急な動きなどがすべて分析されます。

このプラットフォームは、驚くべきスピードとボリュームで、コンテキストと意味においてこれらの微細なマウスの動きを理解します。何億ものセッションにわたってユーザーの行動を継続的かつシームレスに学習し、現在のオンライン・アクティビティーを分析して、さまざまなデバイスで異常な行動を検知します。また、観測された既知の不正利用者の行動と比較して、さらに強力な証拠とします。プラットフォームの高度なアルゴリズムによって異常なユーザー行動または既知の不正利用者の行動が検知された場合、Trusteer Pinpoint Detect は、アクセス管理システムおよびセキュリティー・アナリストを提供し、また推奨される対策を詳細な理由およびセッションの詳細情報と共にリアルタイムで提供し、対策を実施できるようにします。



IBM Security Trusteer Pinpoint Detect では、行動バイオメトリクス機能を導入してコグニティブ技術による不正検知を実施します

その結果、サービス・プロバイダーは、複数のデバイスにわたってリアルタイムでユーザーをより正確に確認し、一方で強力な認証層を最適化してユーザー・エクスペリエンスを向上させることができます。また、行動バイオメトリクス分析が受動的でシームレスな方法であることから、従来の方法と比べて不正利用者が回避するのは非常に困難になっています。見えないものと戦うのは難しいためです。

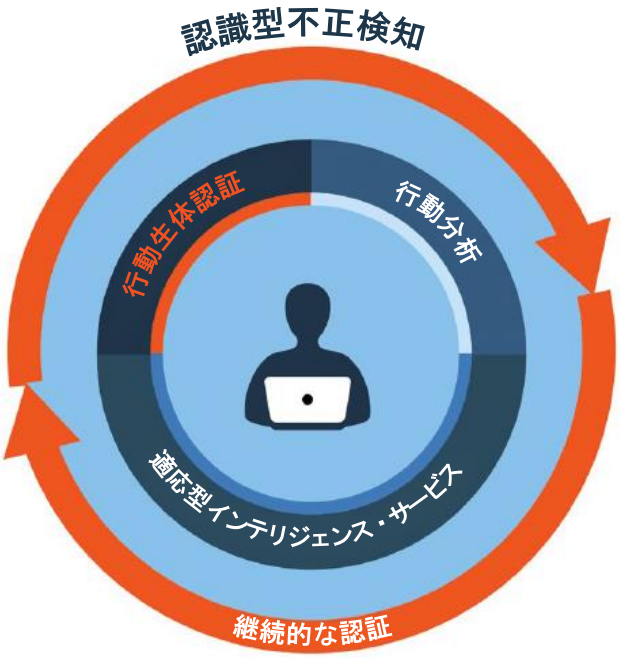
行動分析による実態の把握

行動バイオメトリクスにより、エンド・ユーザーへの影響を最小限にして強力なユーザー認証確認が実施されますが、パズルのピースはほかにもあります。

不正検知では、分析されるデータの量と品質が非常に重要です。データの量が増えれば、不正なアクティビティーと正当なアクティビティーをさらに正確に区別できるようになります。

そのため、マウスの動きのパターンを分析する行動バイオメトリクスに加えて、Trusteer Pinpoint Detect では、デジタル・バンキング・アプリケーションへのすべてのアクセスにおける、デバイス・アクティビティー、トランザクション・データ、地理位置情報データなどの、他の多くの行動指標も分析して、チャネル間でのユーザー、デバイス、セッションの異常を把握します。

このような行動バイオメトリクス分析から得られた知見を、行動バイオメトリクスの結果や、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、リモート・アクセス型のトロイの木馬 (RAT)、および高度な回避手段といった重要な不正指標と相互に関連付けて、脅威の性質と潜在的なリスクの両方を非常に確実に判別できるようにしています。



IBM Trusteer のコグニティブ技術による不正検知

リスクのデータと、そのすべてを理解する統合済みのロジックの組み合わせにより、アプリケーションは効果的にリスクを管理することができ、エンド・ユーザーの操作中に認証を許可するか、制限するか、強化するかをコンテキストを意識して決定するように、ロジックをリアルタイムで修正することができます。

進化する脅威を適応型インテリジェンスにより早期に発見

不正に効果的に対処するには、検知、調査、対策導入のスピードが非常に重要です。IBM のグローバルな脅威情報ネットワークは、何百万ものエンド・ユーザー・エンドポイントやその他のソースから脅威情報を収集します。この情報を武器にして、IBM Trusteer の脅威分析者は、業界や組織に固有の脅威を研究および調査してから、自動的に防御策を修正することができます。金融機関で追加的な作業は発生しません。

この作業を簡単にするため、IBM の専任の研究開発チームが、適応型インテリジェンス・システムを用いて、ユーザーの異常を検知するだけでなく、進化する脅威を理解して優先順位を付けます。

機械学習機能を利用するこの認識システムは、毎日その脅威ネットワークに流れてくる何百万ものデジタル・バンキング・セッションを分析して、新しい脅威パターンと防御ロジックを合成します。例えばシステムは、人間には処理できない量である丸 1 日分の記録 (数百万のセッション) から迅速にデータを選び取り、Web インジェクションを発生時に発見し、IBM セキュリティー研究者にアラートを送ります。

まとめ

IBM Trusteer は、不正からの保護とサービス・オファリングにおける認識機能を統合して、行動バイオメトリクス、行動分析、および適応型インテリジェンスを使用できるようにすることにより、パワー・バランスをシフトさせ、金融サービス・プロバイダーが不正利用者との戦いで優位に立てるようにします。

IBM のコグニティブ技術による不正検知機能は、人間には不可能なスピードと規模で非構造化セキュリティー・データを分析し、継続的にデータから学習することができるため、顧客が本人であるかどうかをより正確かつ透過的に判別し、新たなオンライン・バンキングの脅威が出現したときにそれを検知できるように、金融サービス・プロバイダーを支援します。

IBM では、さまざまなデータを包括的なリスク評価と相互に関連付ける多層構造のアプローチを提供しており、対応の時間短縮と効率向上のために、組織が直面する誤検知の数を減らすことができます。

詳細情報

コグニティブ技術による不正検知の詳細については、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、次の Web サイトをご覧ください。
www.ibm.com/security/jp-ja/trusteer/behavioral-biometrics/

適切なセキュリティーの実施について: IT システム・セキュリティーには、企業内外からの不正アクセスの防止、検知、および対応によって、システムや情報を保護することが求められます。不正アクセスにより、情報の改ざん、破壊もしくは悪用を招くおそれがあり、またはシステムの損傷や、他のシステムへの攻撃を含む悪用につながるおそれがあります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービスまたはセキュリティー対策が、不正アクセスを防止する上で 完全に有効となることもありません。IBM のシステム、製品およびサービスは、合法的で包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

[1] "Fortifying for the future: Insights from the 2014 IBM Chief Information Security Officer Assessment" IBM Center for Applied Insights, December 2014. P.5
http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03061USEN

IBM Security

東京都中央区日本橋箱崎町 19 番 21 号

Produced in Japan
October 2016

本書の情報は最初の発行日の時点で得られるものであり、予告なしに変更される場合があります。すべての製品が、IBM が営業を行っているすべての国において利用可能なのではありません。

本書に含まれるパフォーマンス・データは、特定の動作および環境条件下で得られたものです。実際の結果は、異なる可能性があります。IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

本書に掲載されている情報は特定物として現存するままの状態で提供され、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されています。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。

お客様は自己の責任で関連法規を遵守しなければならないものとします。IBM は法律上の助言を提供することはいたしません。また、IBM のサービスまたは製品が、お客様がいかなる法規も遵守されていることの裏付けとなると表明するものでも、保証するものでもありません。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

Please Recycle

WGW03249-JPJA-00