データシート

Outseer Fraud Manager™

ログインから支払いまでのアカウント保護

OUTSEER

Stop Fraud Not Customers®

概要

- 毎年1,200億件を超えるトランザクションとデジタルインタラクションを保護します
- 年間5兆ドルを超える決済取引を保護します
- すべてのデジタルチャネルにおいて、ログインから支払いまでユーザーのデジタルジャーニー全体を保護します
- わずか5%の介入で95%の不正行為を阻止します
- 柔軟な展開オプション：オンプレミスまたはクラウド

1つのソリューションでログインから取引まであらゆる部分を完全に保護します

デジタルバンキングやオンライン決済の急速な変化とリアルタイム決済 (RTP) の浸透により、不正行為者にとって悪用しやすい脆弱性が露呈しています。不正行為者は詐欺防止戦略の一番の弱点を探しており、サイロ化した状態における詐欺との戦いは防御を弱めます。デジタルジャーニーの各段階においてリスクシグナルの点と点を結ぶことで、お客様の組織は顧客のアカウントを保護しながら、顧客にふさわしい優れたユーザーエクスペリエンスを提供する完璧なバランスを実現することが可能です。

特にRTPの急増は、不正行為者がこれらの決済レールのスピードを悪用し、素早く現金を引き出すという脅威を高めています。詐欺やAPP (Aurhorized Push Payment) が増加する中、アカウント乗っ取りは依然として重要な脅威経路です。実際、最近の[Datos Insights]による調査では、不正対策幹部の71%が、RTPレールを介したアカウント乗っ取り攻撃が増加していると指摘しています。ログインからトランザクションまでの点と点を結び、顧客のデジタルジャーニーの各ステップのリスクを総合的に評価することは、これまで以上に重要になっています。

卓越したデータサイエンスによる卓越した結果

- 最高の脅威環境で実証されたインサイトを活用します
- 独自のコンソーシアムデータで最新の詐欺トレンドから防御します
- 世界最大規模の金融機関における数兆件の取引でトレーニングされたリスクモデルのメリットを提供します

顧客のジャーニー全体で1つの不正管理プラットフォームを活用する

- 認証と決済トランザクションにまたがるインサイトを結びつけます
- ファーストパーティおよびサードパーティのデータシグナルを取り込むことで、リスクスコアリングを改善します
- あらゆる顧客接点において一貫したリスク軽減のコントロールとエクスペリエンスを提供します

カスタマーエクスペリエンスと業務効率を最適化する

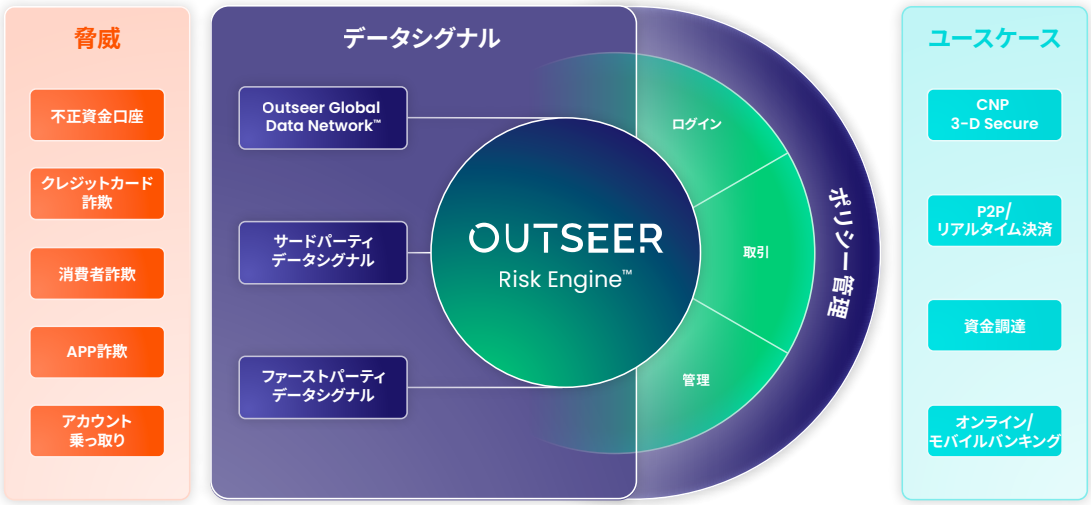
- 正規化されたリスクスコアを使用して、不正行為、カスタマーエクスペリエンス、運用コストのバランスをとります
- 進化し続ける脅威に対応したポリシー変更を実施します
- 継続的な改善とピアベンチマーキングのために専門家とのコラボレーションを行います

[1] Datos Insights（旧Aite-Novarica）。「迅速な決済、迅速な詐欺：狂気を止める解決策」https://www.outseer.com/aite-faster-payments/、2023年5月

顧客のデジタルジャーニーのあらゆるステップを保護するお手伝いをします

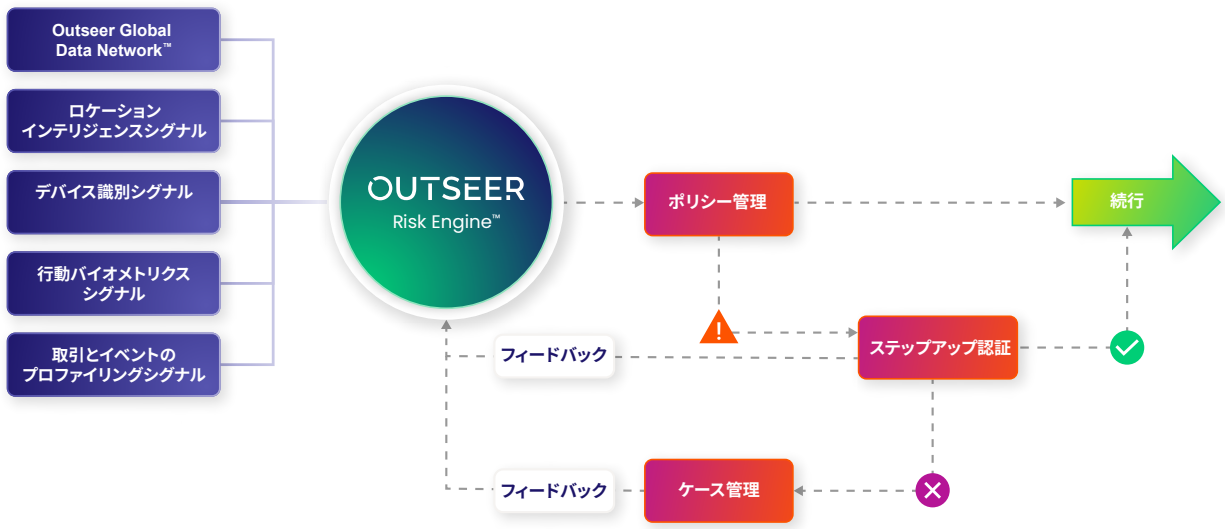
Outseer Fraud Managerの基盤となるOutseerプラットフォームは、実績あるトランザクションリスク管理プラットフォームとして、ログインから支払い完了までデジタルトランザクションのあらゆる部分を一貫して保護することを可能にします。Outseerのお客様は卓越した消費者エクスペリエンスを維持しながら、業務の合理化、アカウント乗っ取りリスクの低減、不正による損失の低減を全て実現し、利益を得ています。

Outseerプラットフォームは、Outseer Risk Engine™によって支えられています。正確な検知のために構築されており、最も効果的なモデルとデータを活用して不正なアクティビティを検知し防止します。当社の予測アルゴリズムは、取引データ、Outseer Global Data Network™からの当社独自のコンソーシアムデータシグナル、そしてファーストパーティとサードパーティのシグナルを分析し、リアルタイムかつ大量規模で機能します。当社のリスクモデルは、世界最大規模の金融機関における数十億件の取引でトレーニングされています。



仕組み

Outseer Fraud Managerには、ユーザーのデジタルジャーニーにおける各取引やデジタルインタラクションに関連するリスクを正確に評価するOutseer Risk Engineが搭載されています。リスクベースのアプローチを適用することで、追加の認証を必要とする活動やトランザクションはごく少数となり、必要となった場合にはすぐに使える一貫したステップアップ認証オプションを使用するか、組織の認証ツールを活用して行うことができます。



Outseer Risk Engine

当社の革新的なテクノロジープラットフォームの中核であるOutseer Risk Engineは、高精度の検出を可能にするために構築されています。当社の実績あるリスクモデルは、最高のリスクスコア精度を提供するために数兆件の取引でトレーニングされています。Outseer Risk Engineは、取引データ、Outseer Global Data Network、サードパーティデータ、そしてファーストパーティデータから得られる何百ものシグナルを分析し、予測アルゴリズムを用いてリアルタイムで不正を検知し防止します。リスクスコアの計算には高度な機械学習統計的アプローチを使用しており、各事象の条件付き確率を調べ、既知の事実や予測因子に基づいてそれが本物である可能性が高いか、不正行為の可能性が高いかを評価します。利用可能なすべてのシグナルが考慮されますが、これらは不正行為との相関性に応じて重み付けされます。したがって、予測性の高いシグナルほどスコアへの貢献度が高くなります。予測の重み計算は、認証結果とケース管理のフィードバックに基づいて、各顧客ごとに更新されます。ブラックボックス型のリスクエンジンとは異なり、Outseerは説明可能な結果を得るために、スコアの上位貢献要因の理由コードを提供します。正規化されたリスクスコアが提供する予測可能性によって、お客様は自信を持ってビジネス目標とリスク許容度に見合ったリスクスコアのしきい値を選択できるようになります。

Outseer Global Data Network

Outseer Fraud Managerは、Outseer Global Data Network（世界中の何千もの金融機関のトランザクションからデータを収集する、グローバルに共有された不正行為インテリジェンスコンソーシアム）によって提供されるデータシグナルから独自のメリットを得ています。ネットワークのメンバーがケース管理アプリケーションでアクティビティを「不正確認済み」または「本物確認済み」とマークすると、これに関連する信号がネットワーク全体に共有されます。試行されたアクティビティにOutseer Global Data Networkからのシグナルが含まれる場合、リスクは自動的に調整され、さらにOutseerのお客様は、「このシグナルがGlobal Data Network内にあるかどうか」などの事実を活かしたルールを定義することができます。

デバイスのプロファイリング

Outseerのデバイスプロファイリング機能により、顧客のデバイスがお客様の組織とのやり取りに常用されているものと異なるかどうか、または既知の不正行為に関連しているかどうかを評価することができます。この評価では、IPアドレス、ジオロケーション、オペレーティングシステム、ブラウザーの種類、その他のデバイス設定などのパラメーターが分析されます。多くの場合、アカウント乗っ取り攻撃は、不正行為者が所有するデバイスから被害者のユーザー認証情報を使って行われます。したがって、アカウント乗っ取りを軽減するためには、ユーザーの既知のデバイスの正確な識別とプロファイリングが鍵となります。Outseerのデバイスプロファイリングとデバイス識別機能は、教師なし機械学習アルゴリズムを使用して、ユーザーが過去にそのデバイスを使用した確率を反映した正確な保証レベルを計算します。

行動分析学によるプロファイリング

当社の行動プロファイリングは、現在のセッション活動と確立された顧客行動を比較して、不正行為を示す可能性のある逸脱行動を検出します。これには頻度、時間帯、活動の種類など、複数のシグナルが考慮されます。（例：これらの支払タイプと関連する取引属性がこのユーザーの典型的な取引と一致しているかどうか。）

モバイルユーザーの保護

Outseer Fraud Managerは、iOSとAndroidデバイスの両方で利用できるOutseer Fraud Manager Mobile SDKを活用することで、安全で摩擦のないモバイルエクスペリエンスを可能にします。このSDKは、お客様のモバイルアプリケーションと統合し、リスク評価のためにモバイルデバイス識別子を収集し、フラグが付けられたトランザクションにはステップアップ認証としてバイオメトリクス認証とOTPプッシュ通知を呼び出します。

Outseerのケース管理

当社のケース管理アプリケーションを使用して、ポリシーをトリガーする活動を監視し、それが不正かどうかを確認することができます。また、さらに詳しく分析するために、攻撃ベクトルに基づいてアクティビティにタグ（例えば詐欺/非詐欺など）を付けることもできます。ウェブベースのアプリケーションを使用することで、例えばポリシーを改訂したり新規ポリシーを開発したりする際に、活動の調査や不正行為のパターン分析を行うことが可能になります。不正であることが確認されたケースは、即座にOutseer Risk Engineにフィードバックされ、リスク分析の精度をさらに高めることができます。また、サードパーティのケースデータを利用したり、サードパーティのケース管理アプリケーションにケースやアクティビティをエクスポートしたりできるAPIも用意されています。

ポリシー管理

Outseerのポリシーエンジンは、データシグナルとリスクインテリジェンスをアクションに変換します。きめ細かなポリシー制御によって、お客様のリスク許容度とビジネス目標に基づき、各リスクしきい値ごとに異なる結果を設定することができます。ウェブベースのOutseer Fraud Managerのポリシー管理アプリケーションでは、支払い時、ログイン時、またはユーザーがアカウント設定を管理している時にのみ発動するポリシーなど、イベントレベルのポリシーを設定できます。ポリシーの定義にコーディングは必要ありません。ポリシーロジックの一部として含めたい要素をクリックして選択するだけです。

オーケストレーション機能

Outseerのプラットフォームは、不正行為の管理を一元化し、さまざまな不正防止ツールへの投資を最大限に活用して不正行為の検知を強化することで、お客様の組織における不正防止と認証の取り組みを支援します。当社のプラットフォームは、顧客のジャーニーでさまざまなアクションにつながる各種の事象に対してきめ細かいポリシーを設定し、ファーストパーティやサードパーティのシグナルを活用するための柔軟性を提供します。Outseerプラットフォームには、他のベンダーと以下のような統合を可能にするインターフェイスが用意されています。

- サードパーティシグナルをOutseer Risk Engineのリスクスコア計算に加味する
- サードパーティシグナルをポリシー管理アプリケーションに送る
- サードパーティのステップアップ認証オプション

ステップアップ認証

リスクの高いシナリオや組織のポリシーに違反するシナリオでは、ステップアップ認証のレイヤーを追加して本人確認をさらに厳しくすることができます。

チャレンジクエスチョン：エンロール時にユーザーが問題を選択し、回答を設定します。

帯域外認証：テキストメッセージ、電話、プッシュ通知でユーザーにワンタイムパスコードを送信します。

バイオメトリクス：モバイルオペレーティングシステム技術に基づく指紋や顔のIDバイオメトリクスで、モバイルアプリケーションユーザーを対象とします。

トランザクション署名：高度な金融マルウェア攻撃に対抗するため、トランザクションの詳細に暗号署名をしてトランザクションの完全性と真正性を検証します。

認証オーケストレーションフレームワーク：外部認証のために、トークンやFIDO準拠のバイオメトリクス認証、パスワードレス認証など、独自の認証方法を使用できます。

実証済みの不正行為管理プラットフォームで不正行為の防止活動を合理化します

Outseer Fraud Managerは、サイエンス主導型イノベーションのパイオニアとしての伝統を活かし、リスク管理と不正防止のソリューションを支援します。お客様はOutseerの卓越したデータサイエンスを利用して、カスタマーエクスペリエンスと業務効率を最適化しながら、不正行為による損失を削減することができます。

Outseer Fraud Managerは、認証と支払いトランザクション全体のインサイトを合理化すると同時に、すべての顧客接点において一貫したリスク管理を実現します。お客様が他の不正ツールへの投資を活用するお手伝いをし、ファーストパーティとサードパーティのデータシグナルを1つのスコアに統合した、より高度なリスクスコアを提供します。当社の正規化されたリスクスコアによって、不正行為、カスタマーエクスペリエンス、運用コストのバランスを予測することができます。その結果、お客様は急速に進化する不正行為のトレンドや規制要件に対応し、ポリシーの変更を迅速に展開することができるようになります。

Outseerについて

Outseerは、顧客ではなく不正行為をシャットアウトするソリューションを提供することで、お客様がデジタル不正行為を世界から追放するためのお手伝いをします。市場をリードするOutseerの不正防止・認証プラットフォームは、世界中の何千もの金融機関に利用され、年間何百万もの顧客口座と何十億もの取引を保護しています。当社独自のコンソーシアムデータを含む実証済みのデータサイエンスを活用することで、お客様は当社のリスクベースの機械学習プラットフォームを使用して、業界で最高の不正検出率と最小の誤検出率、そして最も低い顧客介入率を実現しています。他のソリューションでは見えないものを**outseer.com**でご覧ください。