IBM Security Trusteer Fraud Protection Suite

IBM ソリューションにより、不正行為の迅速かつ効率的な検出、対策、調査、修復を実現できます

ハイライト

- IBM® Security Trusteer® Pinpoint™ Detect が備える、証拠に基づく不正検出機能を使用して、誤検出を大幅に削減しながら不正を検出します
- IBM Security Access Manager 1 が備える脅威認識型認証機能を使用して、実際のリスクに基づく迅速な対策を可能にします
- IBM Counter Fraud Management 1 が備える拡張事例管理およびレポート作成機能を使用して、調査および脅威分析を合理化します
- IBM Security Trusteer Rapport® for Mitigation が備える強力な修復機能を使用して、感染したエンドポイントから既存の金融マルウェアを迅速に除去します

組織は Trusteer Pinpoint Detect を購入して特定の不正検出の問題に取り組み、その後必要に応じて組み込みの統合を使用し、対策、調査、修復のレイヤーを追加できます。こうした統合によって、不正管理のライフサイクル全体で情報を容易に共有できるようになり、管理にかかる初期コストと運用コストの両方を削減できます。

IBM Security Trusteer Fraud Protection Suite は、より正確な不正検出を実現し、さらには対策、調査、修復に関する IBM のソリューションとの統合を簡略化します。結果として、不正管理のライフサイクル全体で可視性と順応性を向上することができます。

- このスイートは、誤検出の少ない、非常に効果的なインテリジェンスおよび証拠に基づく不正検出を実現します。
- IBM Security Access Manager との統合を介して、統計上のリスクではなくエンド・ユーザーの実際のリスクに基づいて、対策に関する顧客の負荷を軽減できます。
- IBM Counter Fraud Management との統合を介して、調査、事例管理、および修復にかかる時間とコストを減らすことで、作業効率を改善できます。
- 感染した顧客のエンドポイントから既存の金融マルウェアを除去できます。
- 簡略化された統合により、不正管理のライフサイクル全体で運用コストを削減できます。

最後に、新たな脅威に対し、広範なセキュリティー・インテリジェンスに基づいて迅速かつ自動的に適応できる能力によって、保護能力を向上することができます。

総合的な Trusteer アーキテクチャーによって、さまざまなレイヤーおよび製品の間にデータ・フローおよびインテリジェンスが提供されます。表には、Trusteer スイート並びに他の IBM 製品によって提供される製品および機能が記載されています。

オファリング	主な機能
IBM Security Trusteer Fraud Protection Suite は、組織がコストを削減し、エンド・ユーザーのエクスペリエンスを向上させながら、不正をより正確に特定して防止するための、簡略化された不正管理アプローチを提供します。	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、高度な回避手段といったさまざまな重大不正行為の徴候を、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、不正トランザクションのより正確な特定を支援するエンジンです。 • Trusteer Pinpoint Detect を使用した証拠に基づく不正検出機能により、誤検出を大幅に削減しながら不正を検出できます。
組織は Trusteer Pinpoint Detect を購入して特定の不正検出の問題に取り組むことができます。その後必要に応じて組み込みの統合を使用し、対策、調査、修復のレイヤーを追加できます。統合によって、不正管理のライフサイクル全体で情報を容易に共有できるようになります。	IBM Security Access Manager* を統合することにより、認証、社内プロシージャーの実行、セキュリティー・ポリシー管理の機能を得ることができます。IBM Security Access Manager によって、ユーザーは組織に対する実際のリスクに基づき、複数のチャネルにわたって脅威認識型のアクセス・ポリシーを作成し、実行することができます。 • IBM Security Access Manager を使用した脅威認識型認証機能により、実際のリスクに基づく迅速な対策が可能です。
IBM Counter Fraud Management* を統合することにより、過去の不正行為や不適切な支払いに関する証拠を集めながら、事例管理、レポート作成、アラート管理の機能を、不正の企ての防止および阻止に利用することができます。これには、高度なアナリティクスおよび調査分析が含まれます。 • IBM Counter Fraud Management を使用した拡張事例管理およびレポート作成機能により、調査および脅威分析を合理化します。	
Trusteer Rapport for Mitigation を統合することにより、組織はエンド・ユーザーに対し、マルウェアに感染したマシンをクリーニングするための手助けを迅速かつ容易に提供することができます。エンド・ユーザーのコンピューター上にマルウェアが検出されたら、銀行の担当者はマルウェアの除去ツールをダウンロードできるリンクをエンド・ユーザーに提供するだけです。このツールはワンクリックで素早くインストールできます。インストールされたらソリューションはすぐに作業を開始し、既存の金融マルウェアの検出と除去を行います。 • Trusteer Rapport for Mitigation を使用した強力な修復機能により、既存の金融マルウェアは感染したエンドポイントから迅速に除去されます。	

デジタル・チャネルでの不正のリアルタイム **検出**
- IBM Security Trusteer Pinpoint Detect (スタンダード/プレミアム)

危険にさらされたエンドポイントの **修復**
- IBM Security Trusteer Rapport for Mitigation

アクセス **対策***および認証管理*
- IBM Security Access Manager

事例 **調査***およびアラート管理*
- IBM Counter Fraud Management - Investigate

IBM Security Trusteer Fraud Protection Suite は、不正のライフサイクル全体に対する十分な可視性を備えた、SaaS ベースのクロスチャネル型ソリューションを提供します。

オファリング	主な機能
IBM Security Trusteer Pinpoint Detect は、IBM Security Trusteer Pinpoint Criminal Detection と IBM Security Trusteer Pinpoint Malware Detection™ の機能を単一のクラウド・ベースのオファリングに統合します。これらの結合された機能が完全に統合された単一ソリューションとして提供され、導入および継続的な更新が著しく簡略化されます。	• 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、高度な回避手段といった重大不正行為の徴候は、可視性によって不正のライフサイクル全体で関連付けられます。 • 脅威の全体にわたり、2 億 7 千万のエンドポイントからインテリジェンスが継続的に収集されます。 • 高い俊敏性により、組織は変化する環境に迅速に適応できます。
IBM Security Trusteer Pinpoint Malware Detection* は、マルウェアに感染したエンド・ユーザーのコンピューターが銀行の Web サイトにアクセスしたり、 金融機関の保護されている Web アプリケーションを使用したりした時点で正確に検出するために設計された、クライアントレスの不正防止エンジンを提供します。	• マルウェアに感染したデバイスや、マルウェアによる Web 詐欺実行の企てを透過的に検出します。 • 不正行為担当チームに高リスクのデバイスについてアラートを送信し、チームが保護アクションを取れるようにします。 • Trusteer Rapport for Mitigation を使用して、エンド・ユーザーのマシンから既存の金融マルウェアを除去します。
IBM Security Access Manager は、認証、対策、セキュリティー・ポリシー管理を可能にします。	• 組織に対する実際のリスクに基づき、複数のチャネルにわたって脅威認識型のアクセス・ポリシーを作成し、実行することができます。 • 統合された認証機能に、極めて正確な検出機能を組み合わせることによって、統計上のリスクではなく実際のリスクに基づいて不正を阻止できる、強力な機能を実現します。
IBM Counter Fraud Management – Investigate が提供する拡張事例管理およびレポート作成の機能により、調査および脅威分析が合理化されます。	• 事例管理、レポート作成、アラート管理の機能を提供します。これによって金融機関は、高度なアナリティクスおよび調査分析などの機能を使用して、過去の不正行為や不適切な支払いに関する証拠を集めながら、不正の企てを防止および阻止することができます。 • きわめて正確な検出機能と組み合わされた統合認証機能により、誤検出が低減され、実際の不正の判別が迅速化されます。
IBM Security Trusteer Rapport は、感染した PC や MAC デバイスに対するマン・イン・ザ・ブラウザー (MitB) マルウェア感染の調査、修復、ブロック、および除去を可能にすることによって金融マルウェアやフィッシング攻撃を防止する、クライアント・ベースのエンドポイント保護機能を提供します。	• 感染したデバイスから、稼働中および非アクティブ MitB マルウェアによる感染を防止および除去するうえで役立ちます。 • アクティブなマルウェアが存在する場合でも、ブラウズ・セッションの保護を支援します。 • フィッシング・サイト、および危険にさらされた特定のアカウントの資格情報と支払カード・データを検出します。 • 不正行為の担当チームにマルウェア感染および除去について通知し、ユーザーの再資格審査を可能にして、さらに将来的な脅威の排除を支援します。
IBM Security Trusteer Rapport for Remediation は、Trusteer Rapport が備える、エンド・ユーザーの感染デバイスにおける MitB マルウェアの調査、修復、ブロック、および除去についての機能を拡張します。	• 活動中または非アクティブな MitB マルウェアによる感染を防止および除去することによって、銀行の顧客、従業員、ビジネス・パートナーが操作するデバイスを保護します。 • 危険にさらされたエンドポイントおよび感染したエンドポイントを修復し、将来の脅威から保護します。
IBM Security Trusteer Mobile は、デバイスに関するリスク要因の分析およびモバイル・デバイスの永続的 ID の使用によって、ネイティブ・モバイル・アプリケーションを保護します。IBM Security Trusteer モバイル・ソリューションは、モバイル・チャネルでの検出をさらに改善するため、組み込み型 SDK を介して Trusteer Pinpoint Detect とシームレスに統合することができます。このコンポーネントは、マルウェア感染、root 化/Jailbreak に関する情報、正確な地理位置情報、および Wi-Fi のセキュリティー状況といった、詳細なリスク情報をモバイル・デバイスから収集します。	• モバイル・ベースのリスクについて次の要因を検出します。 - Jailbreak/root 化デバイス - マルウェア感染 - 信用できない入手元からインストールされたアプリケーション - 非セキュア Wi-Fi 接続 - 古いオペレーティング・システム - 地理的位置 • ハードウェアとソフトウェアの属性に基づく、アプリケーションの再インストールに対して回復力のある永続的デバイス ID を生成します。

IBM をお勧めする理由

不正防止における顧客支援に関しての IBM の専門知識と継続的な成功は、不正に関するグローバルなインテリジェンスおよびマルウェア調査に深く根差しています。IBM は、世界中の 2 億 7 千万を超えるエンドポイントから収集された専有インテリジェンス・データを分析することにより、世界中の金融機関固有のリスク評価を継続的に行っています。この情報を使用することで、Trusteer ソリューションは適切な不正防止ソリューションを顧客へ確実に提供しています。IBM は、Trusteer セキュリティー・チームが特定した新しい脅威および手段に基づき、このソリューションを継続的に更新します。

詳細情報

IBM Security Trusteer ソリューションの詳細については、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。
ibm.com/security/trusteer

IBM Security

東京都中央区日本橋箱崎町 19 番 21 号

Produced in Japan
2016 年 2 月