financial

Trusteer

Trusteer
金融不正防止対策

金融不正防止の業界基準

数々の金融機関とその顧客達は、コンピューターや携帯端末をオンライン詐欺から守るため、Trusteerの実証済みの設計を使用しています。
Trusteerのグローバルフットプリント、ユニークな社員達、テクノロジー、およびプロセスは、お客様のために持続的な不正防止を実現し、必要な規制要件を満たすことができます。

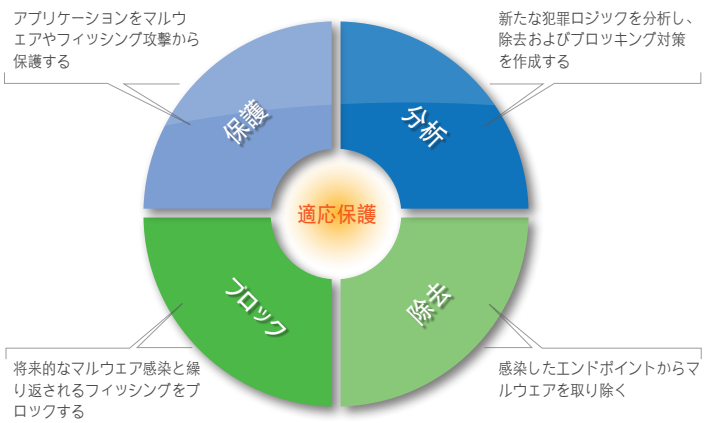
Trusteer はここが違う

- 署名ではなく、犯罪ロジック:
  数百万の保護されたエンドポイントから集められたインテリジェンスを介して、Trusteerは、毎日数万回の犯罪ロジックへの不正攻撃を処理します。Trusteerは、ユニーク、コンパクトで実用的な不正ターゲットおよび戦略のフットプリントを提供します。

- 新たな脅威に対する迅速な適応:
  Trusteerのアダプティブ保護プロセスは、外部からの攻撃を迅速に犯罪ロジックに変え、これらの保護されたエンドポイントへの攻撃を素早く検出し阻止するため、自動的に新たな犯罪ロジックをTrusteerの製品に統合しています。

- リアルタイムでのアプリケーション保護:
  Trusteerのアプリケーション保護技術は、ゼロデイマルウエアおよびフィッシング攻撃に対して、 ブラウザと敏感なクライアント・アプリケーションを透過的に保護します。

Trusteerのアダプティブ保護プロセス



Trusteerのサイバー犯罪防止設計

Trusteerは、デバイス間および業務ライフサイクル間で、複数の保護レイヤーを提供しています。

- **Trusteer Pinpoint** マルウエアに感染したWebセッションおよびフィッシング攻撃を識別し、不正行為のクライアントレス検出を提供します。
- **Trusteer Rapport** 財政上のマルウエアによるPCやMacの感染を防ぎ、改ざんやデータの盗難からラウザを保護し、自動修復を提供します。
- クラウドベースの管理およびインテリジェンス・プラットフォームは、新興犯罪ロジックと攻撃に関する深い洞察を与え、ユーザーベース内での不正リスクを迅速に軽減することを可能にします。
- **Trusteer Mobile** iOSおよびAndroid端末をマルウエアの攻撃から守り、安全なモバイルバンキングを可能にし、オンラインバンキングのための保護された帯域外の認証を提供します。

new threats, ***new thinking***

Trusteer Pinpoint

不正行為のクライアントレス検出

Trusteer Pinpointのマルウェア検出およびTrusteer Pinpointのアカウント・テイクオーバー（ATO）は、任意のデバイス、ブラウザ、またはオペレーティング・システムで行われる不正行為を遠隔的に発見します。マルウェアに感染したウェブ・セッション、およびオンラインバンキング・アカウントへのフィッシング攻撃や不正行為者のアクセスを識別。

マルウェアに感染したエンドポイントを検出します

Trusteer Pinpointのマルウェア検出は、オンラインバンキング・サイトにアクセスするエンドポイントに対するマン・イン・ザ・ブラウザ戦略やマルウェア感染を暴きます。
特定のマルウェアキット、標的の金融機関、攻撃の種類（例：認証情報の盗難、自動化された不正取引）、および盗まれた認証情報を識別します。

リアルタイムのフィッシング攻撃を検出

Trusteer PinpointのATO検出は、リアルタイムでフィッシングやスピアフィッシング攻撃のデータ（例：URLおよび盗まれた認証情報）を収集します。金融機関は、フィッシングキャンペーンに関して通知され、サイトのテイクダウンとURLのブラックリスト化が実施されます。盗まれた認証情報の使用は、アカウント乗っ取りを目的としたログイン試行を識別するために、後で追跡されます。

指紋デバイスおよびタグ犯罪者

Trusteer PinpointのATO検出は、保護されたウェブサイトにアクセスする各エンドポイントに対して、デバイスのあらゆる特徴を収集し固有の「指紋」を生成します。一部の犯罪者は、オペレーティングシステムやブラウザなど、デバイスの特徴をスプーフィングし（なりすまし）デバイスの識別システムを回避しようとします。Trusteerは、デバイスのスプーフィング試行を識別し、実際のセッション情報を検出します。犯罪者が特定されると、関連するすべてのデバイスはフラグ付けされ、将来のアカウント乗っ取り攻撃を防ぎます。

デバイス/アカウントのリスク相関関係により決定的に不正攻撃を識別

Trusteer Pinpointは、デバイスリスクとアカウント盗難の履歴を相関させ、決定的に不正攻撃を識別し対応のアクションを推奨します。たとえば、エンドユーザーのエンドポイントにマルウェアが検出された直後に新たなデバイスからエンドユーザーがアクセスした場合、アカウント乗っ取り詐欺の可能性を強く示しています。一般的に存在するその他の詐欺防止アプローチは、疑わしい取引を検出するために部分的なデータに依存しているため、それらを検証するために詐欺チームや顧客に負荷をかけます。
Trusteer Pinpointは、犯罪者の不正アクセスを正確に検出するために必要な不正ライフサイクル可視性を保持する、唯一のソリューションです。

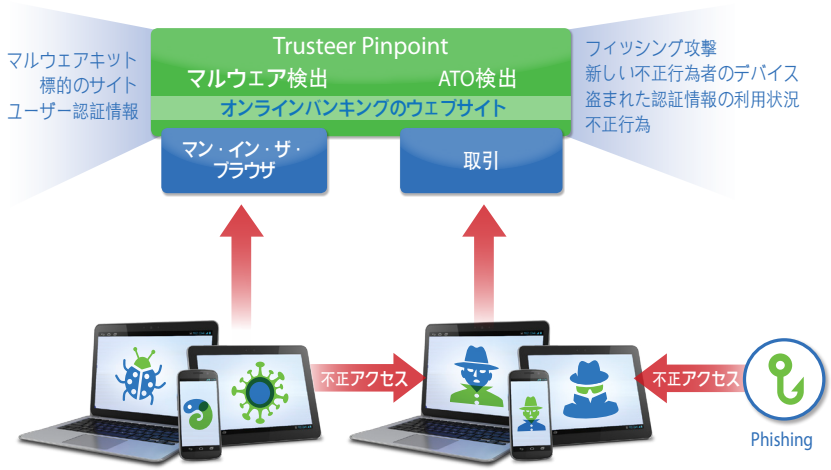
Trusteer Pinpointで詐欺防止を合理化

Trusteer Pinpointは、オンラインバンキングへのアクセスや行動を制限することにより、組織が不正を阻止することを可能にします。これにより、既存の取引確認プロセスやリスク・エンジンなどのリスク情報取り扱いの認証レベルをステップアップすることが可能になります。Trusteer Pinpointは、Trusteer Mobileの帯域外認証を介して取引承認を開始したり、他の強力な認証ソリューションと統合することができます。Trusteer Rapportの顧客は、マルウェアを除去するために、感染した機器でエンドユーザーにアプローチすることができます

Trusteer Pinpointの詐欺リスク分析

- **アカウント履歴**
  - マルウェア感染
  - フィッシング詐欺のインシデント
- **デバイスプロファイル**
  - 新規デバイスID
  - デバイスのなりすまし
  - 知られている犯罪デバイス
- **セッション・プロファイル**
  - 場所と時間
  - 不正アクセス行動

不正行為のクライアントレス検出



Trusteer Pinpointの詐欺防止対策

- 感染や詐欺アクセスを決定的に識別
  - 金融機関の認証プロセスおよびアクセス制限の向上を実現
- 強力な認証のステップアップ
- マルウェアの除去とエンドポイント保護を実施
- 既存の詐欺防止プロセスと統合

Trusteer Rapport

PCとMacのエンドポイントセキュリティ

マン・イン・ブラウザと、マン・イン・ザ・ミドル攻撃からの保護

Trusteer Rapportは、個人情報を引き渡したり、不正取引を承認するように被害者を誘うような悪意のあるWebページのインジェクションを防止するために、ブラウザをロックダウンします。
Trusteer Rapportは、本物のサイトに属するオンラインバンキングのIPアドレスおよびSSL証明書を検証することにより、マン・イン・ザ・ミドル攻撃をブロックします。

資格情報と個人情報の盗難を防ぎます

Trusteer Rapportは、アカウントの乗っ取りやクロスチャンネル不正を犯すのに使用されるログイン資格情報と個人情報の盗難を防ぎます。
そして、ログインと送金ページなどの敏感なアプリケーションのページの画面コピーやキーロギング攻撃を無効にします。

マルウエア感染を防ぎ、既存のマルウエアを除去します

一度インストールされれば、Trusteer Rapportは、エンドユーザー側から既存の金融マルウエアを除去し、ブラウザの脆弱性の悪用およびエンドポイントでのマルウエアのインストール攻撃を防ぐことにより、将来の感染を防ぐことができます。
Trusteer Rapportは、不正チームとサポートチームが、エンドポイント上の脅威を修正し、安全なオンラインバンキングを再開するための、簡単な方法を提供します。

ログイン資格情報と支払いカードデータのフィッシングを停止します

Trusteer Rapportは、保護されたユーザーによるフィッシングサイトへの初めてのアクセスを検出することにより、資格情報と支払カードデータ盗難を防ぐことができます。
Trusteer Rapportは、データロスを防止するために、フィッシング攻撃の可能性のある場合、ユーザーに警告します。
Trusteerの専門家は、ほぼリアルタイムで、サイトが実際に悪意のあるサイトかを確認します。
悪意のあるサイトである場合、そのサイトはTrusteer Rapportのブラックリストに追加され、他のユーザーのアクセスを防ぎます。
金融機関は、タイムリーなテイクダウンとユーザ資格情報の再発行を許可するように通知されます。

悪質な活動は不正チームに通知されます

金融機関は、Trusteer Rapportによって識別されたマルウエアとフィッシング活動に関するインテリジェンス警告を受けます。
これらの警告は、さらに、ユーザ資格情報の再発行、トランザクションのレビュー、およびフィッシングサイトのテイクダウンなどの不正防止と軽減プロセスを駆動することができます。

Trusteerによって管理されたクライアント展開と献身的なカスタマー・サポート

Trusteer Rapportのお客様は、すべてのお客様が継続的に新たな脅威から保護されていることを確保するため、Trusteerによって展開・維持されています。
Trusteer Rapportは、オプトインまたは必須の展開を可能にするTrusteerが提供する「splash」メッセージを介して、ログイン時にエンドユーザーに提供されます。
Trusteerは、エンドユーザーのインストール中または製品を使用時の任意の議寿的な質問に対応するため、専用のエンドユーザー・サポートを毎日２４時間提供しています。

Trusteer Rapportの適応保護

- ブラウザとOSをロックダウンすることによって、エンドポイントを保護する
- Trusteerインテリジェンスによって犯罪ロジックを分析する
- マルウエア除去を自動化する
- 悪用およびマルウエア感染をブロックする

「Trusteerは迅速かつ効果的に新たな脅威に対処します。」

Trusteerのシチュエーションルーム

Trusteerの管理アプリケーション

Trusteer Mobile

保護されたモバイルバンキング、およびアウトオブバンド認証

モバイルバンキングの不正防止

モバイルデバイスをモバイルマルウエアから保護します

Trusteer Mobileは、マルウエア感染と潜在的なセキュリティリスクを検出するために、デバイスをスキャンします。 Trusteerのインテリジェンスセンターは、新たな脅威を識別し、新しい犯罪ロジック（すなわち攻撃戦術）を公開し、対策を作成し、Trusteer Mobileの保護を新興のモバイルマルウエアの脅威に適応します。オペレーティングシステムのセキュリティ状態は、脆弱性を識別するために、現在のセキュリティの最も優れたプラクティスに照らして検証されています。ユーザーは、よりよいセキュリティ状態を作るために、どのようにして脅威を除去しリスクに対処するかについて、指示を受けます。そして、FIsはリスクスコアを活用してリスクの高いトランザクションを検出して処理することができます。

デバイスリスクとセキュリティダッシュボード

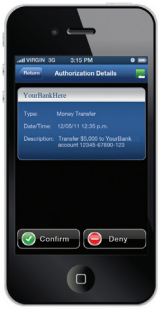
保護されたモバイル・ブラウザで安全なWebアクセス

Trusteer Mobileは、デバイスの解析が完了した後にアクセスすることができる保護されたモバイルブラウザを含みます。埋め込まれたブラウザは、本物のサイトに属するオンラインバンキングのIPアドレスとSSL証明書を検証することにより、 マン・イン・ザ・ミドル（ファーミング）の攻撃をブロックします。
エンドユーザーは、安全にオンラインバンキングのウエブサイトや他のサイトにアクセスし、ブラウザを使用することができます。FIsは、保護されたブラウザからのみオンラインバンキングがアクセスされることを保証し、オンラインバンキングへのアクセスを拒否するためか、より強力な認証を必要とするために、デバイスのリスクスコアを活用します。

オンラインバンキングのためにアウトオブバンド認証を保護します

マルウエアに対してアウトオブバンド・セキュリティ・コントロールを保護します

正当性の認証は、マルウエアの脅威がブロックまたは除去されたデバイス上でのみ信頼することができます。Trusteer Mobileは、マルウエアからモバイルデバイスを保護し、二要素認証とトランザクション・認可サービスの整合性を確保するために設計されています。FIsは、金融取引を検証するために、モバイルデバイスに認証要求を転送することができます。専用のアプリケーション画面は、保留中のトランザクションの受け入れ／拒否、および取引き履歴のレビューを可能にします。さらに、Trusteer Mobileは、ユーザーとモバイル・マルウエア対策アプリケーションとの相互作用を保護します。



金融取引の認証要求

セルフサービス・アカウントのロックダウン

エンドユーザーは、オンラインでバンキングを行っていないとき、アカウントへのアクセスを無効にすることにより、サイバー犯罪者の盗まれた資格情報を使用したり正なトランザクションを提出する機会のウィンドウを排除することができます。アカウントのロックダウンは、簡単なスイッチのON/OFFによって起動させるか、またはユーザーのオンライン・バンキング・セッションが終了した直後に起動するよう設定することができます。

モバイルバンキングの不正防止

- モバイルデバイスをマルウエアから保護する
- マルウエア感染やデバイスのリスクを検出し、警告する
- エンド・ユーザーへの段階的な改善指導を提供する
- モバイルオンラインバンキングの不正を停止するために、FIsのデバイス・リスクスコアの活用を可能にする
- ファーミングとマン・イン・ザ・ミドル攻撃から保護する
- 安全なオンラインバンキングの閲覧を実施する

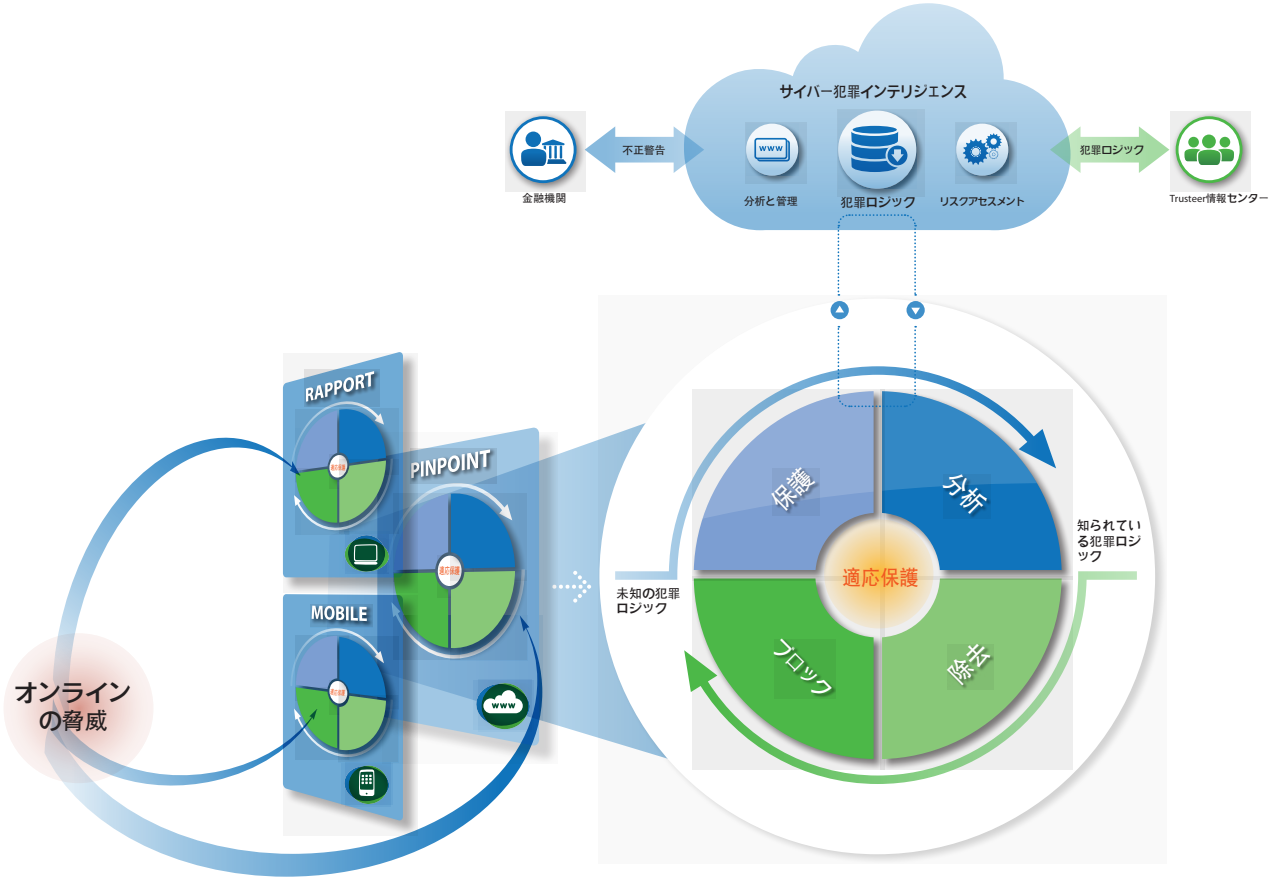
保護されたアウトオブバンド認証

- モバイル・マルウエアからアウトオブバンドのセキュリティを保護する
- オンラインバンキングのログインと取引のモバイル・アウトオブバンド認証を提供する
- エンドユーザーが、モバイル端末からアカウントへのアクセスをロックできる
- エンドユーザーの自己登録を可能にする

柔軟な導入

- セキュア・モバイル・アプリケーション: AppleのAppStore、またはGoogleのPlayアプリケーション・ストアからダウンロードできる標準アプリケーション。
- モバイル・セキュリティ・SDK: スタンドアロンのモバイルアプリにTrusteer Mobile機能を追加する開発キット。

Trusteerのサイバー犯罪防止アーキテクチャー



金融不正防止のためのTrusteer

Trusteer Rapport

オンラインバンキングのためのTrusteer Rapport
- PCやMac上での高度なオンライン脅威の予防と改善

Trusteer Rapportのフィード
- デバイスのセキュリティ構成と脅威活動に関する実用的なフィード activity

Trusteer Pinpoint

マルウェアの検出のためのTrusteer Pinpoint
- マルウェアに感染したエンドポイントのクライアントレスの検出

Trusteer Pinpointのアカウント・テイクオーバー（ATO）検出
- オンラインバンキング・アカウントへのフィッシング攻撃や不正行為者のアクセスのクライアントレス検出

Trusteer Mobile

Trusteer Mobileのバンキングセキュリティ
- マルウェアから守り、安全なモバイルブラウザでWebアクセスを保護

Trusteer Mobileの保護されたアウトオブバンド認証
- 保護されたアウトオブバンド取引、ログイン認証、およびセルフサービスアカウントのロックダウンを提供します

Trusteerインテリジェンスと管理

Trusteerの管理アプリケーション
- Trusteer製品のための統合管理およびレポート作成システム
- 業界全体および固有のオンライン脅威分析のためのインテリジェンス・ポータル

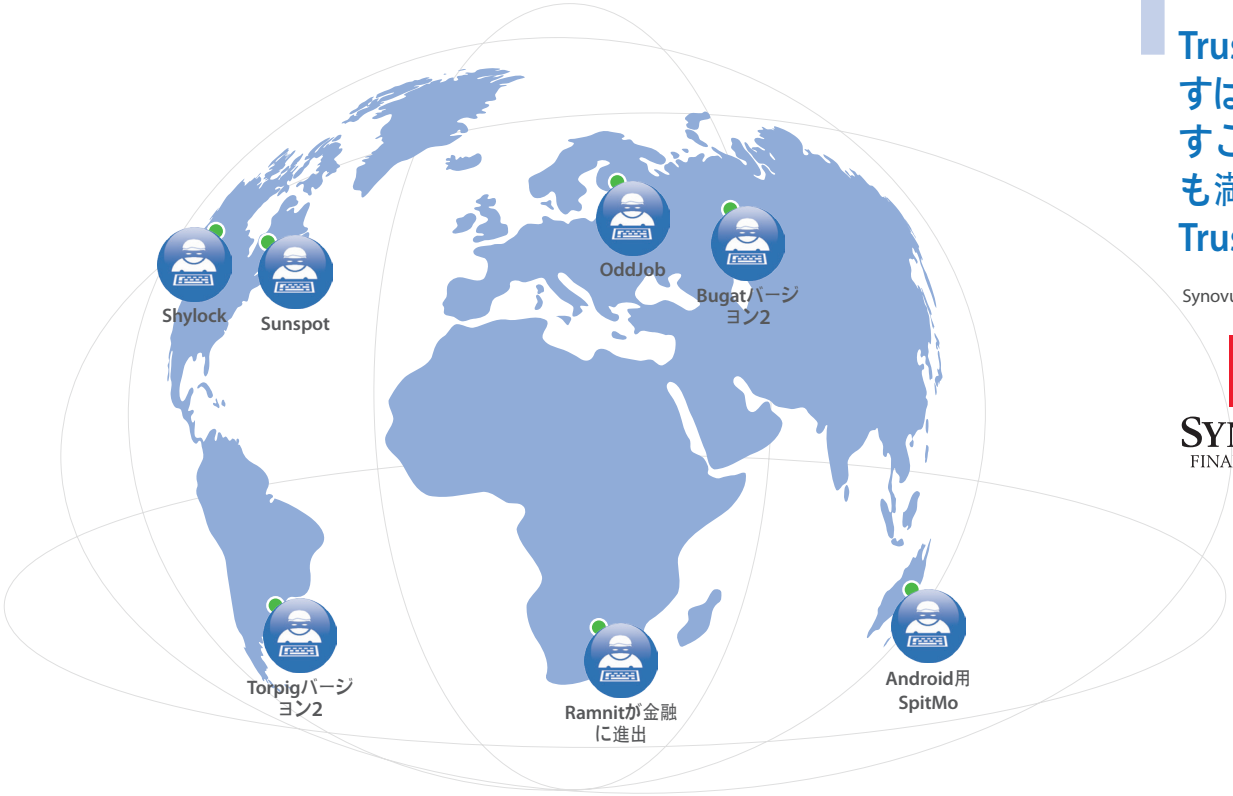
Trusteerは、オンラインバンキングの犯罪防止界のグローバル・リーダーです

Trusteerのサイバー犯罪防止アーキテクチャは、金融機関のビジネスとリテール・バンキングの顧客を、アカウントの乗っ取り、資格情報の盗難や不正取引から保護することを可能にします。

Trusteerは、新たな防犯ロジックを迅速に検出、分析、適応するために、エンドポイント保護技術とリアルタイム・インテリジェンスの専門的な分析を組み合わせた、ユニークなプロセスを作成しました。

数百もの顧客と何千万のエンドユーザーを持つTrusteerは、証明された不正排除のためのソリューションです。

サイバー犯罪から顧客や従業員を保護する方法に関しての詳細は、こちらwww.trusteer.comをご覧ください。



「Trusteerを通して、すばらしい結果を残すことができ、とても満足しています。Trusteer Rapport」

Synovus Bank

SYNOVUS
FINANCIAL CORP.

Trusteer K.K.
恵比寿ガーデンプレイス（18階）
〒150-6018
東京都渋谷区恵比寿4-20-3
T: +813-5789-5747
info.jp@trusteer.com

trusteer.com

Trusteer