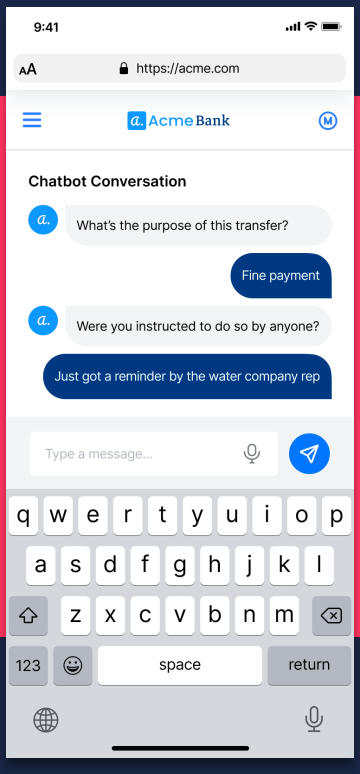
Transmit Security
Détection et protection de la fraude

Inclut nos nouvelles innovations

Détection de la fraude à l'ingénierie sociale

Rapports d'analyses intelligents



Détection de fraude

Challenges, exigences, bonnes pratiques

Vos utilisateurs et applications web/mobile sont constamment attaqués. Que ce soit un bot essayant des identifiants volés sur un autre service, un fraudeur réutilisant un mot de passe dérobé grâce à une arnaque de phishing, ou une attaque d'ingénierie sociale utilisée pour contourner vos mesures de sécurité.

Transmit Security

Détection de la fraude

Exigences – Protection contre la fraude

Authentification sans mot de passe

La plupart du temps, les acteurs malveillants prennent le contrôle des comptes en utilisant **des mots de passe ou des OTP volés,** à travers des attaques de phishing ou des fuites de bases de données. En mettant en œuvre des passkeys conformes à la DSP2, les utilisateurs sont immédiatement sécurisés puisque les secrets sont retirés de l'équation.

Analyse comportementale

En analysant et en apprenant le comportement de vos utilisateurs, vous serez en mesure de **détecter lorsque des fraudeurs tentent de se connecter** avec les identifiants de vos utilisateurs, lorsque des outils de contrôle à distance sont utilisés, ou lorsque des bots interagissent avec votre application.

Fingerprinting d'appareil

Les fraudeurs peuvent agir seuls ou au sein de groupes organisés. Indépendamment de leur structure opérationnelle, les **mêmes individus et appareils reviennent souvent** sur les services ciblés pour exécuter leurs techniques de fraude.

Détection d'émulation

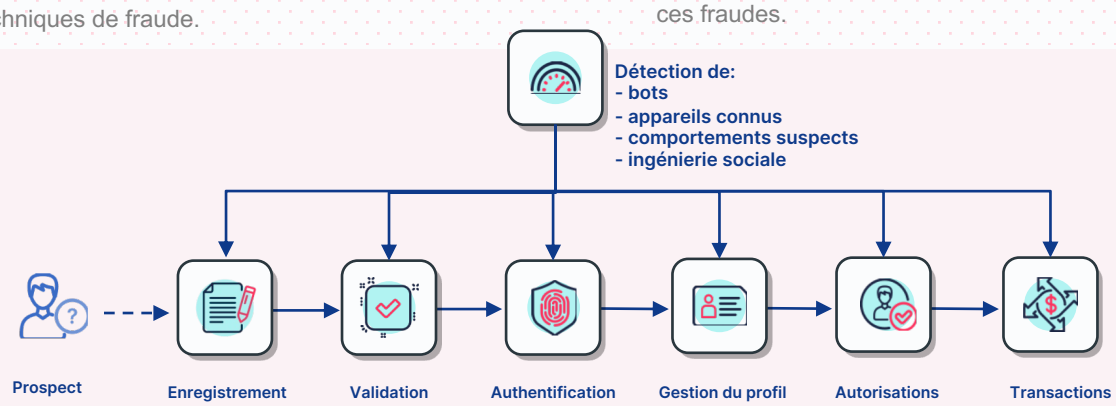
Afin de contourner les systèmes de détection, les fraudeurs peuvent essayer de dissimuler l'identité de leur appareil en utilisant des **techniques de spoofing ou en faisant appel à des appareils émulés** ou virtualisés.

Authentification basée sur le risque

Meilleure l'expérience utilisateur, meilleure la sécurité. Lorsque l'analyse comportementale, du réseau, et de l'appareil établissent qu'un utilisateur est digne de confiance, une vérification d'identité ou une authentification complexe devient inutile. À contrario, la détection de tout risque justifie de challenger l'utilisateur, indépendamment de la validité de la session.

Détection d'ingénierie sociale

Les fraudeurs s'adaptent aux nouvelles mesures de sécurité et manipulent les victimes pour qu'ils exécutent des transactions en leur nom. Il devient alors essentiel d'implémenter des modèles de détection pour prévenir ces fraudes.



Qu'est-ce que l'APP fraud ?

La fraude "Authorized Push Payment" (APP) implique un escroc se faisant passer pour une autorité crédible, comme un employé de banque, et utilisant des tactiques manipulatrices pour contraindre la victime à transférer de l'argent vers un compte contrôlé par le fraudeur ou par un compte mule.

Comment stopper l'APP fraud ?

Dans ce cas, l'utilisateur effectue la transaction avec son propre appareil et dans son environnement habituel, rendant la détection de fraude difficile. Néanmoins, une combinaison stratégique d'analyse comportementale, de révision de l'historique des transactions et d'interaction avec l'utilisateur peut prévenir efficacement de telles fraudes.

transmit security

Transmit Security

Détection et prévention de la fraude

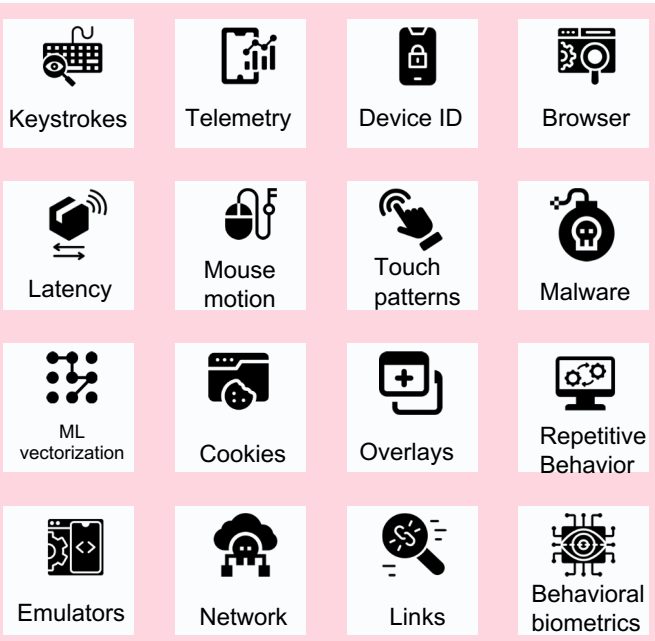
La détection et la prévention de la fraude est une entreprise complexe qui nécessite une solide connaissance des modèles de fraude, mais aussi des technologies de pointe permettant la détection des bots, le fingerprinting d'appareils, l'analyse du comportement des utilisateurs, et le calcul intelligent de score de risques.

Détection multi-méthode Transmit Security

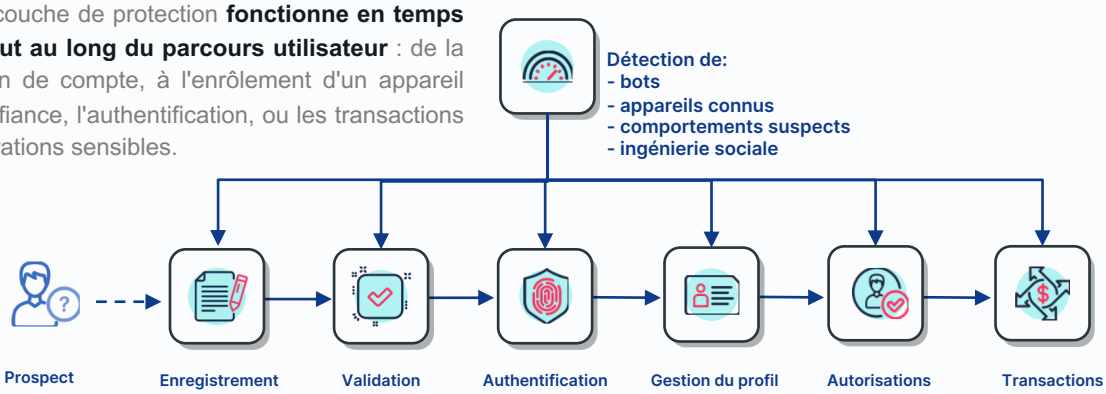
Transmit Security a développé des processus de détection multi-méthodes traitant des centaines de types de télémétrie, les comparant à des modèles de fraude connus et à des comportements de clients de confiance pour **évaluer le risque et la confiance en temps réel.**

L'apprentissage automatique (ML) et l'IA évaluent les signaux dans le contexte complet de votre application et de votre cas d'utilisation pour faire des recommandations intelligentes et précises.

Nos modèles prennent en compte l'ensemble du parcours utilisateur pour protéger votre service contre la prise de contrôle de compte, les bots, la prise de contrôle d'appareil, et plus encore.

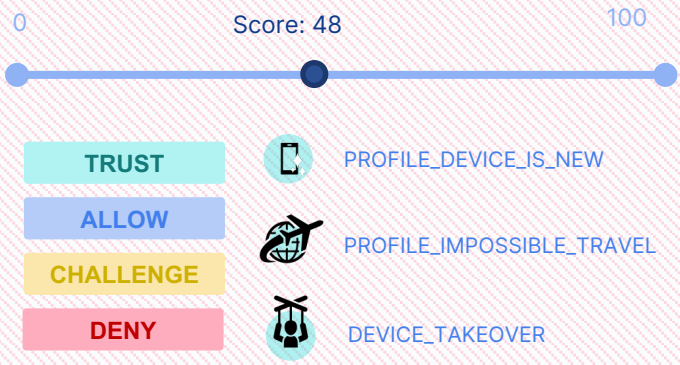


Notre couche de protection **fonctionne en temps réel tout au long du parcours utilisateur** : de la création de compte, à l'enrôlement d'un appareil de confiance, l'authentification, ou les transactions et opérations sensibles.



Une visibilité complète

Transmit Security fournit à la fois un score numérique et une recommandation personnalisée (Trust, Challenge, etc.). De plus, nous fournissons les indicateurs clés sur lesquels la recommandation est basée. **Avec un seul appel API, vous pouvez récupérer une recommandation pour agir en temps réel pendant le parcours de l'utilisateur**. Le tableau de bord vous donne également un résumé des recommandations, y compris les principales raisons de challenger ou de bloquer des actions spécifiques.



transmit security

Transmit Security

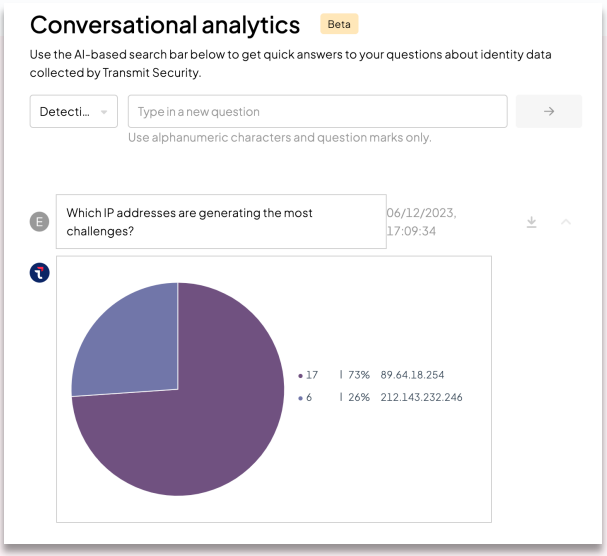
Détection et prévention de la fraude

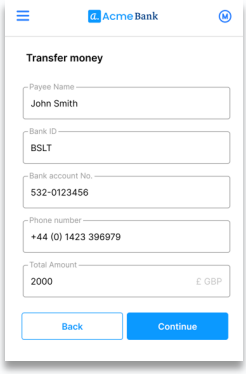
La détection et la prévention de la fraude est une entreprise complexe qui nécessite une solide connaissance des modèles de fraude, mais aussi des technologies de pointe permettant la détection des bots, le fingerprinting d'appareils, l'analyse du comportement des utilisateurs, et le calcul intelligent de score de risques.

Discutez avec vos données

Arrêtez de perdre du temps à apprendre comment interroger vos données et consacrez plutôt plus de temps à les analyser réellement. Notre IA conversationnelle vous permet d'interagir avec vos données en posant des questions et en recevant des réponses sous forme de tableaux, graphiques ou réponses directes. Ces informations peuvent ensuite être facilement intégrées dans vos tableaux de bord quotidiens ou hebdomadaires.

Interroger, rechercher et analyser les données collectées à partir des systèmes de détection de fraude est désormais à la portée de tous, même s'ils ne sont pas des experts techniques.





Analyse de l'historique des transactions

Que ce soit en raison d'une prise de contrôle de compte ou d'une ingénierie sociale, les transactions frauduleuses s'écartent souvent des habitudes de dépenses normales d'une victime. La clé est de comprendre précisément le comportement de transaction de chaque utilisateur et de le relier à d'autres indicateurs pour repérer les attaques potentielles.

Transmit Security utilise des modèles d'IA avancés entraînés à reconnaître les activités transactionnelles typiques d'un utilisateur. Toute activité inhabituelle déclenche une alerte. En réponse à de telles alertes, le système peut challenger l'utilisateur de différentes manières en fonction du niveau de risque : cela peut nécessiter une authentification forte, une vérification d'identité ou, en cas de suspicion d'ingénierie sociale, activer le module de détection de fraude "APP" détaillé ci-dessous.

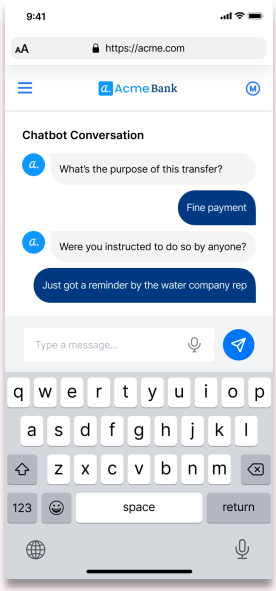
Authorized Push Payment fraud (APP)

Transmit Security a créé le premier chatbot intelligent, unique en son genre, spécialement conçu pour mener des conversations naturelles avec des personnes susceptibles d'être visées par de l'ingénierie sociale, afin d'évaluer leur risque de subir une attaque.

Tirant parti des derniers développements en matière de LLM (Large Language Model), le bot pose des questions pertinentes et générées dynamiquement à l'utilisateur, assurant que les fraudeurs ne peuvent pas facilement s'y adapter.

À la fin de cette discussion interactive, le système calcule un score de risque pour déterminer la probabilité qu'une fraude par ingénierie sociale soit en jeu.

- Comprenez comment les utilisateurs perçoivent leurs propres actions
- Allégez la pression ressentie par l'utilisateur due à l'influence du fraudeur.
- Récupérez un transcript de la conversation, utilisable en cas de litige
- Obtenez un score de risque, basé sur 3 modèles d'IA différents



transmit security

transmit security

Sophie Belloc
Sales Director

06 79 82 56 30
sophie.belloc@transmitsecurity.com

Erwan Dano
Sales Engineer

07 86 98 40 01
erwan.dano@transmitsecurity.com

> *We envision a world where businesses no longer compromise between Security and exceptional Customer Experience.*
>
> Mickey Boodaei
> CEO and Co-Founder, Transmit Security

ILS NOUS FONT CONFIANCE

TIAA · citi · UBS · NN · Rabobank · America's Car-Mart · Intesa Sanpaolo · AXA · usbank · Cattolica Assicurazioni Dal 1896

kuppingercole ANALYSTS

Seul fournisseur à avoir reçu le **statut de leader global :** produit, innovation et marché dans 3 rapports du KuppingerCole Leadership Compass.

"The platform has one of the most feature-rich offerings in the passwordless authentication market and would likely be suitable for any type of organization looking to adopt a passwordless solution."

fido ALLIANCE simpler stronger authentication · Gartner COOL VENDOR 2020 · AICPA SOC · GDPR READY · PSD2