

ÉTUDE DE CAS



Les données fournies par LexisNexis® ThreatMetrix® aident l'e-commerçant espagnol *Wallapop* à mieux détecter les activités frauduleuses tout au long du parcours client

EN QUELQUES MOTS

CLIENT



Wallapop

EXIGENCES

- Offrir aux clients un environnement utilisateur plus sécurisé, permettant de renforcer la confiance entre acheteurs et vendeurs.
- Détecter les fraudes à l'ouverture de nouveaux comptes et les fraudeurs récurrents.
- Améliorer la réputation et l'image de marque tout en protégeant les clients contre la fraude.

SOLUTION

Wallapop, la plateforme leader pour une consommation plus humaine, durable et responsable, utilise les données d'identité numérique du Digital Identity Network® de LexisNexis® pour distinguer en temps quasi réel les comportements en ligne authentiques des comportements frauduleux. Ces informations relatives à l'appareil, à l'emplacement et au comportement aident le commerçant à identifier les situations à haut risque.

RÉSULTATS

- Détection plus fiable et plus précise des fraudes et des fraudeurs récurrents.
- Augmentation significative des taux de détection des fraudes.
- Informations fiables sur les clients et protection des clients contre la fraude.
- Environnement utilisateur plus sécurisé et confiance dans les transactions.
- Amélioration de l'efficacité opérationnelle.

« LexisNexis ThreatMetrix® nous permet de détecter les fraudeurs avant qu'ils ne puissent altérer l'expérience de nos utilisateurs ou leur porter préjudice. Cette aide était indispensable pour offrir à nos clients une expérience optimale. » – Wallapop

Contexte

La technologie géolocalisée de Wallapop rassemble une communauté de 15 millions d'utilisateurs en leur offrant un moyen simple et pratique d'acheter et de vendre des articles qui ne sont plus utilisés. Sa plateforme, qui a déjà permis de donner une seconde vie à plus de 180 millions d'articles, propose des objets originaux à des prix très avantageux, tout en prolongeant la durée de vie de produits en parfait état de marche. Depuis sa création, Wallapop s'est engagée à promouvoir l'innovation continue dans le secteur du marché de l'occasion et à utiliser la technologie pour contribuer au développement durable.

Besoins du client

Aujourd'hui plus que jamais, les clients plébiscitent l'e-commerce, provoquant une croissance exponentielle et constante des transactions en ligne.

Mais les sites marchands sont souvent confrontés au dilemme suivant : offrir à leurs clients (nouveaux et existants) l'expérience la plus fluide possible tout en se protégeant des fraudeurs, qui profitent de l'anonymat procuré par les canaux numériques.

Wallapop met en relation des acheteurs et des vendeurs en leur offrant un moyen simple et pratique d'acheter et de vendre des articles qui ne sont plus utilisés. Mais des fraudeurs tentent parfois d'exploiter la plateforme à leur profit. Wallapop recherchait donc une solution capable d'assurer l'intégrité de la plateforme pour offrir une expérience optimale aux utilisateurs légitimes tout en maintenant les fraudeurs à bonne distance.

Pour Wallapop, les priorités étaient les suivantes :

- Conserver un environnement sécurisé pour les utilisateurs et les interactions de confiance.
- Détecter les fraudeurs qui créent de nouveaux comptes.
- Identifier les fraudeurs récurrents utilisant de nouvelles identités.



Construire l'image de la véritable identité numérique à chaque étape du parcours en ligne

La conception d'une solution efficace pour Wallapop visait avant tout à permettre à l'entreprise d'identifier facilement les clients de confiance et les clients récurrents, quels que soient le lieu ou l'heure de leurs transactions. LexisNexis ThreatMetrix® aide Wallapop à collecter des renseignements concernant l'appareil du client, son emplacement géographique, son comportement en ligne et ses informations d'identification, créant ainsi une identité numérique complète pour chaque utilisateur du site. Ces renseignements sont issus d'une part des transactions réalisées sur Wallapop, et d'autre part de toutes les transactions liées à cet utilisateur recueillies via le Digital Identity Network® de LexisNexis.

Le Digital Identity Network® collecte et traite des millions de transactions effectuées chaque jour dans le monde entier sur des milliers de sites web, et permet ainsi de suivre l'empreinte numérique des utilisateurs en ligne dans de multiples secteurs d'activité et emplacements géographiques.

À partir de ces données, le Digital Identity Network® crée une identité numérique unique pour chaque utilisateur en analysant de multiples connexions entre les appareils, leur emplacement et des données personnelles anonymisées. Tout comportement s'écartant de cette identité numérique de confiance peut être détecté de manière fiable, quasiment en temps réel, et alerter Wallapop si de nouveaux utilisateurs se servent de données d'identification pouvant avoir été volées, masquent leur emplacement ou tentent d'ouvrir de multiples comptes à partir d'un même appareil, ou d'autres situations de ce type.

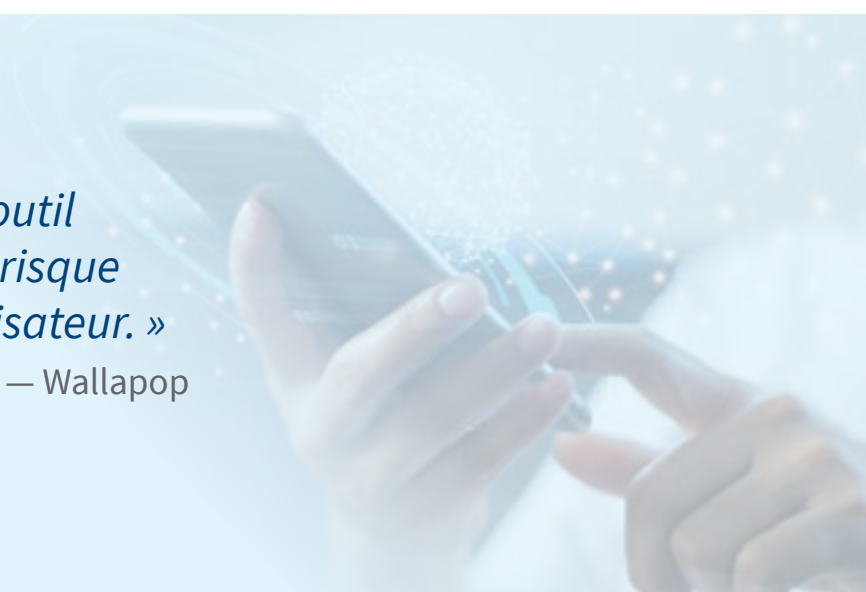
Utiliser des scores de confiance pour identifier les fraudeurs récurrents en temps quasi réel

Même si un fraudeur est en possession d'informations d'identité authentiques, LexisNexis ThreatMetrix® est capable de signaler le fait que la transaction émane d'une entité numérique récurrente associée à de précédents faits de fraude, que le lieu où se trouve l'appareil n'est pas celui habituellement associé à l'utilisateur de confiance, ou que la vitesse de frappe ne correspond pas à un comportement humain normal (il pourrait donc s'agir d'une attaque de bots automatisée).

Grâce à ces données, Wallapop peut identifier les comptes potentiellement à haut risque et les fraudeurs récurrents. Cela a permis à l'entreprise de protéger ses clients authentiques et d'améliorer sa réputation de prestataire de services en ligne fiables et sécurisés.

« LexisNexis ThreatMetrix est un outil essentiel pour mieux évaluer le risque potentiel de chaque nouvel utilisateur. »

— Wallapop





La solution proposée à Wallapop s'appuie sur plusieurs fonctionnalités phares de LexisNexis ThreatMetrix® :

- **ThreatMetrix SmartID®** : identifie les utilisateurs récurrents qui effacent les cookies, utilisent la navigation privée et modifient d'autres paramètres pour contourner les outils traditionnels de prise d'empreintes numériques des appareils. Cet outil améliore la détection des utilisateurs récurrents et réduit le nombre de faux positifs. À partir de l'analyse de nombreux navigateurs, plug-ins et attributs de connexion TCP/IP, SmartID se base exclusivement sur les attributs des appareils pour améliorer la détection des visiteurs récurrents, et en particulier de ceux qui tentent d'échapper à l'identification.
- **ThreatMetrix Mobile** : un kit de développement logiciel (SDK) pour les terminaux mobiles Google Android et Apple iOS, qui offre une protection complète contre la fraude pour l'application mobile Wallapop. Il permet notamment une identification fiable des périphériques persistants, la détection des anomalies et des attaques par usurpation, un contrôle de l'intégrité des applications, la détection des logiciels malveillants, et est également doté de technologies de débrièvement et de détection.
- **TrueIP** : détecte efficacement l'utilisation de services de dissimulation d'emplacement et d'identité tels que les proxys cachés et les VPN pour permettre à votre entreprise de voir la véritable adresse IP, la géolocalisation et d'autres attributs propres à chaque transaction.
- **Les services professionnels de LexisNexis Risk Solutions** : l'équipe des services professionnels de LexisNexis Risk Solutions a apporté une expertise unique en adaptant la solution LexisNexis ThreatMetrix® aux besoins spécifiques et évolutifs de Wallapop. Grâce à nos experts, Wallapop améliore constamment ses règles et ses politiques pour pouvoir détecter un large spectre d'attaques tout en réduisant le nombre de faux positifs et les vérifications manuelles.

Pour plus d'informations, consultez notre site Internet risk.lexisnexis.com/global/fr/fraude



À propos de LexisNexis Risk Solutions

LexisNexis® Risk Solutions exploite la puissance des données et des analyses avancées pour fournir des informations qui aident les entreprises et les entités gouvernementales à réduire les risques et à améliorer les décisions au bénéfice des personnes dans le monde entier. Nous fournissons des données et des solutions technologiques pour un large éventail de secteurs, notamment l'assurance, les services financiers, la santé et le gouvernement. Notre siège social est situé dans la région métropolitaine d'Atlanta, en Géorgie, et nous avons des bureaux dans le monde entier. Nous faisons partie de RELX (LSE : REL/NYSE : RELX), un fournisseur mondial d'outils d'analyse et d'aide à la décision basés sur les informations destinés aux professionnels et aux entreprises. Pour plus d'informations, veuillez consulter les sites www.risk.lexisnexis.com/global/fr et www.relx.com.

Ce document est publié à titre informatif uniquement et ne garantit pas la fonctionnalité ou les caractéristiques des produits LexisNexis® Risk Solutions mentionnés. LexisNexis Risk Solutions ne garantit pas que ce document est complet ou sans erreur.

LexisNexis et le logo Knowledge Burst sont des marques déposées de RELX Inc. ThreatMetrix, Digital Identity Network et ThreatMetrix SmartID sont des marques commerciales de ThreatMetrix, Inc. © 2021 LexisNexis Risk Solutions. NXR15802-00-0123-FR