LexisNexis®
RISK SOLUTIONS

ÉTUDE DE CAS

L'intelligence de LexisNexis® ThreatMetrix® aide Cdiscount à mieux détecter les activités frauduleuses tout au long du parcours client, réduisant considérablement les usurpations de compte et la fraude au paiement

EN BREF

CLIENT

Cdiscount

BESOINS INITIAUX

- Protéger les clients existants des usurpations de comptes.
- Accepter plus de commandes des clients de confiance, en réduisant les frictions.
- Autoriser des solutions de paiement variées pour les transactions sûres.
- Détecter les commandes frauduleuses faites avec des cartes bancaires volées.

SOLUTION

Cdiscount exploite l'intelligence du réseau d'identités numériques de LexisNexis® (Digital Identity Network®) pour différencier de façon fiable les comportements des internautes légitimes et des fraudeurs, et ce en temps réel. Les données sur les appareils, l'emplacement et le comportement du client aident Cdiscount à identifier les scénarios à haut risque.

RESULTATS

- Réduction significative des usurpations de comptes.
- Détection fiable des tentatives de paiement frauduleuses utilisant des numéros de cartes bancaires volés.
- Réduction de l'authentification renforcée 3-D Secure (3DS) pour les transactions sûres.
- Limitation de l'affichage du paiement fractionné aux bons clients.
- Détection de 95% de la fraude en valeur.

Aperçu

Depuis la vente de son premier DVD à moins de 1€ en 1998, Cdiscount n'a cessé de se transformer pour s'adapter aux évolutions du marché et anticiper les envies du consommateur en se positionnant toujours là où on ne l'attendait pas : hightech, électroménager mais également vin, décoration, jouet et aujourd'hui électricité.

La société est passée d'un modèle classique de retailer à un modèle de plateforme en ouvrant une marketplace en 2011, la faisant ainsi passer d'une offre de quelques milliers à près de 40 millions de produits, ce volume représentant l'assortiment de 1,000 supermarchés.

Cdiscount est aujourd'hui le leader français du e-commerce avec en 2018, un volume d'affaires de plus de 3,6 milliards d'euros, plus de 20 millions de visiteurs uniques et près de 9 millions de clients.

Besoins Metier

Aujourd'hui, plus que jamais, les clients se sont tournés vers le E-Commerce dont les transactions augmentent de façon significative.

Cependant, les E-commerçants, sont coincés entre fournir une expérience la plus fluide possible pour les clients (nouveaux et existants), et se protéger des fraudeurs qui tirent parti de l'anonymat procuré par les canaux numériques.

Les fraudeurs sont devenus experts en matière d'usurpation d'identité, se dissimulant derrière de véritables données clients pour paraître totalement convaincants lors d'une transaction en ligne. Les données volées disponibles à l'achat sur le dark web ne manquent pas, et sont constamment alimentées par les vols de données mondiaux.

Comment, par exemple, les E-commerçants peuvent-ils identifier avec précision un fraudeur qui, via la création d'un nouveau compte, va effectuer un paiement mais en utilisant des numéros de cartes bancaires volés? De même, comment peuvent-ils s'assurer que les fraudeurs n'usurpent pas les comptes clients, pouvant ainsi, sans être détectés, utiliser les cartes bancaires enregistrées?

Les priorités pour Cdiscount étaient:

- La détection des fraudeurs utilisant des identifiants volés, souvent via des robots ou des scripts automatisés, pour prendre le contrôle des comptes clients.
- Le blocage de l'utilisation de cartes bancaires volées lors du paiement, ce qui entraîne souvent des niveaux élevés de « chargeback ».
- Veiller à ce que les bons utilisateurs ne soient pas pris au piège d'une politique de détection des fraudes trop stricte les incitant à abandonner leur panier au profit d'une expérience de paiement plus fluide et moins contraignante ailleurs.

"Notre priorité principale est d'aider nos vrais clients à passer des commandes en toute sécurité et sans risquer de compromettre leur compte. En détectant les activités frauduleuses le plus en amont possible du parcours client, ThreatMetrix protège l'intégrité de notre plate-forme."

— Cdiscount

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

La conception d'une solution efficace pour Cdiscount a commencé par être en mesure de reconnaître de manière fiable les clients fidèles et de confiance, quels que soient le moment et le lieu où ils effectuent des transactions. LexisNexis ThreatMetrix aide Cdiscount à rassembler des informations relatives à l'appareil, à la localisation, au comportement en ligne et aux informations de paiement du client, créant ainsi une identité numérique complète de chaque utilisateur effectuant une transaction. Non seulement ces renseignements sont renseignés à partir des transactions de Cdiscount, mais par toutes les connexions relatives à cet utilisateur au sein du Digital Identity Network®.

Le Digital Identity Network collecte et traite chaque jour des millions de transactions mondiales sur des milliers de sites Web, aidant à reconstituer l'empreinte numérique des internautes via des milliers d'entreprises de tous les secteurs.

Cette capacité signifie qu'un comportement qui s'écarte de ce profil de confiance peut être signalé à Cdiscount en temps réel, qu'il s'agisse d'une connexion inhabituelle ou d'une transaction provenant d'un nouvel emplacement pour quelqu'un n'ayant pas l'habitude de voyager.

Tirer parti de la confiance pour identifier l'usurpation de compte en temps réel

Même si un fraudeur est en possession de véritables identifiants de connexion, LexisNexis ThreatMetrix peut signaler le fait que la transaction provient d'un appareil nouveau ou à haut risque, d'un emplacement inhabituel non associé auparavant à l'utilisateur de confiance, ou faite à une vitesse qui est anormale pour un comportement humain (et donc indicatif d'un trafic de bot automatisé).

Cdiscount peut donc bloquer les tentatives de connexion jugées à haut risque, protégeant les bons comptes utilisateurs sans imposer de frictions inutiles.

"La taille et l'échelle du LexisNexis® Digital Identity Network® – ainsi que l'expertise en matière de fraude E-commerce de l'équipe Services Professionnels – nous ont permis d'affiner et d'améliorer continuellement nos politiques de détection des fraudes afin que, indépendamment de ce que les cybercriminels nous lancent, nous sachions nous adapter."

— Cdiscount

Exploiter l'intelligence mondiale partagée pour évaluer de manière fiable les paiements en ligne

Le but ultime d'un fraudeur est le « cash out » – que ce soit en utilisant des cartes bancaires volées pour une transaction de grande valeur ou en accédant à la carte bancaire enregistrée d'un client pour effectuer un achat frauduleux.

La sécurisation du paiement était donc une condition essentielle pour garantir l'intégrité de la plateforme Cdiscount. LexisNexis ThreatMetrix aide Cdiscount à évaluer les risques d'une transaction client au moment du « pré-paiement » :

- Pour les transactions à faible risque, Cdiscount offre aux clients la possibilité de fractionner leurs paiements en 4 fois ; un paiement flexible de plus en plus populaire chez les E-commerçants.
- Les transactions à haut risque sont poussées vers l'authentification renforcée 3DS.

Les scénarios à haut risque qui sont probablement indicatifs d'un fraudeur utilisant des informations d'identification volées peuvent être signalés en temps réel et incluent:

- Des comptes frauduleux créés uniquement pour utiliser des cartes bancaires volées. Cela peut inclure des scénarios tels que plusieurs cartes bancaires associées à la même identité numérique.
- Une même identité numérique tentant de créer plusieurs comptes différents.
- Une identité numérique ayant été marquée comme frauduleuse dans le réseau d'identités numériques.
- Des anomalies par rapport à l'historique des commandes d'un client.
- Des commandes passées à partir d'une géolocalisation considérée comme risquée ou tentée d'être dissimulée.

"La capacité d'exploiter des données aussi riches relatives à la géolocalisation d'une transaction, combinée à l'intelligence de l'identité numérique de chaque utilisateur en ligne, est un facteur de différenciation clé pour nous. C'est là que ThreatMetrix excelle vraiment."

— Cdiscount

ÉTUDE DE CAS

Identifier les tentatives de paiement des robots qui tentent de contourner l'authentification 3DS

En plus de la fraude de paiement utilisant des identifiants volés, Cdiscount subissait également des attaques de robots opérant sur des adresses IP françaises. Les attaques impliquaient généralement plusieurs tentatives de paiement, dont la valeur diminuait avec le temps.

Le but de ces attaques était de tester à quel moment une transaction serait acheminée vers l'authentification 3DS, pour connaître son seuil de déclenchement. Cela permettait ainsi au fraudeur d'effectuer plusieurs paiements frauduleux tombant juste en dessous du seuil et d'éviter les mesures de sécurité supplémentaires requises par le fournisseur de services de paiement de Cdiscount (PSP).

La solution ThreatMetrix aide Cdiscount à détecter ce trafic de bots automatisé en effectuant une analyse comportementale des utilisateurs pendant les périodes de fonctionnement normal et en comparant ces données à celles collectées lors d'une attaque de bots.

La solution Cdiscount repose sur les principales fonctionnalités suivantes 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 empreintes numériques de l'appareil. Cela améliore la détection des utilisateurs qui reviennent et réduit les faux positifs. Dérivé de l'analyse de nombreux attributs de navigateurs, de plug-ins et de connexion TCP / IP, SmartID est basé exclusivement sur les attributs de l'appareil pour améliorer la détection des visiteurs qui reviennent, en particulier ceux qui tentent d'échapper à l'identification.
- **ThreatMetrix Mobile:** un kit de développement logiciel (SDK) léger pour les appareils mobiles Google Android et Apple iOS, offrant une protection complète contre la fraude pour l'application mobile de Cdiscount. Cela inclut l'identification avancée des périphériques, la détection des anomalies et de l'usurpation de périphériques, l'évaluation de l'intégrité des applications, la détection des logiciels malveillants, les services de localisation, les technologies de détection de jailbreak.

- **TrueIP:** détecte de manière fiable l'utilisation des services de dissimulation de localisation et d'identité, tels que les proxys cachés et les VPN, permettant à Cdiscount de voir la véritable adresse IP, la géolocalisation et d'autres attributs de chaque transaction.
- **Champion Challenger:** aide Cdiscount à déterminer l'efficacité des changements de règles, ainsi qu'à affiner les règles pour suivre le rythme des changements de comportement des consommateurs et garder une longueur d'avance sur les nouveaux modèles de fraude.
- **Les Services Professionnels de LexisNexis Risk Solutions:** l'équipe des services professionnels dédiée à Cdiscount fournit une expertise en matière de fraude, adaptant la solution LexisNexis ThreatMetrix pour répondre aux exigences uniques et évolutives de Cdiscount. L'équipe contribue à optimiser en permanence les règles et les politiques pour s'assurer que le spectre complet des attaques frauduleuses est efficacement détecté, tout en minimisant les faux positifs et les examens manuels.

LexisNexis®
RISK SOLUTIONS

En savoir plus sur risk.lexisnexis.com/FIM-EN