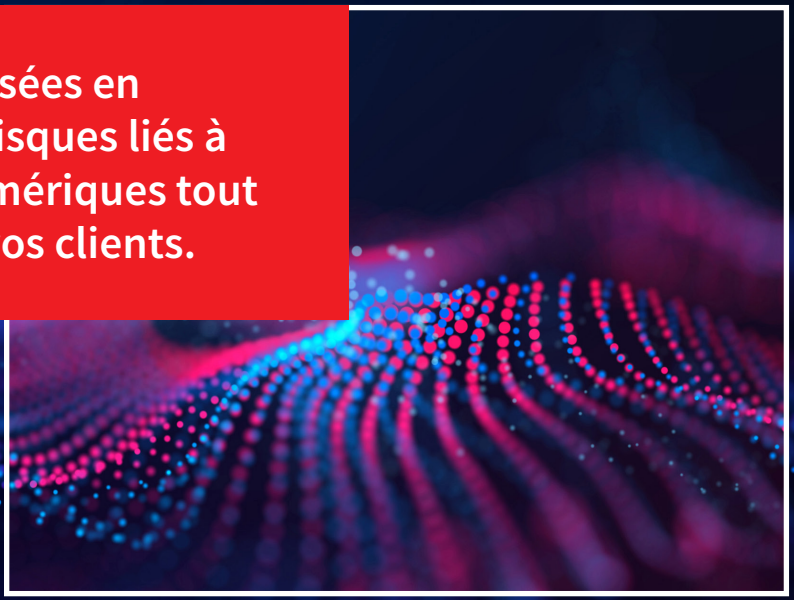
LexisNexis®
RISK SOLUTIONS

LEXISNEXIS® THREATMETRIX®

Prenez des décisions avisées en matière de gestion des risques liés à l'usage des identités numériques tout au long du parcours de vos clients.



Jusqu'à **95 %**

de taux de reconnaissance des clients.

Jusqu'à **90 %**

de réduction des pertes liées à la fraude.

Jusqu'à **70 %**

de réduction des abandons de transactions.

La solution ThreatMetrix de LexisNexis a été conçue pour offrir les meilleurs niveaux de protection antifraude, de vérification d'identité et d'authentification et ainsi aider les acteurs du numérique à distinguer plus efficacement et en temps réel les clients de confiance des fraudeurs potentiels tout en réduisant les points de friction.

Grâce à ThreatMetrix, vous pourrez identifier de manière fiable les clients récurrents, détecter les comportements anormaux et exploiter ces renseignements pour améliorer la modélisation des futurs risques de fraude. ThreatMetrix combine les renseignements sur l'identité numérique avec les attributs d'identité physique pour développer les capacités suivantes :

- Des renseignements sur l'identité numérique.
- Des analyses décisionnelles en temps réel associant l'analyse comportementale à l'apprentissage automatique en mode « boîte blanche ». Un outil de gestion des cas.
- Une authentification intelligente associant une approche par le risque à des stratégies d'authentification forte des clients pour répondre aux évolutions des exigences réglementaires tout en réduisant les points de friction.
- Des solutions d'investigation et d'analyse combinant la gestion des cas à des outils de criminalistique et de reporting pour faciliter le traitement et la résolution des situations à haut risque.

La plateforme ThreatMetrix de LexisNexis permet d'améliorer la prise de décisions en matière de risques tout au long du parcours client.

Une protection à plusieurs niveaux pour optimiser vos décisions en matière de fraude et de risques.

Sachez avec qui vous effectuez des transactions pour développer votre activité en toute sécurité.

PREMIER NIVEAU DE PROTECTION
Évaluation de l'identité numérique

- Renseignements sur les sites Web et sur les appareils mobiles
- Géolocalisation, détection de l'utilisation de VPN, serveurs proxy et TOR
- Anomalies liées à l'identité numérique, aux périphériques et aux localisations
- Vérification de l'identité des consommateurs
- Biométrie comportementale
- Menaces liées aux programmes malveillants (webinject) et bots

DEUXIÈME NIVEAU DE PROTECTION
Outils d'aide à la prise de décision

- Bonnes pratiques et données décisionnelles liées à votre secteur d'activité
- Corrélations et relations entre les données d'identité
- Analyse des fraudes et des comportements de fraude
- Apprentissage automatique
- Gestion des modèles
- Intégration et orchestration

TROISIÈME NIVEAU DE PROTECTION
Authentification

- Liens renforcés entre les dispositifs
- Notifications Push sécurisées
- Mot de passe à usage unique par SMS
- KBA dynamique
- Biométrie
- Authentification de documents

QUATRIÈME NIVEAU DE PROTECTION
Enquêtes et analyses

- Investigation
- Gestion des cas
- Production de rapports
- Rétroaction sur les données de « feed-back » classées par catégorie
- Feed-back, audits et politiques de gouvernance
- Politique de gestion des accès

LexisNexis® Risk Solutions propose une gamme complète de services professionnels pour offrir un accompagnement ciblé à des entreprises de toutes tailles durant tout le cycle de vie de la solution : de l'implémentation au suivi régulier des problématiques spécifiques qui sont rencontrées. Le niveau de service est positionné de façon flexible en fonction des attentes du client.

Prévenir encore mieux la fraude tout en misant sur une expérience utilisateur fluide et personnalisée.

La solution ThreatMetrix de LexisNexis vous aide à décoder l'ADN numérique des utilisateurs, vous permettant ainsi de détecter en temps réel les comportements suspects et de prendre des décisions éclairées en matière de gestion des risques liés aux identités.

En associant les fonctionnalités du LexID® Digital et du Digital Identity Network® de LexisNexis®, ThreatMetrix améliore vos prises de décision en matière de risques grâce à des renseignements sur l'identité numérique et à des données pertinentes sur les transactions. Vous avez ainsi toutes les cartes en main pour gérer rapidement les étapes cruciales tout au long du cycle de vie du client :

Création d'un nouveau compte

Client légitime ou fraudeur ?

Modification des données personnelles

Cette demande de changement d'identifiant est-elle associée à un autre comportement suspect ?

Connexion aux comptes

Comment authentifier les utilisateurs en évitant les points de friction ?

Paiements

Le payeur utilise-t-il des informations volées ?

+ de 75 milliards
de transactions annuelles traitées dans le monde.

8,5 milliards
d'appareils identifiés.

2,5 milliards
d'identités numériques.

195
pays couverts dans le monde.

Rejoignez les milliers d'entreprises mondiales qui allient rentabilité et sécurité, sans compromis.

Digital Identity Intelligence Vous aide à détecter les situations à haut risque en temps quasi réel. Le Digital Identity Network® de LexisNexis® collecte et traite des renseignements obtenus à l'échelle mondiale, basés sur des millions d'interactions de consommateurs (informations de connexion, paiements, demandes de créations de nouveaux comptes, etc.). À partir de ces données, la solution ThreatMetrix 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 qui s'écarte de cette identité numérique de confiance peut être détecté de manière fiable en temps quasi réel et vous alerter sur une possible fraude.

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-in 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 le canal mobile. Il permet notamment une identification fiable des périphériques persistants, la détection d'anomalies et d'usurpation de dispositifs, un contrôle de l'intégrité des applications, la détection de logiciels malveillants, et est également doté de technologies de détection de « jailbreak » et des périphériques « rootés ».

Plateforme décisionnelle dynamique ThreatMetrix Véritable référence sur le marché, la plateforme ThreatMetrix® Dynamic Decision Platform® (DDP) offre une authentification améliorée, une vérification de l'identité et une aide à la prise de décision en cas de fraude. En combinant les renseignements d'identité numérique avec des analyses comportementales et l'apprentissage automatique, cette plateforme intègre également des sources de données tierces pour le traitement des exceptions. La gestion des cas permet d'isoler et d'investiguer les transactions qui nécessitent une étude plus détaillée. Elle aide les entreprises à optimiser l'utilisation des données fournies par ThreatMetrix et à prendre des décisions avisées en matière de gestion des risques.

Behavioral Biometrics Conçue pour compléter la solution ThreatMetrix® et offrir un niveau de protection supplémentaire en matière de lutte contre la fraude et de gestion des risques. La biométrie comportementale permet de comprendre comment un utilisateur interagit avec le site web ou l'application via son clavier, sa souris ou son mobile. Grâce à elle, les entreprises peuvent déceler plus rapidement les comportements à haut risque associés à des fraudeurs, à des bots, à des attaques de type « ingénierie sociale » ou des attaques d'accès à distance, tout en ayant une vision plus claire du comportement de leurs utilisateurs de confiance dans la durée. Ce qui permet d'identifier plus facilement tout écart éventuel par rapport à un schéma de comportement habituel.

LexisNexis®
RISK SOLUTIONS

Pour plus d'informations, consultez la page :

risk.lexisnexis.com/global/fr/products/threatmetrix

Asie-Pacifique
+852 39054010

Amérique latine/Brésil
+0800 8920600

Europe/Moyen-Orient/Afrique
+44 (0) 203 2392 601

États-Unis/Canada
1-408-200-5755

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 pour le 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.

Ce document est publié à titre informatif uniquement et ne garantit pas la fonctionnalité ou les caractéristiques des produits LexisNexis identifiés. LexisNexis 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 et Digital Identity Network sont des marques commerciales de ThreatMetrix, Inc. © 2020 LexisNexis Risk Solutions.

Pour plus d'informations, veuillez consulter les sites www.risk.lexisnexis.com/global/fr et www.relx.com.

NXR15606-00-0822-FR