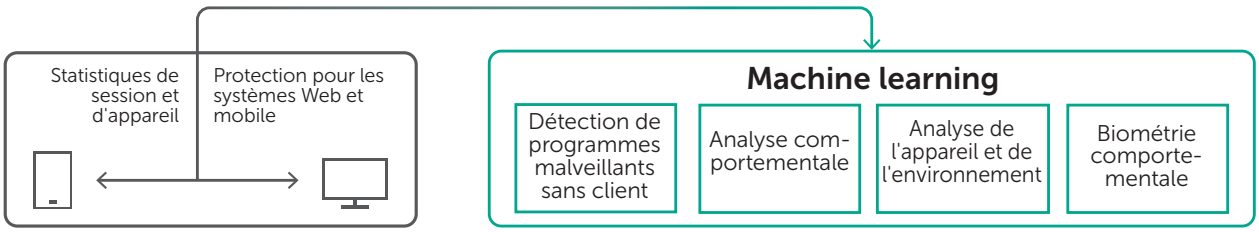
Kaspersky Fraud Prevention

Technologies avancées pour une détection des fraudes dans des canaux multiples en temps réel

Les entreprises fournissent déjà à leurs clients bien plus que les services traditionnels en leur permettant d'accéder à leurs comptes personnels via des systèmes en ligne et sur des appareils mobiles. La transformation numérique apporte de nouvelles opportunités, de nouveaux clients et, bien sûr, un chiffre d'affaires plus élevé. D'un autre côté, elle ouvre la porte aux fraudeurs avec de nouveaux dispositifs sophistiqués et des attaques de canaux multiples à la fois sur l'appareil et le compte de l'utilisateur.

Fraude via de nouveaux comptes	Piratage de compte	Outils d'automatisation de la fraude
Manipulation de transaction	Attaques à l'aide d'outils d'administration à distance	Programmes malveillants et phishing

Kaspersky Fraud Prevention utilise une gamme complexe de technologies avancées dotées du machine learning. Les dispositifs de fraude sophistiqués sont détectés de façon proactive et en temps réel, sur les systèmes mobiles et en ligne, avant que la transaction ne soit effectuée.

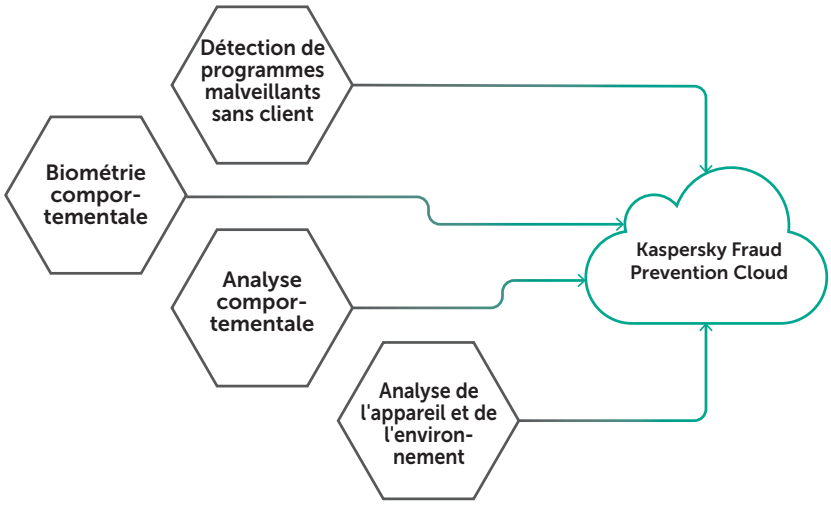


La détection de programmes malveillants sans client vérifie si la machine du client est infectée par des programmes malveillants, sans que l'utilisateur ait besoin d'installer un logiciel supplémentaire. Ces informations sont utilisées afin de déterminer la légitimité des transactions, ainsi que pour l'authentification selon le risque et le modèle de machine learning.

L'analyse comportementale s'intéresse à l'activité de l'utilisateur lors de la connexion et pendant la session en analysant les schémas de navigation et temporel, la façon dont l'utilisateur agit dans le compte personnel, ce sur quoi il clique, et bien plus encore. Ces données permettent la construction de profils à comportement normal, ainsi que la détection de tout comportement suspect ou anormal lors de la connexion et tout au long de la session.

La biométrie comportementale analyse l'interaction de votre client unique avec son appareil (lorsqu'il déplace la souris, touche l'écran ou le balaye rapidement par exemple) afin de détecter si l'appareil est entre les mains d'un utilisateur légitime ou non. Cette technologie peut également être utilisée pour détecter les robots et les outils d'administration à distance.

L'analyse de l'appareil et de l'environnement profite de la présence mondiale de Kaspersky Lab pour identifier les « bons » appareils et utiliser ces connaissances pour authentifier l'utilisateur. En fonction de l'identification générale de l'appareil, de l'adresse IP et de la réputation de l'emplacement, entre autres, tout attribut considéré comme une activité frauduleuse est détecté de manière proactive et identifié comme suspect ou lié à la fraude.



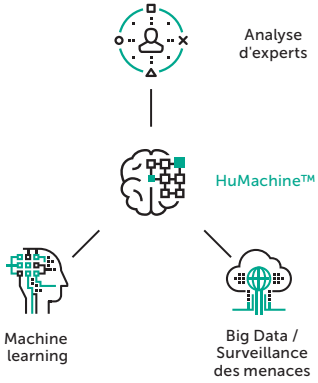
Le machine learning est au centre de la plateforme Kaspersky Fraud Prevention. Plusieurs méthodes de machine learning, telles que **la mise en cluster, l'apprentissage par arbre de décision et les réseaux de neurones artificiels**, sont appliquées afin d'optimiser l'efficacité et la précision des technologies Kaspersky Fraud Prevention. La détection des fraudes franchit un nouveau palier en évitant des étapes d'authentification supplémentaires pour les clients légitimes et en réagissant en temps réel en cas de fraude pendant toute la durée de la session.

Les données dépersonnalisées traitées par 4 technologies clés deviennent des diagnostics en temps réel au sein de Kaspersky Fraud Prevention Cloud. Grâce à l'analyse continue et proactive de l'appareil et de la réputation de la session à travers les systèmes en ligne et mobile, ainsi qu'aux données comportementales et biométriques et à d'autres aspects, notre solution Cloud fournit à vos systèmes de surveillance interne des données cruciales pour détecter les fraudes au bon moment et de façon efficace. Elle permet à vos systèmes actuels de bénéficier d'un contexte supplémentaire pour une prise de décision plus précise et proactive, ainsi que de l'authentification à étapes intelligente et adaptative.

PRINCIPAUX AVANTAGES :

- Détection continue et proactive en temps réel des fraudes avancées avant que la transaction n'ait lieu
- Détection de la fraude sur plusieurs canaux : les systèmes mobiles et en ligne
- Détection de fraudeurs et de blanchiment d'argent
- Amélioration de l'expérience utilisateur grâce à l'authentification selon le risque, ce qui entraîne la croissance et la conservation de la clientèle
- Statistiques complètes sur la session pour les analyses criminalistiques avec l'aide d'une équipe dédiée
- Complémentaire avec les solutions Enterprise Fraud Management existantes
- Améliorations de la productivité grâce à l'automatisation

Pour en savoir plus, contactez-nous sur : kfp@kaspersky.fr



Tout savoir sur la sécurité sur Internet : **www.viruslist.fr**
Rechercher un partenaire près de chez vous :
http://www.kaspersky.fr/partners/buyoffline/liste-des-partenaires

www.kaspersky.fr
#truecybersecurity