WAVESTONE

RÉVOLUTION TECHNOLOGIQUE :
QUELLE PERSPECTIVE POUR LA LUTTE CONTRE LA FRAUDE ?

La protection des actifs, notamment contre leur vol ou leur détournement, est depuis longtemps un enjeu majeur des entreprises. Les dispositifs antifraude s'organisent autour de trois grands piliers : la prévention, la détection et la réaction. Ces dispositifs historiques font aujourd'hui face à de multiples évolutions qui offrent également des opportunités sans précédent que les entreprises se doivent de saisir.

Les expériences et expérimentations du secteur bancaire, en avance sur ces problématiques, permettent d'envisager les perspectives à venir et fournit donc un prisme d'analyse utile aussi pour les autres secteurs.

CONTACTS

Martin DESCAZEAUX
martin.descazeaux@wavestone.com

Mathieu COUTURIER
mathieu.couturier@wavestone.com

MENACES, USAGES, RÉGLEMENTATIONS : TROIS ÉVOLUTIONS MAJEURES QUI IMPLIQUENT DES ADAPTATIONS DES DISPOSITIFS ANTIFRAUDE

Les transformations business et technologiques dans l'ensemble des secteurs d'activité font apparaitre des évolutions impactant directement les dispositifs antifraude historiques.

Les menaces évoluent, les **pratiques de fraude se sont professionnalisées** avec de nouveaux outils et de nouvelles pratiques. Prenons l'exemple du phishing : même sans connaissances informatiques, une cellule de fraudeurs entrainée peut désormais acheter un kit de phishing prêt à l'emploi et met en moyenne seulement trois minutes entre une connexion frauduleuse et une sortie d'argent. Les **tentatives de fraude se sont donc démultipliées** ces dernières années.

En parallèle, les usages évoluent vers une **plus forte digitalisation**, parfois dictés directement par **des évolutions réglementaires**, à la fois à destination des clients ou à destination des collaborateurs. Par exemple la mise en place de l'Instant Payment

en France ou de la directive européenne sur les services de paiement 2e version (DSP2) prévoient des virements instantanés. Ces nouveaux usages accélèrent les transactions financières entre les acteurs entrainant par la même occasion des **besoins d'évaluation instantanée** des risques de fraude. De plus, cette multiplication des canaux de paiement entraîne une **augmentation de la surface d'attaque** avec notamment une diversification des malwares bancaires aux applications mobiles ainsi que l'apparition de pratiques d'ingénierie sociale complexes **multicanales** et appuyées sur une compréhension des processus métier.

La diversification des fraudes, la volumétrie associée et l'augmentation des besoins de traitement instantané rend le traitement manuel presque impossible. La création de règles d'alertes plus restrictives pour minimiser les volumes ferait cependant courir le risque de manquer un grand nombre de fraudes.

Dans ce nouveau paysage, où la fraude devient de plus en plus technologique et peut avoir de multiples origines (clients, donneurs d'ordres, sous-traitants, fournisseurs, administrateurs…), les stratégies de détection doivent évoluer et passer d'une détection réactive des fraudes connues à une détection proactive des menaces encore inconnues.

LES NOUVELLES TECHNOLOGIES, L'AVENIR DE L'ANTIFRAUDE POUR FAIRE FACE À CE NOUVEAU PARADIGME

L'approche historique de la détection de fraude est fondée principalement sur la définition de règles unitaires générant une alerte en cas de non-respect d'un des critères et sur la corrélation d'événements, consistant à mettre en œuvre des règles métiers plus avancées prenant en compte plusieurs types de données, afin de générer une alerte lorsque apparaissent des indices du déroulement d'un scénario de fraude connu.

Cette approche tout en demeurant efficace pour la détection de fraudes connues, par exemple dans la lutte contre le *phishing*, n'est plus suffisante pour faire face aux évolutions en cours. Une approche hybride doit être enrichie sur la base des nouvelles technologies présentes sur le marché (intelligence artificielle/Machine Learning, biométrie comportementale…) qui offrent deux grandes perspectives d'enrichissement des dispositifs actuels.

> Le nombre de variables manipulés par des algorithmes peut facilement dépasser une cinquantaine, là où des règles statiques intègreront difficilement une douzaine de paramètres

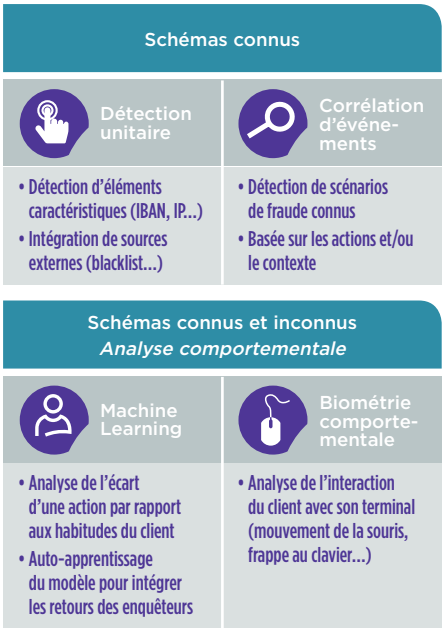
1 - Passer d'une détection de masse à une détection individualisée beaucoup plus fine qui va se concentrer sur les changements de comportement

Le Machine Learning a la possibilité de créer des profils individuels à chaque client. Ces profils, composés de variables construites à l'aide des données collectées, vont permettre de modéliser le comportement. Ainsi, les algorithmes utilisés vont comparer le profil du client (et donc son habitude) avec un événement donné et, de fait, remonter une anomalie lorsqu'une divergence apparait. À noter que le nombre de variables manipulées peut facilement dépasser plusieurs dizaines, là où des règles statiques n'intègreront que quelques paramètres, permettant ainsi de démultiplier le potentiel de détection ou de réduire le nombre de faux positif.

2 - Diversifier les périmètres à couvrir en bénéficiant des économies d'échelle apportées par ces technologies (mutualisation des infrastructures big data, massification des données, automatisation permettant un gain de temps pour les analystes…)

Ces technologies ont la capacité d'intégrer et corréler, grâce à des *Data Lake* sur lesquels elles s'appuient, des volumétries importantes de données brutes, techniques ou métiers (logs applicatifs, connaissances clients, opérations financières…) et d'apporter un potentiel d'enrichissement par des données extérieures (liste de surveillance, transformation d'adresses IP en localisations physiques…). Pour tirer le maximum de bénéfices des systèmes antifraudes, le *Data Lake* doit disposer d'un historique de données pertinentes et conformes, à savoir 13 mois pour des personnes physiques et 6 mois pour des personnes morales.

Principales méthodes de détection



Pour autant ces technologies ne sont pas « magiques », elles nécessitent d'avoir à disposition des données en qualité et en quantité afin de réaliser un important travail préparatoire sur la construction des variables qui portent les capacités de détection des algorithmes. Cette phase de construction nécessite un apport d'expertise à la fois métier mais aussi technologique (*datascience*, développeurs, etc.).

Le choix des algorithmes n'est également pas à négliger, notamment d'un point de vue de la transparence. En effet, certains outils sont basés sur des algorithmes où les résultats sont difficilement justifiables. Le manque de visibilité sur les critères d'établissement des résultats entraine une remontée d'alertes en « boîte noire » et ne permet pas toujours de justifier les blocages aux clients. Une trop grande opacité peut également avoir des conséquences juridiques, voir être illégale, lorsque ces alertes ont des conséquences directes sur des clients.

LE DILEMME DE L'ÉVOLUTION DES DISPOSITIFS ANTIFRAUDE : QUELS LEVIERS POUR INTÉGRER CES TECHNOLOGIES ?

Au vu des spécificités de chaque entreprise et des investissements d'ores et déjà réalisés dans les infrastructures big

data et les initiatives Machine Learning, il convient de se questionner pour trouver le bon équilibre entre solution interne (sur mesure, développée par des *data scientists*) et/ou externe.

Faisant écho à ces problématiques, l'écosystème des éditeurs s'est organisé pour proposer des solutions antifraude s'appuyant sur ces technologies. Ainsi éditeurs et start-ups se sont très largement développés, partout dans le monde (plus de 150 fournisseurs ont été recensés au sein du radar « Antifraude » Wavestone). Le besoin de lutte antifraude a en effet par nature une dimension internationale, notamment dans la protection des flux monétaires qui sont rarement limités à un seul pays.

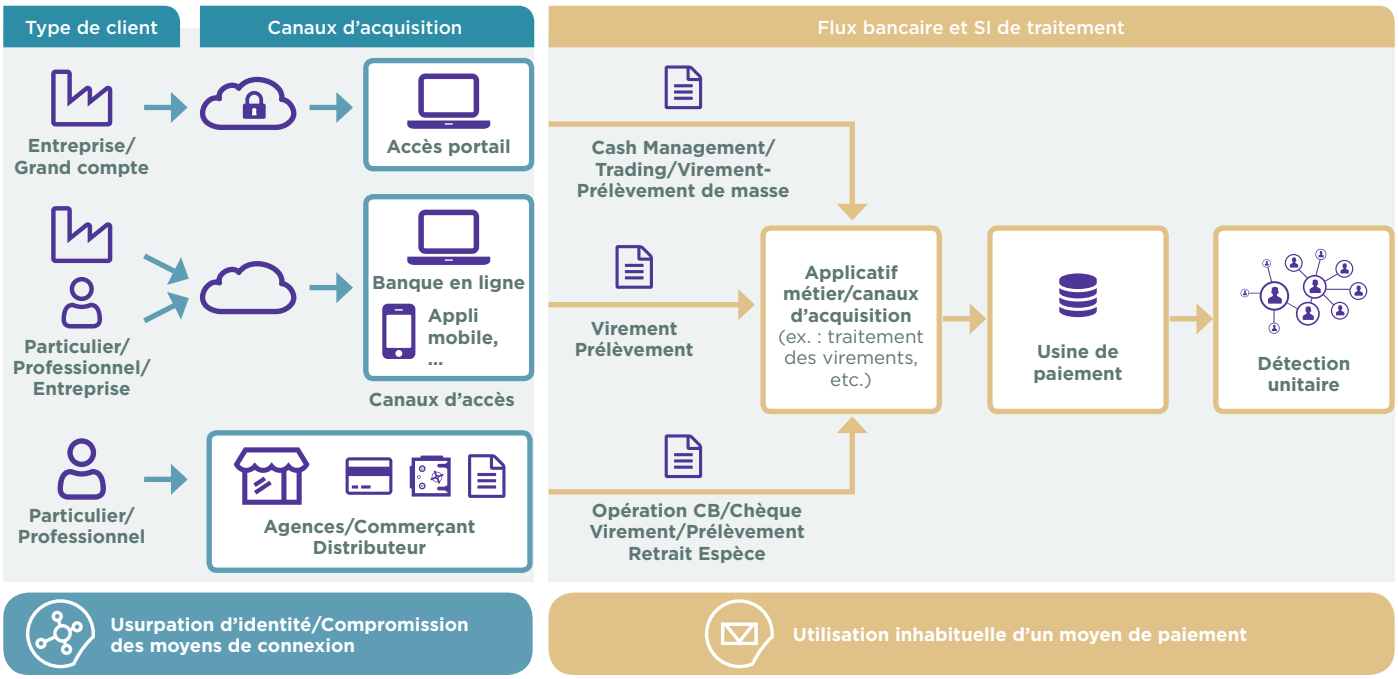
> Usuellement 13 mois de profondeur d'historique sur des personnes morales et 6 mois sur des personnes physiques sont nécessaires pour créer les profils et entrainer les modèles

Même si la lutte contre la fraude apparait comme un *use case* de choix pour démontrer le ROI du Machine Learning (réduction du nombre de fraudes, automatisation de la détection…) et au-delà du choix de la stratégie d'outillage de lutte contre la fraude au regard de la maturité du marché, les questions à se poser doivent rester celles d'une solution SI « standard » (exploitation, maintenance, évolutivité…).

Si les coûts d'infrastructures nécessaires à la mise en place d'outils basés sur le Machine Learning et le big data ne sont pas négligeables, ils permettent de créer un environnement favorable à l'exploitation de la richesse des données pour divers usages (maintenance prédictive des serveurs, connaissance client, etc.) en gardant à l'esprit les garde-fous mis en place par le RGPD.

Exemple du radar des éditeurs antifraude Wavestone (extrait non exhaustif)

Où peut-on agir avec le Machine Learning : exemple d'une banque Wavestone (extrait non exhaustif)



UNE NOUVELLE CIBLE À ATTEINDRE : UNE APPROCHE « SANS COUTURE » TECHNOLOGIQUE ET MÉTIER

Face aux nouveaux enjeux et l'apport des technologies émergentes, une nouvelle stratégie antifraude doit être désormais définie.

La mise en place d'un dispositif **de détection globale de confiance devra respecter 5 grands principes** :

- L'efficience et l'automatisation : il bénéficiera d'une détection à plusieurs critères (moteur de règles et Machine Learning) et d'une efficacité opérationnelle optimisée par l'automatisation de mesures allant de l'augmentation du niveau d'authentification demandé au gel d'un virement.
- L'évolutivité et l'omnicanal : il intègrera plusieurs périmètres dans la détection avec une logique « sans couture » entre le monde cyber et le monde « hors cyber » et sera conçu pour permettre l'intégration de nouvelles données disponibles (ex : données de biométrie comportementale).
- La visibilité et l'exploitabilité : il fournira la visibilité (*reporting*) et l'explication des résultats de détection, aux équipes antifraude, aux clients et également aux régulateurs.
- La conformité et la sécurisation : il respectera les obligations en matière de détection ainsi que les réglementations (RGPD), et traitera les risques inhérents au Machine Learning (tentatives de *poisoning*, compréhension par l'attaquant du modèle…).
- La gouvernance transverse cybersécurité et métier : une collaboration étroite des équipes de détection de menaces cyber et métier antifraude, dépassant les silos encore trop présents, permettra une réponse globale avec une vision 360 des menaces et fera le meilleur usage des données disponibles.

Pour bénéficier de tous les atouts apportés par cette nouvelle stratégie de détection, il conviendra également de ne pas négliger les systèmes d'investigation et de réaction.

Une décentralisation partielle de la lutte contre la fraude, impliquant les conseillers bancaires, permettra une plus grande capacité d'investigation. Ayant la connaissance la plus fine de leurs clients, ces derniers représentent un atout dans le processus d'investigation.

De plus, la biométrie comportementale et le Machine Learning permettent de fournir une meilleure visibilité sur le niveau de confiance qu'on peut accorder à l'utilisateur. Une fois le niveau de confiance défini, il est donc possible d'adapter les niveaux d'authentification demandés en conséquence. Une contribution adaptée et graduée de l'utilisateur permettra ainsi de réduire le nombre d'alertes émises.

La mise en place d'une nouvelle cible antifraude n'est pas seulement pour assurer une réponse adaptée à un changement de contexte mais aussi pour anticiper une vague de fond qui s'amorce aujourd'hui. La détection de fraudes deviendra à l'avenir de plus en plus complexe compte tenu d'une digitalisation qui va continuer à s'accélérer, en particulier sur les moyens de paiement. L'émergence de nouveaux acteurs, comme les *Fintechs*, et la désintermédiation grandissante des banques vont notamment entraîner un appauvrissement de la donnée disponible. Les dispositifs antifraude sont donc voués à évoluer en profondeur afin de garder et développer leur efficacité.

WAVESTONE

www.wavestone.com

Dans un monde où savoir se transformer est la clé du succès, l'ambition de Wavestone est d'apporter à ses clients des réponses uniques sur le marché, en les éclairant et les guidant dans leurs décisions les plus stratégiques.

Wavestone rassemble 2 800 collaborateurs présents sur 4 continents. Il figure parmi les leaders indépendants du conseil en Europe, et constitue le 1er cabinet de conseil indépendant en France.