IBM Counter Financial Crimes Management for Banking

Approches multifacettes de réduction des fraudes, de maintien du niveau de conformité et de gestion efficace.

Points clés

- Solution unique détectant les tentatives de fraude, de blanchiment d'argent et d'activités de cybercriminalité
- Capacité de découvrir des stratégies de produits et multi-canaux complexes et suspicieuses
- Amélioration de l'efficacité des analystes et des investigateurs
- Veille d'entreprise pour ajuster continuellement les opérations et rester en avance sur les tendances

Le paysage changeant des délits financiers

Les délits financiers augmentent en fréquence et en ingéniosité. Les représentants du crime organisé qui attaquent les institutions financières et leurs clients sont présents dans le monde entier. Ce sont des professionnels et des experts en revente d'informations volées. Ces organisations sont toujours à la pointe de la technologie et emploient des modèles commerciaux agiles qui leur permettent de s'adapter rapidement. Les criminels brouillent les pistes de la cybercriminalité, de la fraude et du blanchiment d'argent en jouant sur le manque de visibilité concernant les types de paiement, les canaux et les limites institutionnelles.

Pendant ce temps, les leaders du secteur de la lutte contre la fraude, de la sécurité et de la conformité évoluent dans un environnement commercial redoutable. Les leaders font désormais face à des risques au niveau des conseils d'administration, avec des conséquences et une surveillance accrues. Toutefois, les leaders ne disposent pas toujours des budgets suffisants pour résoudre ces problèmes critiques. La demande de paiements plus rapides, le besoin d'introduire de nouveaux produits innovants et l'attention portée à l'augmentation des volumes de transaction sur les principaux canaux en ligne et mobiles favorisent l'apparition de nouveaux risques et de nouvelles réglementations. Malheureusement, les banques se composent d'équipes distinctes travaillant verticalement avec des solutions ponctuelles disparates. Les différents silos d'informations obtenus créent des écarts d'informations critiques entre lesquels se faufilent les fraudeurs, dont les stratégies de fraude gagnent en complexité.

Les grandes institutions financières changent leurs manières d'appréhender leurs activités pour remporter ce combat, notamment en supprimant des silos d'informations et en implémentant de nouvelles techniques d'analyse plus complètes dans l'entreprise. De plus, l'association avec des partenaires stratégiques permet à ces organisations d'exploiter des techniques et technologies puissantes pour mener efficacement une guerre longue et multifacettes contre les délits financiers.

IBM combat la cybercriminalité, la fraude et le blanchiment d'argent

La solution IBM Counter Financial Crimes Management a pour vocation d'augmenter et d'améliorer les environnements d'exploitation existants, afin de permettre aux institutions financières de combler l'écart entre la technologie et le renseignement en réduisant les compartiments entre les services. Cette solution intégrée offre des capacités de détection, d'identification et de traitement des activités frauduleuses. Elle permet également de se conformer aux exigences de connaissance des clients, de contrôle des transactions, de sélection de listes et de création de rapports en matière de lutte contre le blanchiment d'argent.

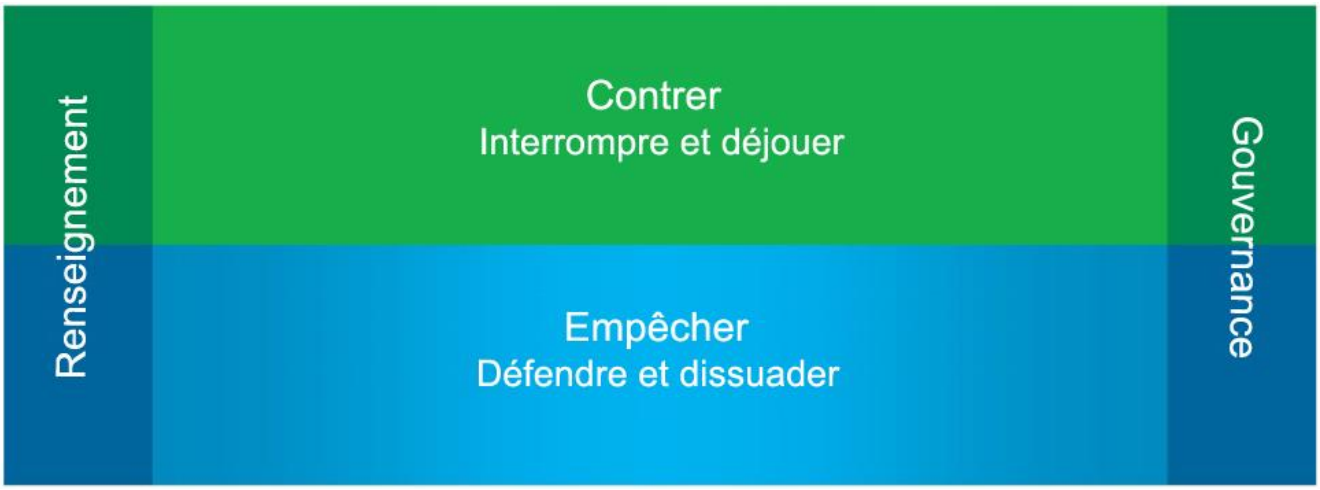

Figure 1 : Le réseau IBM Counter Fraud Network a pour objectif de prévenir et de contrer les délits financiers.

IBM propose des solutions d'analyse avancées et d'analyse d'investigations approfondie pour améliorer l'efficacité, la visibilité et le contrôle en termes de lutte contre la fraude et le blanchiment d'argent. La solution prend en charge des flux d'informations provenant de sources de renseignement internes et externes, y compris de l'équipe de renseignement IBM Red Cell. Les institutions financières peuvent ainsi détecter activement les activités suspectes et agir plus rapidement. Cette approche globale peut se traduire par une réduction des fraudes, une exposition réduite aux réglementations et des coûts d'exploitation qui améliorent les résultats commerciaux et l'expérience du client.

La solution IBM Counter Financial Crimes Management for Banking se compose d'un ensemble de fonctionnalités d'analyse prédictive, d'entités et de Big Data étroitement liées permettant de supprimer les silos d'informations, de développer l'espace d'observation et de fournir une Business Intelligence d'entreprise unifiée de la détection à l'enquête.

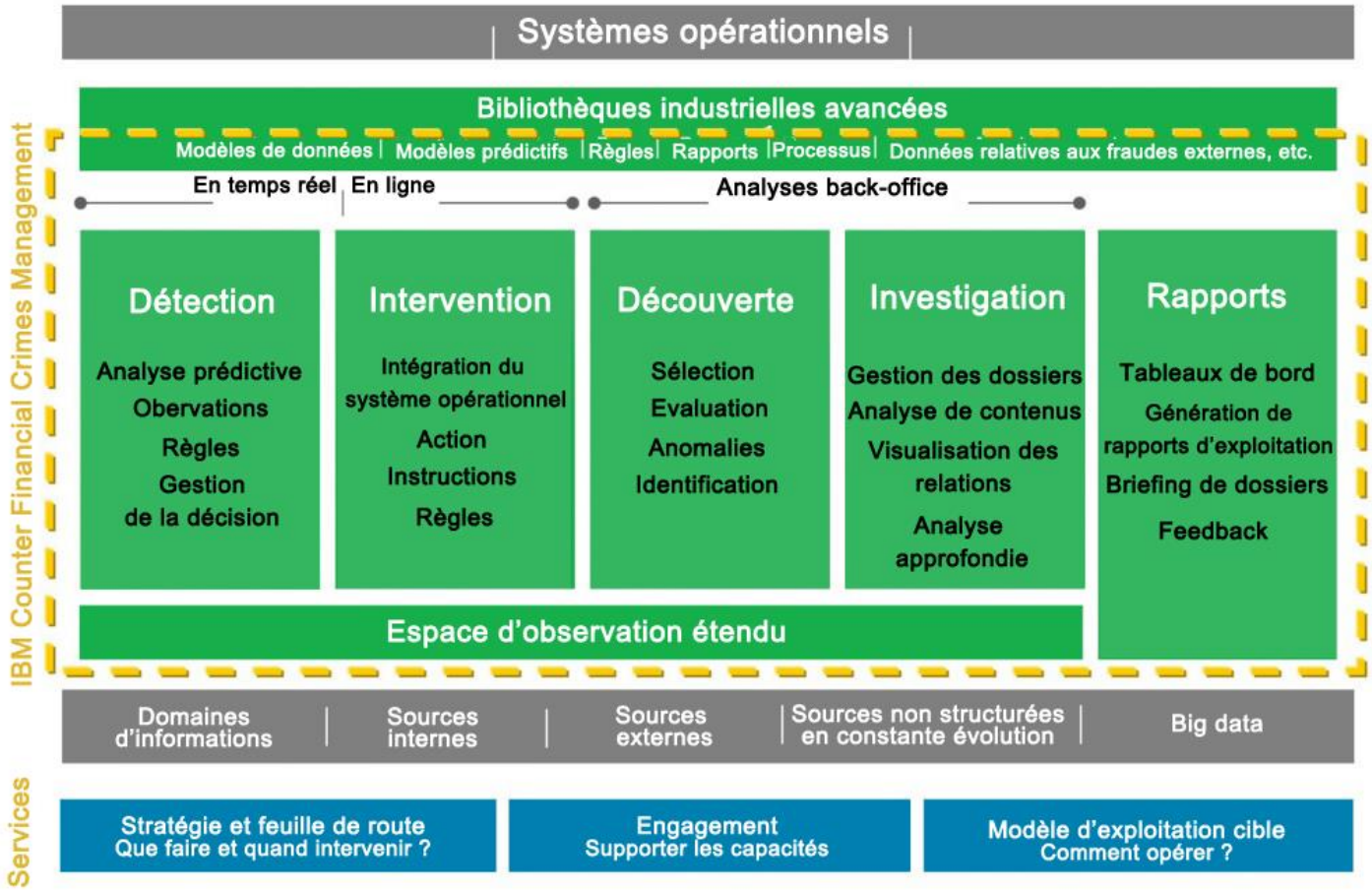

Figure 2 : Le logiciel IBM Counter Financial Crimes et ses services forment une solution globale.

Conçu pour suivre et résoudre les activités frauduleuses durant l'intégralité du cycle de vie de la transaction financière, IBM Counter Financial Crimes Management for Banking fournit d'importantes informations permettant de prendre des décisions proactives et anticipées pour se conformer aux quatre composants opérationnels suivants : *Détection, intervention, découverte* et *investigation*. Ces informations répondent aux besoins de tous les services de l'entreprise et offrent aux unités d'investigation spéciales et aux unités d'investigation financières des capacités d'analyse approfondies et uniques.

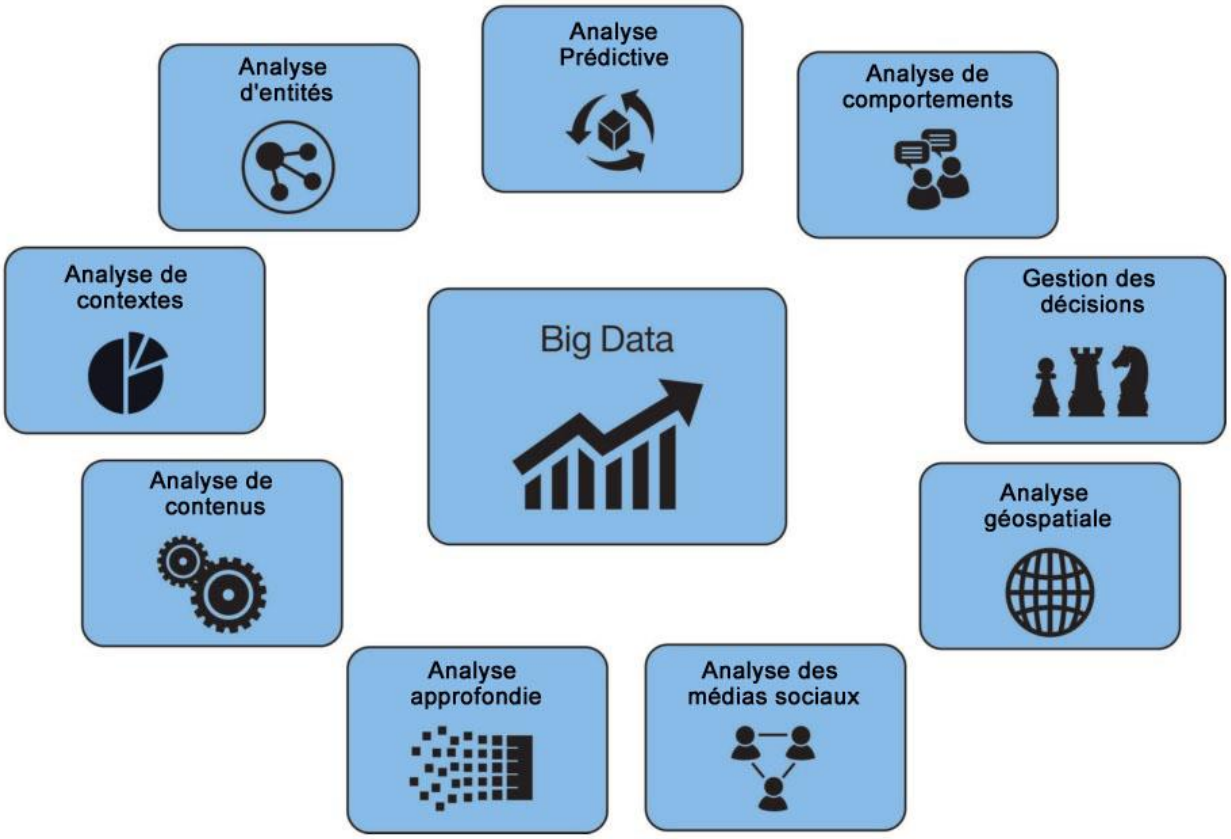

Figure 3 : IBM combine plusieurs types et couches d'analyse pour combattre les délits financiers.

Quatre composants clés

Détection : la lutte contre la fraude nécessite une stratégie de défense approfondie, dotée de plusieurs techniques et outils d'analyse pour faire face aux menaces d'aujourd'hui et de demain. La couche de détection mélange une vaste gamme de fonctionnalités pour adopter la stratégie appropriée à chaque problème. Il peut s'agir d'analyses d'entités, de règles, de modèles statistiques, d'analyses prédictives, d'analyses réseau, d'informations géospatiales et non structurées et de Big Data. La vitesse est importante, particulièrement lorsqu'il s'agit d'analyser des transactions en temps réel et d'utiliser des ensembles de données de plus en plus importants. La possibilité d'utiliser des systèmes NoSQL et de distribuer les analyses entre différents serveurs, y compris de façon native sur le matériel IBM, permet de rapprocher les analyses et les données et ainsi d'augmenter la vitesse et de réduire le mouvement des données. De plus, ces outils d'analyse ne sont pas basés sur un modèle associatif de type boîte noire nécessitant des mises à jour périodiques du fournisseur. Cette solution IBM donne au contraire à votre organisation un contrôle et une visibilité accrus grâce à des outils éprouvés et des compétences techniques largement accessibles. Le contrôle et la visibilité sont appréciés par les parties prenantes, tandis que les outils et fonctionnalités permettent à l'organisation de s'adapter aux menaces en constante évolution.

Intervention : les informations précises supplémentaires vous permettent de répondre aux menaces en toute confiance et de prendre des actions légitimes, tout en empêchant ou en interrompant les actions suspicieuses par une réponse immédiate aux modèles, activités et intentions criminels. Des réponses rapides incitent les criminels à rechercher des cibles plus faciles et protègent vos clients avec un service amélioré.

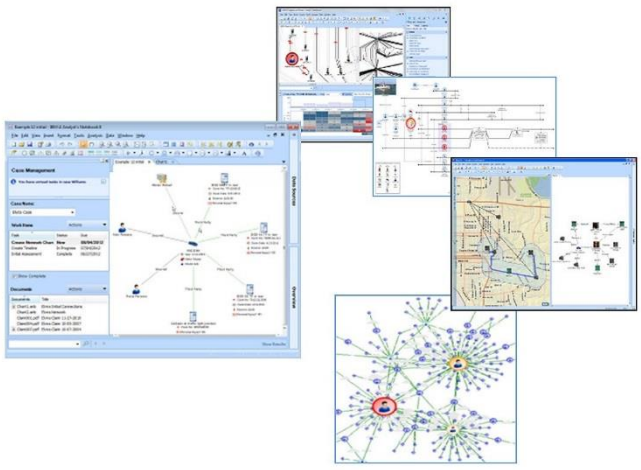

Figure 4 : Utilisation d'analyses approfondies pour découvrir des relations cachées.

Investigation : les équipes d'investigation peuvent s'appuyer sur des fonctions complètes immédiatement disponibles concernant la connaissance des clients, la sélection de listes, le blanchiment d'argent et différents types et cas d'alerte, ainsi que sur des fonctions de configuration de changements spécifiques aux clients sans codage. Les systèmes d'alerte et de gestion des dossiers s'appuient sur une base commune de données de délits financiers. La présence de différents types et cas d'alerte sur une infrastructure partagée permet de réduire les coûts et d'augmenter l'efficacité. Les demandes groupées permettent de minimiser les mouvements de données et offrent des calendriers et des jalons pour mieux interpréter les informations de dossiers, des capacités de modification complète dans les commentaires des rapports d'activités suspectes et de recherche de texte non structuré dans tous les documents et toutes les données. Un processus de gouvernance établi valide les nouvelles règles, les nouveaux modèles et les nouvelles listes de contrôle essentiels à la boucle de rétroaction durant le cycle de vie de gestion. Il est ainsi possible de gérer les changements dynamiques dans la lutte contre la fraude et le blanchiment d'argent.

Découverte : la solution comprend un ensemble complet de fonctionnalités d'analyse incluant une analyse visuelle approfondie de pointe, l'identification des activités suspectes grâce à une analyse rétrospective des données d'historique, l'analyse des modèles et la génération de listes de surveillance pour identifier les individus ou les organisations susceptibles de mener des activités frauduleuses. Les fonctions d'analyse de contenu exclusives permettent de rechercher des informations et des modèles dans les données non structurées.

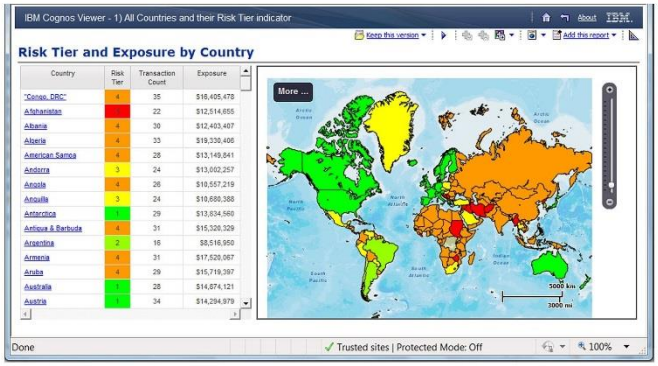

Figure 5 : Les tableaux de bord complets affichent des informations concises accessibles en un coup d'œil.

Les tableaux de bord complets regroupent les informations en provenance des quatre composants pour offrir une vue concise et informative du processus de gestion des délits financiers. Les rapports système permettent d'analyser les expositions existantes et potentielles et l'efficacité des procédures actuelles. Les visualisations illustrent les corrélations contextuelles, qui permettent aux membres de l'équipe de disposer d'informations approfondies en termes de blanchiment d'argent et de fraude. Les alertes hiérarchisées visuelles permettent de confirmer les tentatives de fraude et de blanchiment d'argent, tout en identifiant d'autres parties prenantes d'un réseau malveillant et de blanchiment d'argent d'ampleur. Ces deux composants forment le moteur de l'efficacité.

Spectre de cas d’utilisation de lutte contre la fraude et de conformité

Les solutions IBM Counter Financial Crimes Management permettent de contrôler le cycle de vie client au niveau des individus, des transactions et des appareils à n'importe quelle phase, de la détection à l'investigation.

- Les cas d'utilisation de blanchiment d'argent, incluent, mais sans s'y limiter, une fonctionnalité de sélection de sanctions intégrant des analyses de pointe pour résoudre un nom en fonction de listes de sanctions publiées, des listes de contrôle relatives au secteur et des listes de personnes politiquement exposées, une évaluation de la connaissance des clients pour les nouveaux comptes et une réévaluation continue du cycle de vie, ainsi qu'une fonction de contrôle des transactions de blanchiment d'argent.

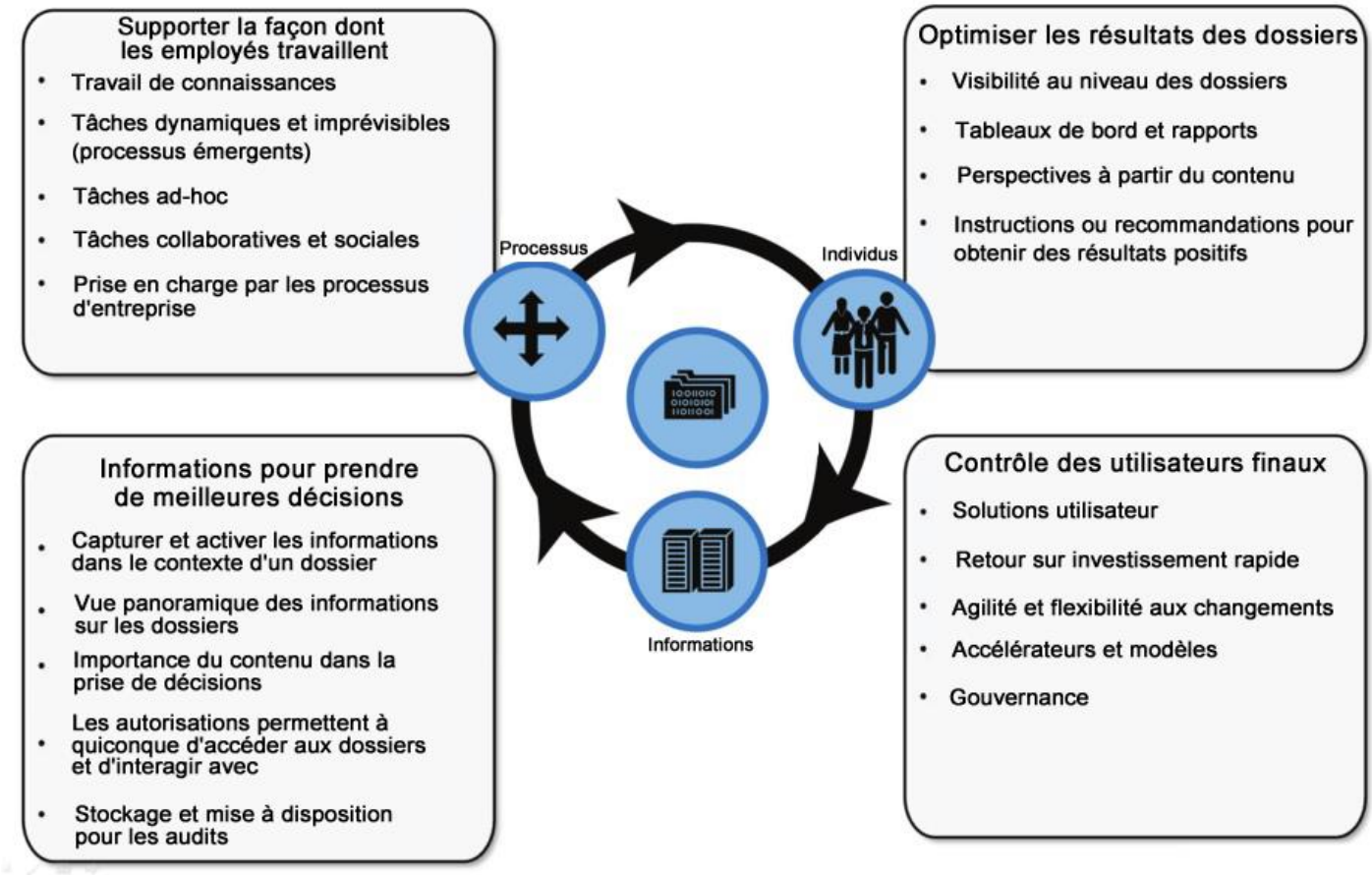

Figure 6 : La solution IBM Counter Financial Crimes Management for Banking vous offre le contrôle nécessaire pour façonner la solution adaptée à votre activité. Vous disposez d'informations vous permettant de prendre de meilleures décisions, d'optimiser les résultats des dossiers et de prendre en charge la direction de votre activité.

- Les cas d'utilisation de lutte contre la fraude couvrent plusieurs types et canaux de paiement tels que les dépôts à distance (chèques), le contrôle des virements et via le système ACH à la recherche de fraudes, de sanctions, d'abus d'employés sur les comptes client, de prise de contrôle de comptes et de stratégies frauduleuses. Chaque scénario de fraude nécessite de mélanger différentes techniques de détection dans une solution unique comprenant des règles, des profils, des modèles prédictifs et des analyses non structurées, de réseau, d'entité et géospatiales. Cette solution prend en charge la sélection en temps réel et la sélection par lots. Elle utilise des connecteurs préconfigurés à IBM et des sources tierces pour offrir des modèles contenant des informations contextuelles complètes sur l'identité, les appareils, le comportement de la session, les centres de paiement et bien plus encore. En augmentant l'espace d'observation, les taux de détection augmentent et les taux de faux positifs baissent. La détection des fraudes nécessite une analyse adaptative et flexible capable de suivre les changements des stratégies de fraude. IBM propose une analyse ouverte facile à modifier et à ajuster en fonction des exigences en constante évolution.
- Les cas d'utilisation multi-canaux analysent généralement des ensembles de données limités, voire des typologies uniques. Grâce à la solution IBM, les cas d'utilisation multi-canaux viennent compléter les moteurs de détection existants. Ils appliquent des modèles prédictifs et des données extra-contextuelles pour regrouper plusieurs sources d'informations afin de détecter les activités organisées lucratives tout en réduisant le nombre de faux positifs.
- Les équipes de tri d'alertes et les unités d'investigation financières peuvent utiliser une infrastructure d'investigation et de données commune dotée d'un centre de gestion des investigations solide et de fonctions d'analyse des textes non structurés, d'analyse des liens et de génération de rapports. De plus, vous disposez toujours de la flexibilité nécessaire pour prendre en charge les différents écrans et processus des différentes équipes. La boucle de rétroaction permet d'obtenir des informations sur les processus de découverte et d'investigation passés afin de trouver des activités liées et alimenter des algorithmes de détection à l'aide de ces informations. Cette méthode permet de mieux détecter les incidents inter-canaux et les tentatives de fraudes d'ampleur sur des services par des organisations criminelles.

Avantages d'IBM Counter Financial Crimes Management for Banking

Le logiciel IBM Counter Financial Crimes Management for Banking apporte les avantages suivants :

- Fournir une solution unique capable de détecter les tentatives de fraude, de blanchiment d'argent et d'activités de cybercriminalité
- Réduire le nombre d'alertes faussement positives et vraiment négatives tout en améliorant la qualité des alertes
- Découvrir plus rapidement les stratégies de produits et multi-canaux complexes et suspectes
- Différencier rapidement les fraudeurs des clients honnêtes
- Améliorer l'efficacité des analystes et des investigateurs
- Réduire les pertes et minimiser l'impact sur l'expérience client
- Respecter les exigences relatives aux réglementations
- Utiliser la veille d'entreprise pour ajuster continuellement les opérations et rester à l’avant-garde des tendances

Un partenaire à long terme qui vous permet de vous adapter en fonction de l'évolution des menaces

Grâce à IBM et à la solution IBM Counter Financial Crimes Management for Banking, les organisations avant-gardistes peuvent lutter de manière proactive et plus efficacement contre la fraude, le blanchiment d'argent et les cyber-menaces pour améliorer les résultats commerciaux et réduire les pertes tout en conservant une expérience client positive. Pour offrir une stratégie complète et puissante et permettre à ses clients de gérer efficacement la fraude, IBM a développé un logiciel interne et y a intégré des acquisitions stratégiques de fonctions de service et de logiciels d'analyse et de Big Data, ainsi que des méthodes d'analyse de pointe issues de 12 laboratoires de recherche et 290 brevets liés à la gestion des fraudes. IBM apporte de la valeur en se basant sur les préceptes suivants :

- **Innovation.** IBM fait avancer *massivement* les secteurs de l'apprentissage machine et de l'application pratique de ces techniques d'analyse pour gérer le risque dans le cycle de vie du délit financier.
- **Renseignement.** L'association de l'équipe de renseignement IBM Red Cell et des offres de sécurité d'IBM, telles que IBM X-Force® et Trusteer, permet de réduire l'exposition aux menaces et activités frauduleuses liées à la cybercriminalité et à la fraude.
- **Simplicité.** IBM offre tous ces composants techniques dans une solution unique adaptée à un ou plusieurs cas d'utilisation de conformité ou de lutte contre la fraude. Les données, modèles, composants de dossiers, rapports et API sont transparents. Vous pouvez donc configurer le système en fonction de vos besoins métier.

Pour plus d'informations

Pour en savoir plus sur IBM Counter Financial Crimes Management for Banking, contactez votre représentant IBM ou accédez à la page **ibm.com**/smartercounterfraud

Compagnie IBM France
17 avenue de l'Europe
92275 Bois Colombes Cedex

Imprimé en France
Août 2014

KIS03004-FRFR-01