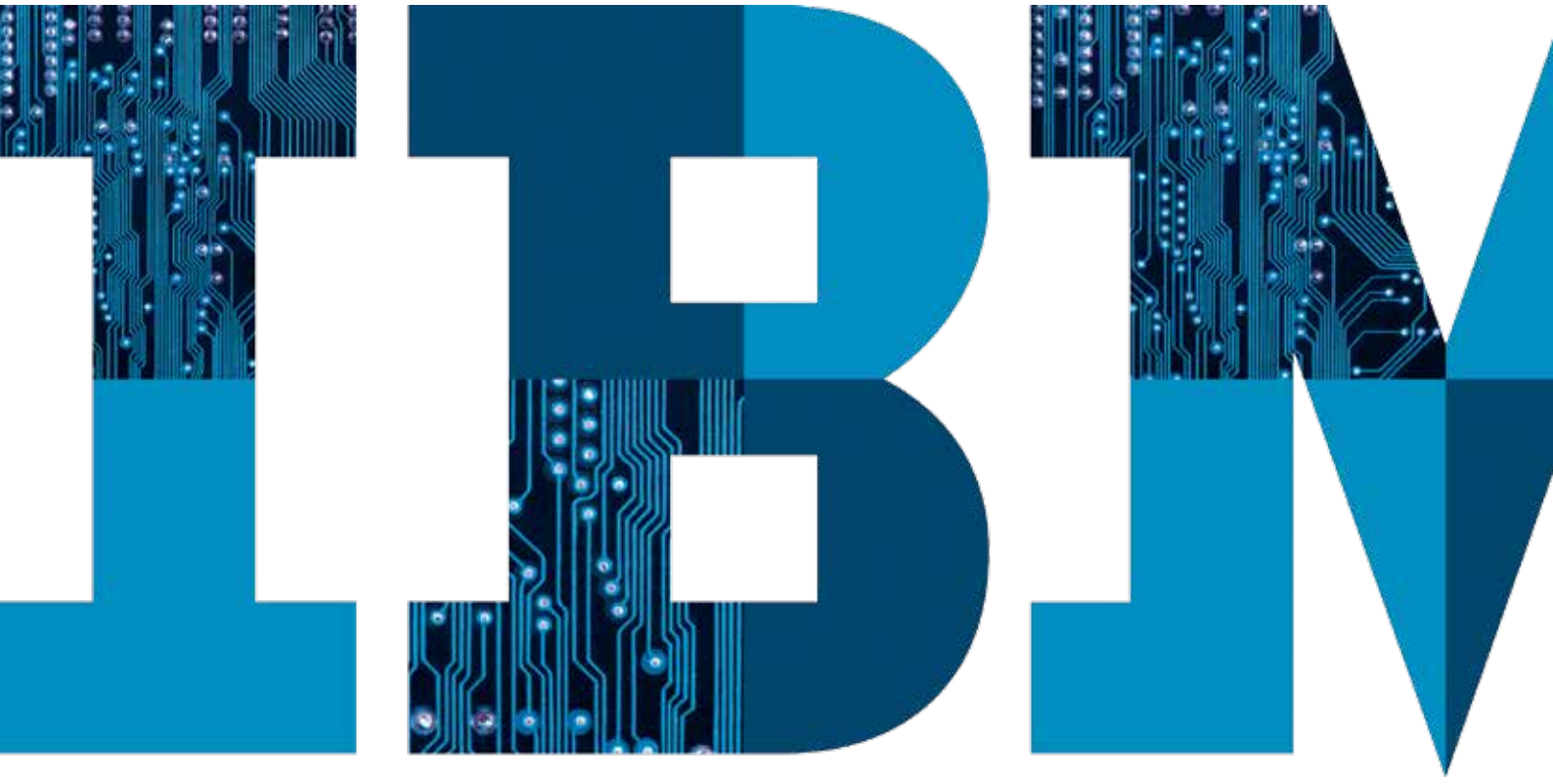
# L'analyse prédictive des menaces et des fraudes : relever les défis de la Smarter Planet



IBM

## Sommaire



## Introduction

Une planète plus intelligente est source de nouvelles possibilités, mais aussi de complications et de risques inédits. Grâce aux progrès récents de la technologie, avec l'apparition des périphériques mobiles, du cloud computing et des média sociaux, nous avons créé un univers interconnecté, instrumenté et intelligent, dans lequel l'accès à l'information est quasiment sans limite. Cette mutation a ouvert la porte à des possibilités passionnantes et sans précédent, mais est aussi à l'origine des menaces et de vulnérabilités nouvelles. Les entreprises sont confrontées chaque jour à une multitude de menaces, provenant tant de l'extérieur (sécurité du territoire national, contexte économique) que de l'intérieur (fraude des employés, risque crédit et gestion de l'information). Le nombre et la gravité de ces menaces ne cessent de s'accentuer et peuvent se solder par des millions, voire des milliards de pertes pour les entreprises.

Exemples :

- Selon une enquête récente de l'Association of Certified Fraud Examiners, 5% du chiffre d'affaires d'une entreprise est en moyenne englouti par la fraude chaque année. Le montant annuel des fraudes dans le monde entier est estimé à plus de $3,5 billions. [1]
- Près de la moitié des entreprises victimes de fraudes ne peuvent jamais récupérer leurs pertes. [2]
- La National Health Care Anti-Fraud Association a calculé qu'aux Etats-Unis, les coûts des fraudes aux soins de santé sont de $68 milliards par an. D'autres estimations atteignent jusqu'à $230 milliards. [3]
- Le coût total de la fraude à l'assurance (hors assurance-santé) est estimé à plus de $40 milliards par an, soit un coût de plus de $700 à supporter pour une famille américaine moyenne sous la forme d'une augmentation des primes d'assurance, selon le FBI.[4]
- Dans le monde, le coût total des fraudes à la carte de crédit est évalué à $5,5 milliards. Aux seuls Etats-Unis, 10% des citoyens sont victimes d'escroqueries à la carte de crédit. [5]

Il n'est donc pas surprenant que la diminution des menaces et des fraudes soit devenue une priorité essentielle des entreprises. En plus des pertes financières, l'atteinte à la réputation et à l'image de marque d'une entreprise mal préparée à la problématique des fraudes peut aussi coûter très cher. Selon une étude récente internationale d'IBM sur les cadres supérieurs, 75% déclarent que les vols de données et les cyber-attaques ont un impact sur la satisfaction des clients et la réputation de la marque. Pour 61 %, ce sont les facteurs qui mettent le plus en péril la réputation de leur société. [6]

La meilleure défense contre les menaces et les fraudes est une approche systématique qui permet de réduire la vulnérabilité et d'atténuer l'impact négatif. Mais par où commencer ? Dans un univers en perpétuelle mutation, vous devez être très attentif à gérer aussi bien les menaces dont vous avez conscience que celles qui vous sont inconnues. Par exemple, vous devez pouvoir anticiper comment un employé pourrait infiltrer vos systèmes informatiques sécurisés, rechercher des signes d'activités terroristes éventuelles, prévoir l'impact probable des événements économiques ou identifier les nouvelles tendances à la fraude, le tout avec une très grande précision.

Dans cet article, nous allons voir comment construire une stratégie proactive de gestion des menaces s'appuyant sur la technologie d'analyse métier, puis comment distribuer ces informations aux personnes chargées de faire changer les comportements indésirables. Nous allons voir comment des entreprises du monde entier ont recours à des solutions d'analyse métier pour atténuer l'impact néfaste du risque et accentuer les résultats positifs. Vous allez aussi découvrir les procédures pratiques que vous pouvez appliquer pour lutter contre les menaces et les fraudes dans l'entreprise.

## Qu'est-ce que l'analyse métier ?

Le terme « analyse métier » désigne une approche complète et déterminée par les données, qui associe la science de l'analyse prédictive à des fonctionnalités sophistiquées d'information décisionnelle. L'analyse prédictive fait appel à des algorithmes d'analyse avancés pour traiter des données historiques et créer des modèles pouvant permettre de faire des prévisions concernant les résultats futurs. L'information décisionnelle fournit ensuite des éléments de prédiction aux personnes et aux services principaux concernés dans l'entreprise afin de les aider à atteindre leurs objectifs.

Chacune de ces technologies est puissante de par sa nature même. Associées à l'analyse métier, elles créent une solution d'exception qui permet d'améliorer les performances métier dans de très nombreux domaines fonctionnels. Selon la société d'analystes IDC, les entreprises qui cumulent l'utilisation de l'analyse prédictive et de la business intelligence obtiennent un retour sur investissements moyen de 250 pour cent.[7]

Les logiciels d'analyse métier modernes sont faciles à utiliser et peuvent être employés par des utilisateurs ayant différents niveaux de compétences, des professionnels en contact avec le public aux analystes expérimentés. Les entreprises de nombreux secteurs d'activité différents appliquent l'analyse prédictive pour comprendre leurs clients, augmenter leur profitabilité et améliorer leur efficacité opérationnelle. Appliquée à la prévention des menaces et des fraudes, cette technologie offre des avantages similaires. En fournissant des conclusions fiables sur les conditions existantes et les événements futurs, elle permet d'établir un plan d'action efficace basé sur ces données.

## Limiter les vulnérabilités et atténuer l'impact

La multiplication des exigences réglementaires, la croissance des transactions en ligne et des communications, la prolifération des périphériques mobiles et la menace constante de l'incertitude économique soulignent l'importance d'une gestion proactive des menaces sous toutes leurs formes – et ce, qu'elles concernent les entreprises, les données ou les événements. Il s'agit non seulement de comprendre les événements antérieurs, mais d'être capable d'anticiper l'avenir, et de déterminer la façon dont votre entreprise va réagir à ces situations. Une solution d'analyse performante permet aux entreprises d'optimiser leur efficacité et de réduire l'impact des menaces. En outre, c'est aussi pour elles un moyen de différencier leur modèle de gestion par rapport aux concurrents qui n'ont pas adopté une culture de l'analyse.

L'analyse métier est cruciale pour atténuer les vulnérabilités et défendre l'entreprise des milliers de menaces auxquelles elle est confrontée chaque jour. Elle permet d'accéder en temps réel à des éclairages prédictifs reposant sur des faits concrets, paramétrés en fonction des besoins spécifiques de votre entreprise.

L'environnement dynamique actuel nécessite une approche systématique de la gestion des menaces. En utilisant l'analyse prédictive tout au long de votre cycle décisionnel, vous affinez continuellement vos décisions et vos choix stratégiques. Vous maîtrisez la situation et prenez des mesures fondées sur des connaissances concrètes. Comme le montre la Figure 1, utiliser l'analyse métier, c'est se donner de nombreux atouts :

- Vous définissez des paramètres et des règles souples et tournés vers l'avenir, mais tenant aussi compte des événements antérieurs, des nouveaux défis, et des changements internes ou externes – qu'il s'agisse de facteurs climatiques ou de modifications des réglementations.
- Vous surveillez votre environnement en continu, en vous appuyant sur des données très diversifiées provenant de nombreuses sources. Vous ajoutez de nouvelles données si besoin est et en retirez des enseignements. Les connaissances obtenues vous aident à identifier des déclencheurs et des alertes.
- A l'aide de l'analyse métier, vous détectez les comportements suspects tels que les menaces, les vols de données, les actes criminels et la fraude afin d'identifier les anomalies et de déterminer le risque potentiel lié à une action.
- Vous interceptez ou laissez passer une menace potentielle en fonction de son impact prévisible sur votre entreprise. Vous éliminez ou gérez le risque, en appliquant une stratégie maîtrisée, déterminée par les résultats, qui réduit les risques ou les pertes, et optimise l'impact positif de toute action exécutée. Par exemple, une banque peut analyser les informations d'un client sollicitant une carte de crédit, son état-civil, son ancienneté chez son employeur actuel et son salaire, et calculer son risque relatif de défaut de paiement. La banque peut ainsi conclure que le risque de défaut de paiement n'est pas assez élevé pour qu'elle refuse la demande de carte de crédit, mais néanmoins décider de ne pas proposer la carte à un taux d'intérêt faible afin d'amortir une part du risque qu'elle va assumer.

Comme vous pouvez le constater, le cycle est continu : lorsque vous obtenez de nouvelles données, vous les analysez et en tirez des enseignements. Les connaissances obtenues vous permettent d'améliorer vos règles et vos paramètres et de protéger en permanence votre entreprise contre les risques à chaque étape.

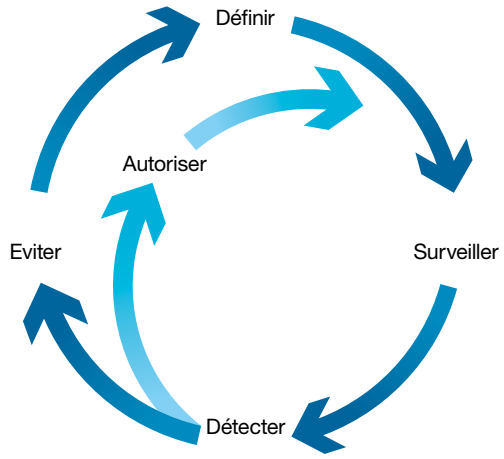



*Figure 1* L'environnement dynamique actuel nécessite une approche systématique de la gestion des menaces et des risques.

Maîtriser l'analyse prédictive est un long processus qui consiste à exploiter d'abord les informations disponibles pour en extraire des connaissances, puis à déterminer la marche à suivre la mieux adaptée à un individu, un scénario ou un décisionnaire particulier. Les techniques d'analyse métier permettent aux entreprises d'identifier les principales menaces, de s'adapter aux réglementations, ou d'affiner et surveiller leurs règles, en s'appuyant sur leur connaissance des événements antérieurs ainsi que sur les données obtenues en temps réel.

Voici quelques exemples de scénarios :

- L'entreprise s'aperçoit qu'une demande de remboursement médical ou de sinistre automobile est de nature frauduleuse lors de son traitement.
- Des policiers sont envoyés dans les secteurs les plus visés par une hausse de la criminalité à certaines dates, en fonction de facteurs de prédiction tels que la météorologie, les comportements de la veille, le jour de la semaine ou d'autres éléments.
- L'entreprise repère un employé qui semble subitement se livrer à des activités anormales sur le réseau ou à des opérations suspectes sur les données.
- L'entreprise fournit des rapports de renseignements actualisés et personnalisés sur les menaces à certains employés, afin de leur permettre d'anticiper et de résoudre les risques dans leurs domaines de responsabilité.

Disposer de certaines réponses par avance permet de décider des mesures à prendre et du moment où agir, et ainsi de planifier, d'implémenter et de prévenir. Faute d'analyse, vous ne pouvez réagir qu'à posteriori, après qu'une menace a été identifiée, au lieu d'appliquer une procédure maîtrisée et clairement définie qui vous garantira les meilleurs résultats possibles. Les conséquences peuvent être très lourdes pour l'entreprise : coûts élevés en termes de pertes de chiffre d'affaires ou d'opportunités, baisse de la crédibilité auprès des employés, des partenaires et des investisseurs, retombées nuisibles pour l'environnement, ou, dans le plus noir des scénarios, une perte de vies humaines.

**En mettant en place une stratégie de gestion des risques s'appuyant sur l'analyse métier, vous pouvez :**

- **Accéder en temps réel aux informations sur les menaces dans toute l'entreprise, afin de déterminer le meilleur moment auquel accepter le risque ou le stopper net.**
- **Prendre des décisions plus rapidement et passer moins de temps à « éteindre des incendies. »**
- **Avoir plus confiance envers les décisions prises.**
- **Réduire les coûts et tirer le meilleur profit des ressources.**
- **Créer une entreprise plus solide, suffisamment résiliente face au changement et prête à exploiter de nouvelles opportunités.**
- **Soutenir l'innovation métier tout en réduisant le niveau de risque opérationnel ou en le maintenant à un niveau acceptable.**
- **Eviter la publicité négative.**

## Identifiez les menaces organisationnelles avec l'analyse métier

Les tendances révélatrices de menaces ou de comportements suspects sont souvent noyées dans des masses énormes de données. Pour cette raison, une approche proactive de la gestion des menaces commence par l'analyse des masses de données recueillies et stockées par votre entreprise : par exemple, données transactionnelles, emails, rapports réseau, données d'enquêtes, information sur les contribuables, dossiers fiscaux et notes des centres d'appels. Il est tout aussi important de surveiller et d'analyser les quantités gigantesques d'informations qui transitent par les média sociaux tels que les sites de réseautage, les blogs et les sections des commentaires des sites Web.

Les solutions d'analyse métier comportent des techniques sophistiquées qui permettent à l'entreprise d'analyser aussi bien les données dites « structurées » résidant dans les tables et les bases de données que les données « non structurées », telles que le contenu des emails, des forums de discussion, des réseaux sociaux et des données d'enquête. Contrairement aux seules méthodes de détection et d'analyse régies par des règles, l'analyse métier est capable d'identifier des comportements relativement inhabituels, même ceux présentant des différences subtiles qui échappent souvent aux autres méthodes. Du fait que de nouvelles tendances apparaissent et se modifient avec le temps, ce processus facilite aussi l'identification des nouvelles menaces.

L'entreprise a ainsi la possibilité de combiner des types de données diversifiés, y compris des données spécifiques à son secteur d'activité en termes de tests de performances ou de données externes. L'analyse métier permet de combiner régulièrement une grande variété de dimensions, de types et de sources de données.Elle offre la possibilité de détecter rapidement et de manière fiable les signatures involontaires laissées par les pirates informatiques, les criminels ou les terroristes lorsqu'ils créent de nouvelles cyber-discussions. Elle permet aussi de tester des tactiques originales d'accès aux informations sensibles, ou de calculer le risque de crédit d'un individu. Vous avez à votre disposition différentes techniques qui vous aident à décider de la meilleure marche à suivre.

Lorsque vous comprenez vos données, et savez différencier les comportements normaux des comportements inhabituels, vous pouvez élaborer des facteurs prédictifs fondamentaux, ou des indicateurs de menaces potentielles. Vous pouvez ensuite les combiner à vos indicateurs clés de performance afin de mettre en évidence les aspects susceptibles de menacer votre entreprise. Vous pouvez alors commencer à fonder vos décisions opérationnelles et stratégiques sur des renseignements prédictifs qui indiquent non seulement les résultats et les comportements futurs, mais décrivent aussi en détail les facteurs influençant ces événements. Vous apprenez ainsi à gérer proactivement les menaces et à les arrêter avant même qu'elles ne surviennent.

L'analyse métier permet aussi à l'entreprise de fournir des modèles et des règles métier qui viennent appuyer des décisions cohérentes et optimisées au « point d'impact. » Voici un exemple concret : vous pouvez transmettre directement les résultats d'une analyse aux principaux interlocuteurs concernés, sous la forme de rapports d'information décisionnelle, de tableaux de bord ou de représentations graphiques faciles à lire (graphiques, cartes). Les employés reçoivent des rapports personnalisés adaptés à leurs problématiques particulières. Ils peuvent alors explorer plus en détail les données pour identifier les causes premières et comprendre plus en profondeur le contexte, et ainsi mieux prévoir et empêcher les retombées néfastes des menaces.

Ces indications peuvent aussi être incorporées aux systèmes opérationnels tels que les sites Web et les centres d'appels afin d'accompagner des décisions et des actions plus intelligentes, en harmonie avec la stratégie et les objectifs globaux de l'entreprise. L'intégration de l'analyse crée une couche vitale de décisions optimisées, permettant au personnel d'une entreprise ou à des systèmes automatisés d'interagir avec les clients, les fournisseurs ou les partenaires. L'information sur les résultats permet ensuite d'affiner les modèles prédictifs et les actions futures recommandées.

Nous allons maintenant examiner quelques domaines dans lesquels les stratégies de contrôle des risques et des menaces basées sur l'analyse métier sont particulièrement efficaces.

## Eliminez les menaces venues de l'intérieur

Dans la plupart des entreprises, les données se sont transformées en une ressource d'une valeur inestimable. Elles sont devenues la pierre angulaire de leurs opérations. L'accès à ces données est désormais ouvert à un groupe d'utilisateurs de plus en plus vaste, comprenant employés, partenaires commerciaux, fournisseurs et clients. Les infrastructures informatiques sont plus étendues, plus complexes, plus distribuées, et aussi plus accessibles. Cette interconnexion se traduit par de nombreux avantages pour les entreprises, les organismes gouvernementaux et les consommateurs, mais implique aussi de gros risques potentiels. Les entreprises et les organismes gouvernementaux doivent respecter des exigences strictes en matière de réglementation et protéger leur capital intellectuel contre la concurrence ou des entités politiques malveillantes. Les consommateurs sont surtout préoccupés par le risque du vol d'identité et des violations de confidentialité.

Le scandale WikiLeaks dans lequel s'est retrouvé impliqué l'US State Department est un exemple idéal de l'un des principaux défis à la sécurité des données : le délit d'initié, posé par un usager interne doté de toutes les autorisations adéquates. Dans ce cas précis, des quantités considérables de documents secrets – dont plusieurs milliers de messages d'ambassades et plusieurs centaines de milliers de documents concernant la guerre en Afghanistan et en Irak – avaient été copiés par des utilisateurs autorisés sur des CD et des DVD et envoyés à WikiLeaks.

Les analystes des intrusions au sein d'un organisme gouvernemental sont souvent submergés par plusieurs millions d'événements par jour, dont beaucoup sont des demandes de mappage ou une collecte d'information et non de réelles menaces. Ce nombre phénoménal d'événements rend difficile la détection des attaques réelles ou des problèmes potentiels. A l'aide des logiciels IBM d'analyse métier, les analystes peuvent se concentrer sur les alarmes les plus préoccupantes, et dans un cas précis, ils ont ainsi réussi à réduire le nombre d'événements nécessitant un examen manuel de 97 % sur une seule période de 30 jours.

Les menaces liées au délit d'initié ne sont pas spécifiques au secteur public ou militaire. Toute entreprise détenant des informations métier sensibles telles que des comptes de résultats, des projets de fusion et d'acquisition, des plans marketing, des données de recherche et de développement, des informations personnelles identifiables ou des emails internes confidentiels sont en danger.

L'un des plus grands sujets de préoccupation dans le secteur de la santé est ainsi le vol des données sensibles. Plusieurs grands noms dans ce secteur ont récemment été victimes de vols d'informations de santé personnelles en raison de l'insuffisance de leurs dispositifs de protection. Par exemple, l'Utah Department of Health déclare que les numéros de sécurité sociale, les adresses, les diagnostics médicaux, les dates de naissance et d'autres informations confidentielles de 780 000 patients ont été compromis lors d'une attaque de pirates informatiques en 2012. Il ne s'agit pas là d'un incident isolé. Les gouvernements estiment que plusieurs centaines de milliers de dossiers patient ont été dérobés à divers organismes de santé. [8]

L'affaire WikiLeaks et les attaques contre le secteur de la santé démontrent à quel point il est vital de mettre en œuvre une technologie d'analyse métier pour éviter les vols de données.

## Limitation du risque lié aux cartes de crédit

Sur le marché financier tumultueux d'aujourd'hui, les organismes émetteurs de cartes de crédit doivent être aussi bien renseignés que possible sur leurs clients. Ils doivent comprendre les facteurs et les comportements indiquant si un client potentiel présente un bon risque de crédit. De même, ils doivent savoir déceler les schémas ou les tendances pouvant faire soupçonner un risque de défaut de paiement ou de retards de règlement chez un client ou un prospect. En outre, ils doivent élaborer des stratégies plus sophistiquées pour fidéliser les bons clients et limiter les risques liés aux clients non rentables. Le logiciel IBM Business Analytics permet aux entreprises de concevoir des modèles de crédit basés sur une stratégie de segmentation plus affinée, prenant en compte les données individuelles spécifiques à un client. Il permet ainsi de mettre en adéquation les politiques de crédit avec le niveau de risque du client et de garantir un résultat aussi rentable que possible.

En Suisse, un organisme bancaire privé indépendant a amélioré son système de gestion du risque crédit en mettant en place un nouveau système de notation du risque crédit basé sur le logiciel IBM Business Analytics. La solution a permis à cet organisme d'améliorer la gestion du risque crédit et la procédure globale de collecte, et a réduit les impayés de 15 %.

## Détection et prévention de la fraude

La fraude est un problème qui coûte plusieurs milliards de dollars aux pays et aux industries. L'étendue des fraudes et l'ingéniosité des fraudeurs posent un formidable problème à ceux qui sont chargés de leur détection et de leur prévention. Ces activités criminelles ont cependant une chose en commun : chacune laisse dans son sillage des données comportementales et transactionnelles – demandes de remboursement d'assurance, demandes de prêts hypothécaires ou de perception de bénéfices, remboursements de santé, demandes de dégrèvements fiscaux, etc. – qui sont enregistrées au même titre que l'information provenant des interactions légitimes. Une analyse classique permet de détecter une fraude après coup. En revanche, les logiciels IBM Business Analytics peuvent eux prévoir les événements risquant de se produire, et détecter les événements en temps réel. Ils fournissent des renseignements cohérents sur la fraude aux équipes en première ligne, afin de leur permettre de prendre les fraudeurs en flagrant délit, voire de les empêcher d'agir.

- Le département de lutte anti-fraude d'un pays d'Europe du sud a implémenté les technologies IBM Business Analytics afin de détecter les fraudes de façon beaucoup plus rapide, efficace et simple, grâce à une identification précise et automatique des contribuables à haut risque.
- Dans le monde entier, les grands organismes de santé utilisent les solutions IBM Business Analytics afin d'atténuer les répercussions des fraudes aux remboursements. Ces solutions leur permettent de détecter en amont les cas de fraudes probables avant que leur règlement n'intervienne.
- Les services de gestion des remboursements et des garanties peuvent réduire les coûts et améliorer la relation avec les fournisseurs en redirigeant les demandes de remboursements dans le cadre d'une garantie et en les présentant ces informations à l'aide de méthodes de reporting dans les systèmes de gestion des demandes.

## Réduisez les pertes sur stock

L'analyse métier permet d'identifier les produits, les conditions dans les magasins, et les employés ou les clients ayant une responsabilité potentielle dans la démarque inconnue. Les solutions IBM de gestion de la démarque inconnue permettent aux fournisseurs de connaître la performance d'un produit et d'un magasin, en vue de contrôler le stock et les activités frauduleuses, et améliorent la rentabilité des opérations en magasin.

## Evaluation des pannes du réseau

L'analyse métier permet aux opérateurs de télécommunications ou à la grande distribution d'améliorer la gestion des ressources réseau en prévoyant la défaillance d'un réseau et l'impact de cet événement sur les opérations et l'expérience client. Les solutions IBM Business Analytics permettent aux entreprises d'agir rapidement pour réparer les réseaux à fort trafic exposés au risque et leur éviter tout temps d'indisponibilité, et, par conséquent, l'insatisfaction des clients et la perte de chiffre d'affaires.

## Prévention des fraudes énergétiques

Les fraudes énergétiques peuvent être difficiles à détecter. Elles entraînent de très grosses pertes financières pour les producteurs d'énergie et se soldent par une hausse des prix pour les consommateurs. Les solutions IBM Business Analytics contribuent à éviter les fraudes énergétiques ou le vol d'énergie en détectant les activités suspectes, en se basant sur la distribution, la consommation, la tarification et des compteurs intelligents, puis en déterminant les stratégies d'intervention appropriées. Elles permettent aussi aux producteurs de mieux répartir les équipes d'enquêteurs, de prévoir les domaines les plus exposés à la fraude et au vol, d'anticiper les risques de récurrence et de satisfaire davantage les clients en diminuant les coûts entraînés par le vol d'énergie.

## Protection des frontières nationales

Se protéger des menaces commence souvent aux frontières, dans les aéroports et dans les ports. Les solutions IBM Business Analytics aident les organismes à identifier les conteneurs susceptibles de transporter des matériaux indésirables ou dangereux, à déterminer les passagers d'une compagnie aérienne devant être soumis à un contrôle plus poussé, ou à prévoir le degré de risque des véhicules au passage des frontières. L'analyse prédictive permet aux organismes d'optimiser les missions des personnels d'inspection, d'augmenter les taux de détection et d'assurer une meilleure protection du pays et des citoyens.

### Analyse des passages aux frontières du territoire national

**Un grand pays comptant environ 300 points de passage de ses frontières utilise des caméras pour enregistrer la plaque d'immatriculation de tous les véhicules tentant de pénétrer sur son territoire. Une fois la plaque déchiffrée, des consignes s'affichent sur les écrans du poste frontière, indiquant aux contrôleurs de laisser passer le véhicule ou de le diriger vers le deuxième poste de contrôle. Si un véhicule doit subir une deuxième inspection, des informations sont envoyées au terminal mobile de l'inspecteur chargé de l'affaire, indiquant la probabilité de chaque type de risque (drogue, armes, contrebande, immigration illégale, etc.) et donnant des conseils sur ce qu'il doit rechercher. Les véhicules sélectionnés, les évaluations des risques et les résultats des contrôles sont ensuite enregistrés pour permettre d'établir un reporting continu sur les niveaux d'inspection par type de risque, les taux de réussite, les taux de faux positifs et le volume et la valeur des saisies. Cette stratégie permet de tirer le meilleur parti du personnel d'inspection, d'accroître les taux de détection, de mieux protéger le pays et ses citoyens et d'améliorer l'expérience des voyageurs à faible risque en accélérant leur passage à la frontière.**

## Meilleure protection des communautés

Les services de police et les autres organismes de sécurité publique peuvent utiliser l'analyse métier afin de combiner des données issues de sources disparates et favoriser une meilleure utilisation des personnes et des informations disponibles pour surveiller, mesurer et prévoir la criminalité et ses tendances. L'analyse métier génère des connaissances qui permettent aux officiers de police de suivre les activités criminelles, de prévoir la probabilité des incidents et de déployer efficacement des ressources, avec à la clé une baisse de la criminalité, une sécurité renforcée et une plus grande satisfaction des citoyens. Par exemple, les organismes de sécurité publique utilisent désormais ces solutions pour identifier l'origine des actes criminels, effectuer des enquêtes sur les cambriolages, gérer les délinquants récidivistes et garantir davantage de sécurité aux officiers de police.

Le service de police de Memphis a déployé la technologie IBM Business Analytics et obtenu des indications en temps réel extrêmement précieuses sur les activités criminelles et les tendances de la criminalité. Le service peut désormais modifier sa tactique, redéployer ses patrouilles selon les besoins pour éviter les incidents, et augmenter les interpellations en flagrant délit. Le programme a réduit les crimes graves de 30 %, fait diminuer de 15% les crimes avec violence, et multiplié par quatre le nombre des arrestations. Le tout s'accompagne d'un retour sur investissements de 863%, d'après une évaluation réalisée par le cabinet d'analystes indépendants Nucleus Research.[9]

La même technologie peut également servir au secteur de l'éducation pour sécuriser les établissements scolaires et les campus universitaires. Les solutions IBM Business Analytics permettent ainsi de créer des scénarios de simulation visant à déterminer les contraintes, les règles et les stratégies d'intervention les plus efficaces pour optimiser la sécurité des étudiants et du personnel des établissements scolaires. Avec les indications fournies par l'analyse, les services de sécurité des établissements peuvent anticiper de façon optimale l'affectation des ressources et tenter de réduire la criminalité. Les informations de prévision de la criminalité peuvent être envoyées au moyen d'alertes par email, de tableaux de bord interactifs et de scorecards. Ce renseignement homogénéisé peut ensuite être exploité par les officiers, les superviseurs, les administrateurs, les chercheurs et les enseignants du service de criminologie, ainsi que dans d'autres domaines de l'écosystème de l'établissement.

Comme vous pouvez le constater, les solutions d'analyse métier permettent aux entreprises de tous les secteurs d'analyser de façon fiable et efficace les variables en rapport avec les menaces internes et externes. A l'aide d'un ensemble complet et flexible de techniques comprenant la notation des risques et la détection des anomalies, vous pouvez détecter les circonstances suspectes et réagir rapidement pour intercepter la fraude à sa source, ou en atténuer les conséquences. Les enquêteurs peuvent en outre se concentrer sur les transactions ou les événements ayant le plus de risque d'être frauduleux, afin d'augmenter les taux de réussite et de réduire les coûts. Facilement mis à jour, les modèles prédictifs permettent aux entreprises de détecter les situations ou les comportements inhabituels même lorsque les tactiques des fraudeurs ou les conditions changent.

## Gestion du risque financier

Les solutions IBM Business Analytics complètent le portefeuille reconnu de produits de gestion du risque d'IBM. Elles aident les cadres à prendre des décisions tenant compte des risques et à se mettre en conformité avec les exigences réglementaires, via des programmes et des méthodologies plus intelligents. La vaste gamme des domaines concernés sont les solutions du risque liquidité, le risque opérationnel, la modélisation actuarielle, la gouvernance, la gestion des règles et de conformité. Combinées aux solutions prédictives de lutte contre les menaces et les fraudes, elles permettent de bâtir une stratégie complète qui rationalise les processus de gestion du risque et garantit un retour sur investissements accru, sur un marché en rapide évolution.

## Identifiez la marche à suivre optimale

L'analyse métier est une technologie qui est en train de devenir très vite prédominante dans les entreprises de tous les types. Même si son utilisation et son adoption varient, avec une portée qui peut concerner toute l'entreprise ou tout un service, ceux qui optent pour une approche cohérente et contrôlée de la gestion des risques constatent un retour sur investissements et des avantages importants.

Certaines entreprises sont déjà plus avancées dans ce domaine mais il existe en général deux types d'approches. Fournir des connaissances aux principaux décisionnaires est la priorité majeure de nombreuses entreprises. Dans ce cas, les techniques d'analyse avancées permettent de brosser un tableau clair des événements et de leurs causes. Une génération de rapports réglementaires et un processus décisionnel fondés sur les principaux indicateurs de menaces sont des exemples de ce type d'approche. D'autres entreprises cherchent à aller au-delà du stade des connaissances pour identifier la meilleure mesure à prendre dans un processus indispensable à la mission. Quelques exemples : choisir l'affectation d'un officier de police un jour précis ; décider si un véhicule doit être fouillé lors de son passage à la frontière; évaluer la nature frauduleuse d'une demande de remboursement de sinistre et décider s'il y a lieu de faire une enquête.

Notre expérience montre que les entreprises gagnent progressivement en maturité au niveau de l'analyse. Certaines ont déjà mis en place des technologies de reporting ou d'analyse, mais sont conscientes qu'elles n'apportent pas de réponse parfaite aux défis métier critiques et ne permettent pas à l'entreprise de maîtriser totalement ses décisions. Cette prise de conscience incite l'entreprise à évoluer vers une plus grande maturité analytique en optant pour l'analyse métier, qui améliore son processus décisionnel. Les entreprises qui franchissent ce pas peuvent se différencier en améliorant les processus et en gérant proactivement leur connaissance des menaces et leur réaction à ces dernières. Nous pouvons décrire ces entreprises comme « expertes » : elles utilisent l'analyse métier d'une façon sophistiquée et innovante afin de se protéger des nuisances potentielles et exploitent au mieux les données au cours du processus décisionnel.

*« Dans un délai très court, nous pouvons diriger les officiers vers un secteur particulier, un jour précis, en opérant jusqu'au niveau de la rotation des équipes. C'est un peu comme une partie d'échecs. La solution IBM nous permet d'effectuer des arrestations qui auraient été impossibles auparavant. »*

– Larry Godwin, ex-directeur des services de police, Memphis PD

Les entreprises les plus avancées mettent en œuvre des décisions basées sur l'information pour gérer les menaces en temps réel. Quelle est la meilleure marche à suivre, selon les informations dont je dispose ? Comment dois-je allouer mes ressources ? Comment puis-je garantir que les menaces sont identifiées au point même d'interaction, et non une fois après s'être produites ? Quel est le risque de défaut de paiement de cet emprunteur si nous lui accordons ce prêt ?

Les entreprises ayant atteint ce niveau utilisent leurs connaissances des événements antérieurs pour prévoir les événements futurs, et les mettent en application pour créer des stratégies qui leur permettent de réagir comme il se doit au point d'impact.

- Infinity Property & Casualty Corporation (Birmingham, Alabama, Etats-Unis) prend ses décisions métier de façon plus précise et cohérente, et plus rapidement grâce à l'analyse métier. Depuis la mise en œuvre des solutions IBM Business Analytics, Infinity a doublé la précision de l'identification des fraudes aux demandes de remboursement, augmenté ses résultats de $1 million en éliminant environ $70000 par mois d'honoraires versés à des tiers, et réalisé un retour sur investissement de 403 % grâce à une réduction des paiements de demandes de remboursement et une amélioration de la subrogation.[10]
- MedeAnalytics, qui aide les hôpitaux à optimiser le processus de collecte des paiements, a intégré IBM Business Analytics à sa solution de façon à ce que ses clients puissent hiérarchiser les meilleurs payeurs parmi les patients réglant directement (sans passer par une assurance). Le but recherché est de focaliser les opérations de collecte sur ce segment très rentable de la population.[11]

L'adoption de l'analyse métier pour détecter les menaces et les fraudes peut aussi permettre à votre entreprise de réussir avec d'autres stratégies critiques souvent apparentées, comme la connaissance approfondie du client et l'excellence opérationnelle. Par exemple, quand Infinity Property & Casualty a déployé une analyse métier pour identifier les fraudes potentielles au remboursement plus rapidement et avec plus de précision, elle a aussi constaté une augmentation importante de la satisfaction des clients. Le traitement des demandes dans son ensemble étant plus efficace, les demandes légitimes soumises par des souscripteurs à faible risque pouvaient être traitées et réglées rapidement, les demandes suspectes étant marquées en vue d'un traitement spécial, puis étudiées le temps nécessaire pour déterminer si elles étaient ou non frauduleuses.

Même si vous vous situez à un niveau différent d'adoption de la solution, il est tout à fait envisageable d'accéder au statut d'« entreprise experte » si vous avez une idée précise de la façon dont vous utilisez les données pour contrôler les menaces, et de la marche à suivre pour atteindre le niveau idéal.

*« Avec l'analyse métier, nous avons pu supprimer une source de perte régulière d'argent. »*

–Bill Dibble, SVP du service des remboursements, Infinity Property & Casualty

## Cinq étapes vers une stratégie proactive de gestion des menaces

Pour pouvoir gérer les menaces dans notre univers moderne, intelligent, instrumenté et interconnecté, les entreprises doivent réfléchir à une application de l'analyse métier au point d'interaction, là où les stratégies en temps réel, déterminées par les tendances, fusionnent avec le contexte situationnel. Ce niveau de transformation nécessite une série de changements dans la façon dont une entreprise gère les informations et dont elle les applique pour atteindre ses objectifs.

IBM peut collaborer avec vous pour créer une feuille de route comprenant une série d'étapes incrémentielles qui vous permettent d'atteindre vos objectifs de gestion des menaces. Avant de prendre des décisions concernant des technologies ou des solutions spécifiques, vous devez pouvoir répondre à certaines questions critiques sur la stratégie actuelle et l'utilisation des données de votre entreprise :

1. Déterminez la stratégie actuelle de gestion des menaces de votre entreprise : identifiez votre approche des menaces, à la fois en tant qu'entreprise et dans les principaux domaines opérationnels, tels que la finance ou le service clientèle, et les types d'actions que vous mettez en œuvre pour contrôler les menaces. Vous décririez-vous comme étant réactif, proactif ou un peu des deux, en fonction de la situation ou de l'opportunité ? Quel stade souhaitez-vous atteindre dans votre utilisation de l'analyse métier ? Comment utilisez-vous l'analyse pour définir les paramètres de vos politiques ? Ce processus est-il dynamique, vous permettant de modifier les politiques au fur et à mesure de l'évolution des conditions ?

2. Examinez la façon dont vous utilisez actuellement l'analyse métier. Où l'utilisez-vous et comment ? Quels types de résultats avez-vous obtenus ? Avez-vous une idée claire des menaces et des opportunités liées à vos opérations et prenez-vous des mesures préventives pour gérer efficacement les risques ? Comment surveillez-vous proactivement l'activité actuelle ?

3. Intégrez la gestion des menaces aux opérations quotidiennes et assurez-vous que toutes les parties prenantes ont la volonté de soutenir le projet. Etes-vous capable de répondre aux obligations en matière de réglementation ? Pouvez-vous exploiter davantage les données afin de les transformer en ressources, et ne plus les limiter à de simples livrables ? Peuvent-elles devenir un facteur qui permettra à l'entreprise d'aller de l'avant et de réduire ses coûts ?

4. Evaluez votre entreprise et ses données externes. Quelles données incluez-vous dans votre analyse des menaces et quelles autres données devez-vous inclure ? Quels sont les types de données disponibles ? Les différents services ont-ils un fonctionnement compartimenté en silos ? Mettez-vous à profit l'énorme gisement d'informations que représentent les données non structurées (forums sociaux, blogs) ou les sources internes (emails, notes prises par les centres d'appels) ?

5. Identifiez les opportunités d'automatisation et de contrôle. Avez-vous une attitude proactive pour déterminer les types de menaces que vous pouvez autoriser, par opposition à celles que vous voulez éviter ? Contrôlez-vous le résultat lorsque des menaces apparaissent ou appliquez-vous plutôt une procédure corrective ? Disposez-vous de processus ou des décisions pouvant aisément être automatisés ? Les décisions peuvent-elles être prises en temps réel ?

Vos réponses à ces questions vont vous aider à identifier les domaines dans lesquels vous pouvez commencer à obtenir des résultats réels et bénéfiques pour l'entreprise.

*« Nous souhaitons optimiser la productivité des organismes collecteurs en leur fournissant une liste de patients qui sont plus susceptibles de rembourser leurs frais hospitaliers et de mettre tout en bas de la liste les mauvais payeurs potentiels. »*

– David Mould, Ph.D., spécialiste en analyse prédictive, MedeAnalytics

## Les solutions IBM Business Analytics : un outil d'accès aux connaissances

Les solutions IBM d'analyse métier peuvent aider les entreprises à bénéficier de toutes les fonctionnalités décrites ci-dessus. Les solutions IBM sont faciles à utiliser, ne nécessitent pas de compétences techniques avancées et s'intègrent aisément aux systèmes et technologies existants. Les entreprises leader ont choisi les solutions IBM Business Analytics pour détecter et prévenir les menaces et les fraudes, et informer correctement les employés en leur fournissant des rapports de renseignements à jour.

Forte de plus de 40 années d'expertise dans l'analyse, IBM, avec ses solutions IBM SPSS Predictive Analytics, aide les entreprises à effectuer des prévisions en toute confiance et leur permet de prendre des décisions plus intelligentes et d'améliorer les résultats. Avec tout l'éventail de fonctionnalités d'analyse statistique, d'exploration de données et de texte, de modélisation prédictive, d'analyse des média sociaux et d'optimisation des décisions, les solutions SPSS d'analyse prédictive peuvent aider votre organisme à anticiper les changements et à obtenir des connaissances exploitables à partir de vos données.

Les logiciels IBM Cognos de business intelligence et de gestion de la performance proposent aux entreprises les tableaux de bord intégrés, les scorecards, la génération de rapports, et les fonctions d'analyse, de planification et de budgétisation dont elles ont besoin pour acquérir des connaissances concrètes et agir en conséquence . Les utilisateurs professionnels peuvent créer des rapports détaillés et personnalisés sans devoir solliciter l'aide du service informatique. Ils peuvent explorer en détail les données afin de se procurer des indications plus significatives et atténuer l'impact négatif des risques auxquels ils sont confrontés.

Solutions entièrement intégrées, les technologies d'analyse prédictive IBM SPSS et de business intelligence d'IBM Cognos offrent aux entreprises toute la puissance des fonctionnalités et des avantages de l'analyse métier. Elles les aident à obtenir des informations métier exploitables et des performances supérieures, qui vont au final leur permettre de mener à bien leurs stratégies et de réaliser leurs objectifs.

## Conclusion

Notre monde devient plus instrumenté, plus interconnecté et plus intelligent. Ces facteurs créent de nombreuses opportunités pour les sociétés du secteur public et privé, mais posent aussi des défis, notamment une exposition accrue aux menaces.

Les entreprises les plus innovantes se tournent vers l'analyse métier, qui constitue une approche proactive de la gestion des menaces et leur offre les possibilités suivantes :

- Surveiller leurs environnements en incorporant une grande diversité de données dans de nombreuses sources.
- Détecter les comportements suspects pour identifier les menaces, les vols d'information, les actes criminels et les fraudes.
- Contrôler les résultats afin de déterminer la réaction la plus appropriée pour réduire la vulnérabilité ou les pertes et optimiser l'impact de toute action.

Avec l'analyse prédictive, votre entreprise peut trouver un moyen de mieux comprendre ses opérations et utiliser cette connaissance pour développer des approches proactives aux multiples défis auxquels elle est confrontée chaque jour.

## À propos d'IBM Business Analytics

Les logiciels IBM Business Analytics fournissent des informations orientées données pour aider les organisations à travailler de manière plus intelligente et à surpasser leurs concurrents. Le portefeuille de produits, très complet, inclut des solutions de Business Intelligence, d'analyse prédictive, d'aide à la décision, de pilotage de la performance et de gestion des risques. Les solutions IBM Business Analytics aident les entreprises à identifier et à visualiser les tendances et les schémas présents dans certains secteurs (comme l'analyse client) qui peuvent avoir un effet déterminant sur leurs performances. Elles leur permettent de comparer des scénarios, d'anticiper des menaces et des opportunités potentielles, de mieux planifier, budgétiser et prévoir leurs ressources, d'équilibrer le rapport entre les risques potentiels et les retours sur investissement prévus, et de respecter les réglementations. En élargissant l'utilisation de l'analyse, les organisations peuvent adapter leurs décisions tactiques et stratégiques afin d'atteindre leurs objectifs.

Pour plus d'informations, visitez le site
**ibm.com**/business-analytics/fr

### Demander à être appelé

Pour être contacté ou pour poser une question, accédez au site
**ibm.com**/business-analytics/fr

Un représentant IBM vous répondra sous deux jours ouvrés.

**Compagnie IBM France**
17 Avenue de l'Europe
92 275 Bois-Colombes Cedex

La page d'accueil d'IBM est accessible à l'adresse suivante :
**ibm.com**



[1] Association of Certified Fraud Examiners, « 2012 Global Fraud Study » (http://www.acfe.com/rttn-highlights.aspx)

[2] Ibid.

[3] http://www.bcbsm.com/content/microsites/health-care-fraud/en/fraud-statistics.html

[4] Insurance Fraud, Federal Bureau of Investigation. (http://www.fbi.gov/stats-services/publications/insurance-fraud)

[5] Credit Card Fraud Statistics, (http://www.statisticbrain.com/credit-card-fraud-statistics/)

[6] 2012 IBM Global Reputational Risk and IT Study, (**ibm.com**/services/us/gbs/bus/html/risk_study.html).

[7] IDC: The business value of predictive analytics, juin 2011, (http://forms.cognos.com/?elqPURLPage=4206&offid=wp_spssrc_business_value_of_predictive_analytics_ytw03183)

[8] Infographie : Les plus grands vols de données dans le secteur de la santé en 2012, Healthcare IT News. (http://www.healthcareitnews.com/news/infographic-biggest-healthcare-data-breaches-2012)

[9] « ROI Case Study: IBM SPSS – Memphis Police Department. » Nucleus Research. Juin 2010.

[10] « Infinity Property & Casualty: Driving the auto insurance industry forward. » IBM Corporation, 2011.

[11] « Helping hospitals capture more revenue: MedeAnalytics employs IBM SPSS Modeler to help prioritize providers' collection efforts. » IBM Corporation, 2010.



Pensez à recycler ce document

YTW03173-FRFR-02