Juin 2016

# Sécurité cognitive

## Transformez vos défenses avec une solution de sécurité qui comprend, raisonne et apprend


# Sommaire

03 Le nouvel impératif

03 Qu’est-ce que la sécurité cognitive ?

04 Passer de la conformité à une approche cognitive

06 L’avant-poste de la protection cognitive

07 Explorer plus loin et plus largement

07 Résoudre la question de la pénurie des compétences

08 Cas d’utilisation : la sécurité cognitive révélée

09 L’avenir : retourner le système économique de la cybercriminalité

09 Intégration et expertise d’un écosystème cognitif

10 Comment IBM peut vous aider ?

10 Les trois étapes à engager dès maintenant

# Le nouvel impératif

Depuis quasiment un siècle, nous programmons des ordinateurs pour mieux résoudre des problèmes complexes. Nous pouvons aujourd'hui prévoir la météo, séquencer des génomes et partager instantanément des données à l'échelle mondiale. Mais demander à un ordinateur d'agir comme le font les humains dans leur quotidien — reconnaître une image, lire un livre ou expliquer le sens d'un poème — est une tout autre affaire. Les systèmes traditionnels sont dépassés.

Et la sécurité aussi. Depuis des décennies, nous programmons les ordinateurs pour identifier des virus, des logiciels malveillants et des exploits. Même si nous adaptons ces logiciels en permanence pour gagner en précision, cela ne suffit plus. En effet, nos adversaires transforment constamment leurs attaques et adoptent des approches créatives pour percer les défenses. Ce dont les entreprises ont besoin, c'est de la capacité à détecter des changements subtils dans les activités et de les analyser en les rapprochant des informations contextuelles les plus larges pour repérer les menaces inédites et les éliminer.

**80 %**
des données mondiales
ont été
invisibles.

**Jusqu'ici.**

Ce qui nécessite une surveillance constante et une exploitation maximale des données pour identifier les attaques et les comportements anormaux avant tout dommage. Pour autant, plus de 2,5 milliards de trilliards d'octets ($10^{30}$) sont générés chaque jour, dont 80 % sous une forme non structurée. Les informations relatives à la sécurité sont produites en langage naturel – oral, écrit ou visuel –, compréhensible par les humains, mais pas par les systèmes de sécurité traditionnels. En réalité, des milliers de billets de blogs contenant des informations détaillées sur les menaces sont publiés tous les jours. Mais il est impossible pour un analyste spécialisé dans la sécurité d'assimiler leur contenu. De plus, la sécurité traditionnelle est dans l'incapacité d'analyser ces informations et de les appliquer aussi efficacement qu'un analyste.

Ce qui explique pourquoi les problèmes de sécurité les plus complexes nécessitent encore une intervention humaine pour prendre les bonnes décisions pour agir et identifier les fausses alertes. En fait, les professionnels de la sécurité les plus performants construisent chaque jour l'essentiel de leurs connaissances grâce à leur expérience, en dialoguant avec leurs collègues, en assistant à des conférences et en actualisant leurs compétences grâce à la recherche.

Au sein de l'équipe IBM® Security, nous « formons » une nouvelle génération de systèmes pour qu'ils comprennent, décodent et assimilent les informations relatives à des menaces en évolution constante. Nous commençons à intégrer une expertise et des réflexes de sécurité dans de nouvelles défenses capables d'analyser des rapports de recherche, du texte publié sur le web, des données relatives aux menaces, ainsi que d'autres données structurées et non structurées concernant la sécurité – exactement comme les professionnels de ce domaine le font quotidiennement – mais à une échelle sans précédent. Telle est la nature de la sécurité cognitive.

Résultat : les analystes vont pouvoir s'appuyer sur les systèmes cognitifs pour étoffer et même automatiser l'analyse d'une menace... ce qui va contribuer à leur connaissance des menaces les plus récentes et leur permettre de mieux employer leur temps précieux à des problèmes plus urgents.

# Qu'est-ce que la sécurité cognitive ?

Les systèmes cognitifs apprennent de manière automatique en s'appuyant sur le data mining, l'apprentissage automatique, le traitement du langage naturel et les interactions homme–machine pour imiter le fonctionnement du cerveau humain.

### La sécurité cognitive s'appuie sur deux fonctionnalités associées et aux capacités étendues :

- L'utilisation de systèmes cognitifs pour analyser les tendances de sécurité et distiller d'énormes volumes de données structurées et non structurées pour en extraire des informations, puis des connaissances exploitables pour assurer une sécurité en continu et améliorer les activités métier.
- L'utilisation de technologies, de techniques et de processus de sécurité automatisés et pilotés par les données assure le fonctionnement des systèmes cognitifs hautement performants en matière d'analyse de contexte et de précision.



# Passer de la conformité à l'approche cognitive

**Depuis l'avènement des premiers réseaux et celui des hackers par la suite, nous avons transformé la technologie de la sécurité pour stopper les attaques. À ce jour, nous distinguons deux périodes pour la cyber-sécurité : les contrôles périmétriques et la sécurité intelligente. Ces deux aspects constituent des briques de construction alors que s'ouvre une troisième période, celle de la sécurité cognitive.**

## Contrôles périmétriques : la protection par le confinement (avant 2005)

La sécurité s'est appuyée, à ses débuts, sur des protections statiques pour contenir ou limiter le flux des données, avec notamment les pare-feu, les logiciels antivirus et les passerelles web. L'évolution de la sécurité de l'information dans l'entreprise a été d'abord une démarche de conformité. L'objectif était de verrouiller et restreindre l'accès aux informations sensibles grâce à des mots de passe et à des stratégies de contrôle d'accès. Le succès tenait alors à la réussite d'un audit. Si les protections périmétriques sont encore valides, elles ne sont en revanche plus suffisantes par elles-mêmes dans l'environnement d'aujourd'hui.

## Sécurité intelligente : la protection qui vous aide à réfléchir (2005, et au-delà)

Par la suite, nous avons évolué vers des systèmes de surveillance sophistiqués, destinés à collecter et passer au peigne fin des volumes massifs de données pour repérer les vulnérabilités et hiérarchiser les attaques potentielles. Cette transition a abouti à donner la priorité aux informations en temps réel pour détecter les activités suspectes. Aujourd'hui, la sécurité intelligente s'appuie sur la collecte, la normalisation et l'analyse en temps réel de données structurées, générées par les utilisateurs, les applications et l'infrastructure.

Elle utilise l'analyse pour détecter les écarts par rapport aux formes régulières, mettre en évidence les changements dans le trafic réseau et identifier les niveaux d'activité situés au-delà de valeurs définies. Dans une infrastructure de sécurité intelligente, les analyses s'appliquent à des volumes massifs d'informations pour comprendre les données de l'entreprise en tenant compte de leur contexte et hiérarchiser les activités quotidiennes. En déterminant les écarts significatifs, cette démarche de sécurité peut non seulement détecter plus rapidement les atteintes, mais également réduire le nombre de faux positifs, ce qui évite des pertes de temps et réduit les besoins en ressources.

## Sécurité cognitive : la protection qui comprend, raisonne et apprend à grande échelle (2015 et au-delà)

Fondée sur une sécurité intelligente dotée d'outils d'analyse du Big Data, la sécurité cognitive se caractérise par une technologie capable de comprendre, de raisonner et d'apprendre. Les systèmes cognitifs accèdent aujourd'hui à un éventail de données de sécurité considérablement plus large, et peuvent traiter et interpréter 80 % des données disponibles, non structurées, notamment le texte écrit et le langage parlé.

Après assimilation d'un corpus de connaissances et la gestion par des experts sur différents sujets, un système de sécurité cognitive fait l'objet d'un apprentissage en y introduisant des paires question-réponse. Ce « savoir » automatisé est ensuite étoffé par les interactions de professionnels de la sécurité avec le système, ce qui permet de connaître la fiabilité des réponses du système. Cette différence est essentielle : un système cognitif comprend et traite de nouvelles informations à une vitesse bien supérieure à celle d'un être humain. Il est maintenant possible de former les défenses techniques pour analyser des milliers de rapports de recherche, de documents issus de conférences, de mémoires universitaires, d'articles d'actualité, de contributions à des blogs et d'alertes sectorielles —et ce, chaque jour.

Grâce à leur capacité permanente à observer des événements et des comportements — et à distinguer les bons des mauvais — les systèmes cognitifs bénéficient d'une puissance sans cesse croissante pour exploiter leurs protections intégrées afin de bloquer de nouvelles menaces. En renforçant l'efficacité des analystes spécialisés dans la sécurité et en accélérant la réponse aux menaces émergentes, la sécurité cognitive contribue à réduire les écarts de compétences en matière de sécurité, en apportant des niveaux inédits de confiance et de maîtrise du risque. Voir figure 1.

# Historique de la sécurité

## Contrôles périmétriques

**Avant 2005**

- Défenses statiques
- Protections par mot de passe
- Priorité à la conformité
- Succès = réussite d'un audit.

## Sécurité intelligente

**2005, et au-delà**

- Observation des activités en temps réel
- Priorité aux écarts par rapport à des formes connues
- Capacité à hiérarchiser les menaces potentielles
- Système réactif et fondé sur des règles.

## Sécurité cognitive

**2015, et au-delà**

- Raisonnement similaire à la réflexion humaine
- Capacité à analyser des données structurées et non structurées pour comprendre les comportements et les significations
- Apprentissage automatique fondé sur la connaissance des menaces en continu
- Démarche essentiellement proactive utilisant les relations et les recommandations.

*Figure 1*

**La sécurité cognitive s'appuie in fine sur un environnement fondé sur les éléments essentiels de la sécurité traditionnelle. La sécurité intelligente ne s'en écarte pas, car elle constitue une brique de construction fondamentale de la sécurité cognitive. Ce qu'apporte la technologie cognitive, c'est la mise en place d'une approche permettant d'aiguiller les informations et la détection des menaces et produire des informations exploitables, à une vitesse et à une échelle sans précédent.**



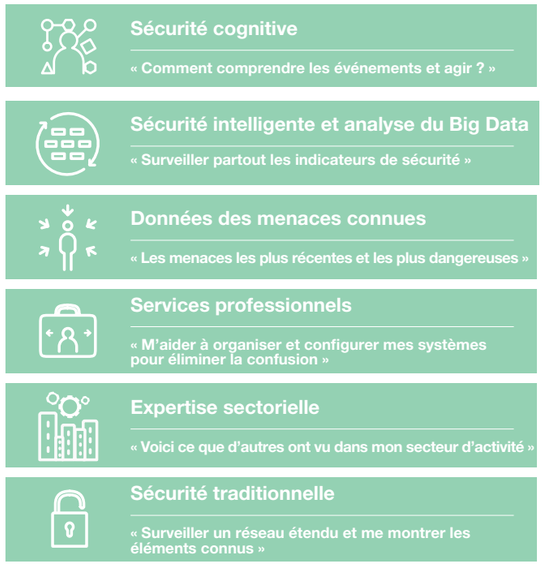


*Figure 2*

**La sécurité intelligente et les outils d'analyse du Big Data étant traditionnellement non structurés, l'aspect cognitif apporte un niveau supplémentaire important dans leur compréhension des événements et des actions à mettre en œuvre. Grâce à cet ensemble de strates de sécurité, vous disposez d'un niveau maximal de protection pour votre environnement de sécurité. Voir figure 2.**

# L'avant-poste de la protection cognitive

Les systèmes de sécurité programmables traditionnels répondent à des demandes, procèdent à des déterminations et analysent les données en fonction de paramètres prédéfinis. De leur côté, les systèmes cognitifs interprètent les données, enrichissent leurs bases de connaissances pratiquement à chaque interaction, pondèrent les probabilités en fonction d'un niveau de connaissance et vous aident à mettre en œuvre des actions en prenant en compte les variables pertinentes.

Ainsi, alors que la génération actuelle de systèmes est réactive, avec la capacité à détecter et à réagir à des anomalies ou à des attaques, la sécurité cognitive est par nature proactive. Tournés vers l'avenir et fonctionnant de manière continue en mode multitâches, les systèmes cognitifs traquent les vulnérabilités, révèlent des schémas, détectent des variances et passent au crible des milliards d'événements pour construire à partir d'une base de connaissances exploitable.

Les solutions cognitives produisent non seulement des réponses, mais formulent aussi des hypothèses, des raisonnements et des recommandations fondés sur des preuves. Il est aujourd'hui possible d'interpréter 80 % des données disponibles, non structurées, jusqu'ici inaccessibles pour les systèmes existants – et de les intégrer avec les données structurées issues d'innombrables sources et emplacements. Dans une économie mondiale où l'information est un gisement de valeur de plus en plus capital, les données constituent une matière première parmi les plus abondantes, riches et complexes au monde. Nous disposons donc maintenant des moyens pour accéder à des données structurées et non structurées et extraire en permanence des caractéristiques et des modèles permettant de disposer en temps réel des informations contextuelles nécessaires pour améliorer le processus décisionnel.

La sécurité cognitive fonctionne selon trois axes, à une vitesse extrême, en appliquant des modes de réflexion similaires à ceux de la pensée humaine :

1. **Comprendre** et mettre en lumière le sens des données non structurées et du texte en langage naturel. Il s'agit ici d'ingérer et de traiter les informations obtenues par la « lecture » de livres, de rapports, de blogs et de données sectorielles, la « vision » et l'analyse d'images, et l'« écoute » de contenus vocaux en langage naturel, replacés dans leur contexte.
2. **Raisonner** en s'appuyant sur la capacité à interpréter et organiser des informations, et apporter des explications sur leur sens, ainsi qu'une logique motivant les conclusions.
3. **Apprendre** en continu avec l'accumulation des données et la production de connaissances résultant des interactions.

# Explorer plus loin et plus largement

Une démarche exclusivement focalisée sur la détection des menaces et des logiciels malveillants, des valeurs aberrantes et des anomalies peut conduire à un nombre excessif de faux positifs. D'où l'avantage d'un domaine d'intervention multidimensionnel qui est précisément celui des systèmes cognitifs.

Dans le monde d'aujourd'hui, la capacité à distinguer le blanc du noir n'est plus le seul aspect de l'expertise nécessaire pour une infrastructure de sécurité intégrée. Il existe aussi des domaines « grisés » de plus en plus étendus où l'approche cognitive devient indispensable.

Renforcés par des niveaux inédits d'intuition, d'intelligence et de connaissance, les systèmes cognitifs sont conçus pour s'enrichir en permanence à l'aide des données et ainsi mieux distinguer les comportements acceptables des variations subtiles potentiellement représentatives de menaces émergentes. Résultat : des perspectives étendues et une focalisation proactive sur une vision élargie du contexte.

# Résoudre la question de la pénurie de compétences

**Si nos systèmes sont confrontés aux difficultés de rester à niveau face à l'environnement actuel de la sécurité, ces défis concernent également le personnel. Le nombre de postes non pourvus concernant la sécurité de l'information est estimé à 208 000 et devrait atteindre 1 500 000 d'ici 2020. C'est ici que la sécurité cognitive peut également intervenir.**

Ressource évolutive capable de contribuer aux interventions humaines, les systèmes cognitifs peuvent constituer des extensions extraordinaires pour des départements de sécurité fréquemment en sous-effectif. Cette nouvelle dimension est vitale, car se contenter de surveiller l'état de votre seul système n'est plus de mise. Vous devez aussi surveiller les menaces à l'échelle mondiale pour vous préparer à des attaques potentielles. À cet effet, les systèmes cognitifs sont capables d'accéder à des réseaux d'échange mondiaux qui analysent des centaines de milliers d'événements de sécurité chaque seconde pour des milliers de clients partout dans le monde.

La démarche cognitive facilite le travail des analystes de sécurité en assurant des communications essentiellement humaines, notamment des visualisations évoluées, des analyses interactives de vulnérabilité, des évaluations de risques, ainsi que des actions de résolution et des attributions possibles. De plus, les systèmes cognitifs seront capables de repérer les anomalies et les défaillances logiques, et de proposer des raisonnements fondés sur des preuves. Il sera ainsi possible pour les analystes de pondérer différents résultats et d'améliorer leur processus décisionnel.



# Cas d'utilisation :

## la sécurité cognitive révélée

1

### Étoffez les ressources de vos analystes de sécurité

Capables de comprendre d'immenses volumes de données structurées et non structurées, les systèmes cognitifs peuvent contribuer à développer considérablement le niveau de compétence d'un analyste débutant. Ils permettent d'automatiser l'assimilation des informations – notamment les rapports de recherche et les meilleures pratiques – et produisent des résultats en temps réel. Jusqu'ici, l'acquisition de ces connaissances exigeait des années d'expérience.

### Accélérez vos réponses grâce à une intelligence externe

Lorsqu'une attaque exploitera la prochaine vulnérabilité Heartbleed, les blogs feront état des techniques de protection que vous pourrez appliquer pour vous en protéger. Même si une signature n'est pas encore disponible, l'accès au langage naturel en ligne vous permet de répondre à la question. Les systèmes cognitifs permettent de parcourir ces informations pour découvrir rapidement comment se protéger contre l'exploitation de vulnérabilités inédites.

2

3

### Identifiez les menaces grâce à l'analytique avancée

Pour identifier les menaces potentielles, les systèmes cognitifs ont à leur disposition différentes méthodes d'analyse, notamment l'apprentissage automatique, le regroupement, la mise en évidence de graphes et la modélisation des relations entre entités. Ils peuvent accélérer la détection du comportement des utilisateurs à risque, l'exfiltration des données et la détection des logiciels malveillants avant tout dommage.

### Renforcez la sécurité des applications

Les systèmes cognitifs peuvent comprendre le contexte sémantique de vos analyses et de vos données, mais aussi explorer le code et ses structures. Ils ont la capacité à traiter plusieurs milliers d'indicateurs de vulnérabilité et à ramener les résultats à un ensemble réduit d'éléments exploitables – et à vous indiquer les emplacements de votre code où vous pourrez les résoudre.

4

5

### Améliorez le risque pour l'entreprise

Dans le futur, les systèmes cognitifs pourront certainement analyser des corpus d'interactions, établir la nature de ces interactions et leur exposition pour créer des profils de risques pour les organisations, les actions d'entreprise, la formation et la transformation des comportements. Ils pourront également traiter les contenus en langage naturel pour repérer des données sensibles au sein d'une organisation, et les masquer.

# L’avenir : retourner le système économique de la cybercriminalité

Les systèmes cognitifs peuvent analyser des caractéristiques dans d’énormes ensembles de logiciels malveillants et y détecter des points communs subtils. Pour quelle raisons cette détection est-elle essentielle ? Parce que si la diversité des logiciels malveillants est considérable, les groupes de cybercriminels font évoluer leurs codes et que la plupart des logiciels actifs aujourd’hui sont en fait liés à d’autres logiciels malveillants. Grâce aux systèmes cognitifs, nous pouvons analyser les milliers de caractéristiques d’un fichier exécutable suspect et les regrouper pour en extraire des modèles. De plus, alors qu’un être humain ne peut connaître ces caractéristiques, ni la manière ou les raisons de leur détection, le système peut identifier un modèle pour mieux découvrir et classer de nouvelles variantes de logiciels malveillants.

Alors que la communauté des adeptes de la sécurité cognitive s’étend et que la viabilité des nouvelles attaques diminue, le cybercrime va être confronté à une nouvelle réalité économique. En effet, les efforts nécessaires pour développer des logiciels malveillants capables de déjouer les détections vont devenir de plus en plus complexes et coûteux. Selon l’étude Cost of Data Breach Study 2015 du Ponemon Institute, le délai moyen nécessaire à une entreprise ou à une organisation pour détecter des menaces persistantes avancées est de 256 jours, et le coût moyen d’une attaque contre des données aux États-Unis est de 6,5 millions de dollars. La sécurité cognitive va apporter aux analystes de sécurité les capacités nécessaires pour identifier les signes avant-coureurs d’attaques potentielles et en accélérer significativement la détection. Ce qui amènera les cybercriminels à constater que les profits seront de plus en plus difficiles à réaliser.

L’informatique cognitive conduit à une véritable transformation non seulement par la maîtrise des données, mais surtout par la signification de ces données, les connaissances, les flux de processus et la progression des activités, et ce, de manière ultra-rapide et étendue. Pour les entreprises qui s’engagent dans l’approche cognitive, l’avantage concurrentiel sera large et significatif.

# Intégration et expertise d’un écosystème cognitif

L’intégration et l’expertise sont essentielles pour une bonne sécurité. Trop de pratiques de sécurité sont fondées sur un ensemble de produits spécifiques isolés et dépourvus de la visibilité et de l’intelligence exploitable nécessaires pour réagir rapidement.

L’intégration est incomplète tant que toutes vos capacités spécifiques ne peuvent pas communiquer entre elles dans un environnement informatique hybride et intervenir au-delà des limites de votre entreprise pour englober l’ensemble de votre écosystème. Ainsi, une bonne intégration vous apporte la visibilité dont vous avez besoin pour réagir rapidement aux incidents de sécurité dès qu’ils se produisent. L’intégration vous permet de faire davantage avec moins de ressources, ce qui constitue une approche fondamentale pour combler les écarts de compétence en matière de sécurité.

De nouvelles menaces sont mises en évidence tous les jours, d’où l’aspect fondamental de l’expertise en matière de sécurité et de la connaissance des menaces. Dans ce contexte, si vous ne disposez pas d’une expertise de très haut niveau intégrée dans un ensemble de solutions et de connaissances, vous serez probablement rapidement distancé. À cet effet, IBM X-Force Exchange répertorie les informations relatives à plus de 88 000 vulnérabilités, plus de 25 milliards de pages web et les données de 100 millions de terminaux — ce qui vous donne accès à une expertise mondiale, disponible en temps réel et immédiatement exploitable.



# Comment IBM peut vous aider ?

La démarche cognitive n’en est qu’à ses débuts, mais IBM dispose de la puissance intellectuelle et financière indispensable pour apporter cette révolution dans la sécurité. Plus de 7 500 spécialistes de la sécurité d’IBM travaillent chaque jour dans 36 centres de sécurités mondiaux, chargés de surveiller 133 pays, et analysent 35 milliards d’événements quotidiennement. IBM investit depuis plusieurs décennies dans les technologies cognitives et a réalisé des progrès considérables au cours des cinq dernières années — notamment la capacité à traiter le langage naturel, les contenus vocaux et les images, mais aussi à transformer des données non structurées à l’aide d’outils comme les bases « knowledge graph », qui facilitent l’application de requêtes. IBM va poursuivre son engagement dans les technologies cognitives pour enrichir de manière durable les applications de sécurité et produire des informations pour les analystes.

IBM Security apporte aujourd’hui des capacités de sécurité intégrées dans des solutions. L’apprentissage automatique, par exemple, contribue à améliorer la fiabilité de la détection des vulnérabilités et à les hiérarchiser pour vous permettre d’y répondre plus rapidement. Par ailleurs, l’apprentissage des comportements permet d’anticiper et d’identifier des anomalies caractéristiques des menaces qui touchent les réseaux.

Les offres IBM Security permettent une protection de bout en bout et apportent une approche de système immunitaire englobant des analyses détaillées, l’identité et les accès, la fraude évoluée, les données, les applications, les réseaux, les terminaux, le Cloud, les appareils mobiles et la recherche. Chacune de ces plateformes contribue aux capacités cognitives d’IBM. Si vous êtes intéressé par les avantages de la sécurité cognitive, envisagez d’adopter des plateformes IBM qui bénéficient des innovations et des fonctions intégrées issues des technologies cognitives.

# Les trois étapes à engager dès maintenant

1. Découvrez comment exploiter les capacités cognitives pour anticiper les menaces.
2. Développez un plan d’action pour gagner en maturité concernant la sécurité et vous préparer à adopter la sécurité cognitive.
3. Facilitez l’intégration dans votre infrastructure de sécurité.

# Pour en savoir plus

Contactez votre interlocuteur commercial ou votre partenaire commercial IBM, ou visitez le site : ibm.biz/cognitivesec

# À propos de l'offre IBM Security

IBM Security propose l'une des gammes les plus évoluées et les mieux intégrées de produits et de services de sécurité pour l'entreprise. Adossées aux compétences de l'équipe de recherche et de développement IBM X-Force, reconnue dans le monde entier, ces offres apportent la sécurité intelligente nécessaire aux entreprises pour protéger de manière globale leur personnel, leurs infrastructures, leurs données et leurs applications, avec des solutions permettant, notamment, la gestion des identités et des accès, la sécurité des bases de données, le développement des applications, la gestion du risque, la gestion des terminaux et la sécurité des réseaux. Ces offres permettent aux entreprises de gérer plus efficacement les risques et de mettre en œuvre des solutions de sécurité intégrées pour les mobiles, le Cloud, les médias sociaux et d'autres architectures d'entreprise. Doté de l'une des structures les plus larges au monde en matière de recherche, de développement et de production dans le domaine de la sécurité, IBM surveille 35 milliards d'événements de sécurité par jour, dans 133 pays, et détient plus de 3 700 brevets en matière de sécurité.

De plus, IBM Global Financing peut vous permettre d'acquérir la solution dont vous avez besoin de la manière la plus appropriée à votre stratégie financière. Les clients qualifiés pour un crédit bénéficieront d'une solution de financement adaptée à leurs objectifs, à leur gestion de trésorerie et au coût total de possession. Financez vos investissements IT critiques et poussez votre organisation plus loin avec IBM Global Financing. Pour en savoir plus, visitez ibm.com/financing/fr

IBM France
17 Avenue de l'Europe
92275 Bois Colombes Cedex



SEW03134-FRFR-00