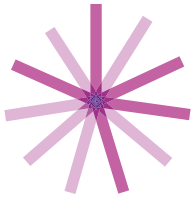
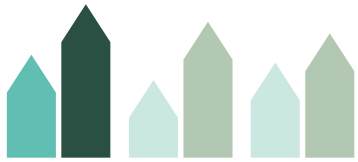
L'IMPÉRATIF DE SÉCURITÉ : FAVORISER LA CROISSANCE DE L'ENTREPRISE DANS L'ÉCONOMIE DES APPLICATIONS >>

Sponsorisé par ca technologies

COLEMAN PARKES RESEARCH

Sommaire





UTILISATION DE CE PDF INTERACTIF

Les fonctions interactives varient sur les tablettes et smartphones en fonction du lecteur de PDF installé. Certains éléments peuvent donc ne pas fonctionner lorsque vous affichez ce PDF en mode d'aperçu de la messagerie. Il est recommandé d'utiliser Adobe Acrobat Reader.

ACCUEIL (première page) | **SOMMAIRE** | **PAGE PRÉCÉDENTE** | **PAGE SUIVANTE**

Résumé

L'économie des applications a totalement remanié le paysage de la sécurité IT. La démarcation entre l'intérieur et l'extérieur de l'entreprise s'est estompée. Le périmètre du réseau d'entreprise a non seulement bougé, mais il s'est aussi fragmenté. Votre nouvelle frontière de sécurité réside désormais là où chaque utilisateur décide d'accéder à votre réseau.

Malheureusement, cela n'est pas le seul problème. Les clients, les employés et les partenaires attendent aujourd'hui un accès permanent, facile et transparent, quels que soient la plate-forme et le périphérique qu'ils utilisent.

Les stratégies de sécurité IT traditionnelles ne peuvent plus fonctionner dans un environnement aussi complexe. Les organisations doivent être à même d'authentifier des identités très distribuées provenant de multiples sources, tout en assurant une expérience utilisateur fluide. Il est nécessaire pour ce faire de trouver un savant équilibre entre une protection solide et la satisfaction de l'utilisateur, ce qui exige une approche nouvelle de la sécurité, centrée sur l'identité. Cette approche doit intégrer des outils d'analyse du comportement et du contexte et des méthodes plus prédictives, afin d'offrir une expérience client agréable tout en protégeant les identités et les données.

Enfin, une sécurité centrée sur l'identité vous permet d'établir des relations numériques de confiance avec vos clients, qui constituent le meilleur atout de votre entreprise dans l'économie des applications.

Face à ce constat, CA Technologies a demandé au cabinet Coleman Parkes Research de réaliser une enquête auprès de 1 770 dirigeants métier et IT, y compris plus de 100 responsables de la sécurité (CSO) et responsables de la sécurité des informations (CISO). Nous leur avons demandé quelles étaient leurs pratiques en matière de sécurité IT et les éléments clés adoptés dans le cadre d'une approche de sécurité centrée sur l'identité.

Cette enquête nous a permis de déterminer l'approche différente adoptée par les utilisateurs avancés en matière de sécurité orientée identité et l'impact de cette approche sur leur organisation.

Les résultats penchent nettement en faveur d'un nouveau modèle de sécurité numérique, un modèle conforme aux exigences de l'économie des applications et à même d'apporter de vraies améliorations qui se traduisent aussi par des résultats financiers.

Une sécurité centrée sur l'identité vous permet d'établir des relations numériques de confiance avec vos clients, qui constituent le meilleur atout de votre entreprise dans l'économie des applications.

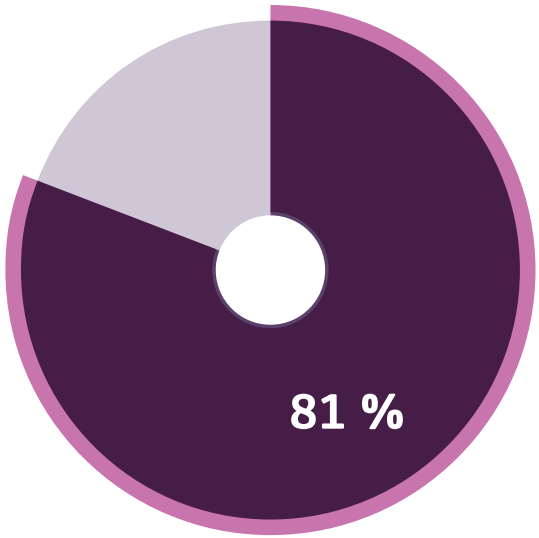
Notre analyse a permis d'établir les constats suivants :

- **81 %** des entreprises s'accordent sur le fait que la sécurité ne doit pas générer de frictions, pour ne pas accabler les utilisateurs d'exigences de sécurité onéreuses.
- **82 %** des entreprises affirment qu'une sécurité centrée sur l'identité est critique pour leur activité, pourtant **seules 25 %** d'entre elles peuvent être considérées comme utilisatrices avancées de ce type d'approche.
- Par rapport aux utilisateurs de base, les utilisateurs avancés d'une approche de sécurité centrée sur l'identité ont été deux fois plus nombreux à observer une réduction des violations de données, soit **41 % contre 21 %**.
- **91 %** des utilisateurs avancés d'une sécurité centrée sur l'identité ont observé une amélioration de la portée numérique, **87 %** une amélioration de l'expérience client et **87 %** une amélioration de la fidélisation des clients.
- Les utilisateurs avancés d'une approche de sécurité centrée sur l'identité observent également des résultats métier quantifiables :
  - **47 %** d'amélioration de la croissance de l'activité
  - **50 %** d'amélioration de la productivité des employés
  - **45 %** d'amélioration de la satisfaction client

« La sécurité est le principal moteur de notre cheminement vers le numérique. »

Directeur de la technologie, organisme gouvernemental américain

81 % des entreprises s'accordent sur le fait que la sécurité ne doit pas générer de frictions, pour ne pas accabler les utilisateurs d'exigences de sécurité onéreuses.



Introduction : une nouvelle frontière

La révolution numérique a totalement changé la donne en matière de sécurité IT, et cela continue aujourd'hui. Elle a créé un monde multicanal, multiplate-forme et multipériphérique. Un monde où vos clients, partenaires et employés sont toujours connectés, et attendent de vous que vous le soyez aussi.

Dans l'économie des applications actuelle, les clients exigent des téléchargements et un accès rapides, une expérience transparente ainsi qu'une protection robuste. Ils n'hésiteront pas à se détourner de vos services si vos mesures de sécurité les ralentissent ou si vous ne parvenez pas à protéger correctement leurs données.

Le périmètre réseau tel que nous le connaissions n'existe plus. Les utilisateurs accèdent à votre réseau à tout moment, où qu'ils soient et sur la plate-forme ou le périphérique de leur choix. L'identité de l'utilisateur, et non plus le pare-feu, est désormais la frontière qui protège les données.

Pour fonctionner, cette situation exige une relation de confiance bidirectionnelle entre l'utilisateur et l'entreprise.

Elle impose une approche de sécurité davantage centrée sur l'identité, qui place l'identité de l'utilisateur au cœur de son fonctionnement. La sécurité orientée identité s'appuie sur des outils d'analyse comportementale et contextuelle, et sur des approches de sécurité plus prédictives, afin de garantir que chaque utilisateur est bien celui qu'il prétend être. Cela permet aux utilisateurs d'accéder en toute sécurité aux données de votre société, quand et où ils le souhaitent, sur l'appareil de leur choix.

« La sécurité est un obstacle majeur pour satisfaire aux exigences de rapidité des clients. »

Directeur IT, association de collectivités locales, États-Unis

Les utilisateurs accèdent à votre réseau à tout moment, où qu'ils soient et sur la plate-forme ou le périphérique de leur choix.

Toutefois, une approche centrée sur l'identité est bien plus qu'une méthode efficace pour protéger les données. Correctement exécutée, elle peut également être un précieux moteur d'activité. Elle peut par exemple vous permettre de livrer plus rapidement de nouveaux services. Elle peut améliorer l'engagement et la fidélité des clients, qui reposent tous deux sur la confiance. Et dans un monde numérique, la sécurité est le premier facteur de confiance.

« Une sécurité centrée sur l'identité sera à l'avenir la principale approche sécuritaire adoptée par les sociétés de télécommunications. »

Directeur marketing, opérateur télécom européen

Dans le cadre de notre enquête sur l'évolution des entreprises à l'ère numérique, nous avons étudié les efforts de celles-ci pour adopter une approche de sécurité davantage centrée sur l'identité. Nous avons interrogé des cadres métier, sécurité et IT senior du monde entier sur les aspects suivants :

- Leur perception de la sécurité en tant que créateur d'opportunités métier
- Les principaux indicateurs clés de performance (KPI) qu'ils utilisent pour évaluer l'impact de la sécurité IT, et les résultats qu'ils ont observés
- Leurs progrès dans l'adoption d'une approche de sécurité centrée sur l'identité, indispensable dans l'économie des applications
- L'impact d'une utilisation plus avancée d'une sécurité orientée identité sur les performances métier

Le présent rapport offre une synthèse de nos observations. Il examine la façon dont les organisations peuvent faire évoluer leur sécurité IT de manière à accroître leurs performances, leur compétitivité et leur croissance dans l'économie des applications.

Une approche centrée sur l'identité est bien plus qu'une méthode efficace pour protéger les données. Correctement exécutée, elle peut également être un précieux moteur d'activité.

01. État des lieux de la sécurité dans l'économie des applications

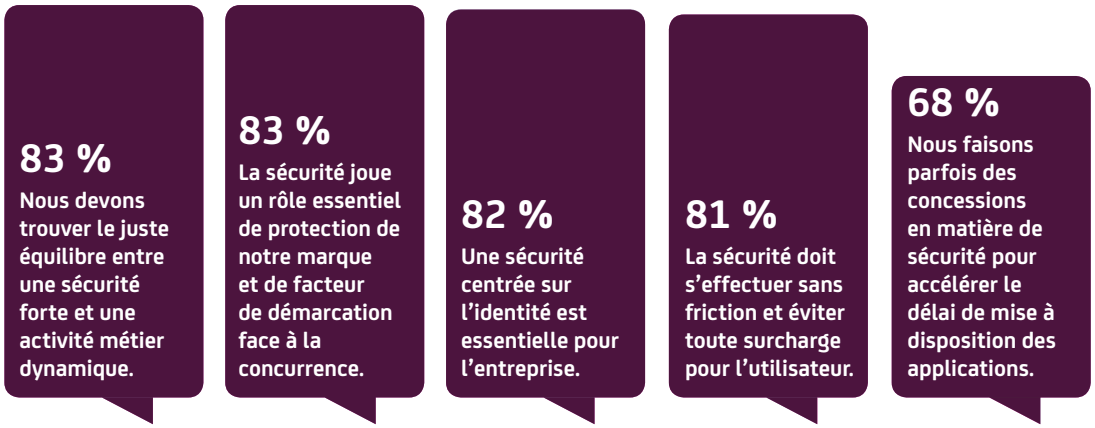
Les résultats de l'enquête suggèrent que les entreprises reconnaissent le rôle que la sécurité peut jouer dans l'environnement économique et commercial actuel. Elles restent focalisées sur les objectifs de sécurité traditionnels, tels que la protection contre les intrusions et les violations, et le respect des lois en vigueur. Dans le même temps, toutefois, les personnes interrogées lors de notre enquête considèrent aussi la sécurité comme une opportunité de développer leurs activités et d'être plus compétitives dans l'économie des applications.

Plus de 80 % des sondés affirment que la sécurité peut générer de nouvelles opportunités métier, offrir un avantage concurrentiel et octroyer aux employés et aux clients l'accès rapide, pratique et permanent auquel ils aspirent de nos jours (voir illustration 1).

Cela se reflète dans les indicateurs clés de performance (KPI) utilisés pour évaluer l'impact de la sécurité IT. Les métriques de performances métier externes, telles que la portée numérique, l'expérience client et la satisfaction client, sont autant (voire plus) utilisées que les mesures de sécurité traditionnelles, telles que le nombre de violations de sécurité et les échecs d'audit de conformité (voir illustration 2).

Plus de 80 % des sondés affirment que la sécurité peut générer de nouvelles opportunités métier, offrir un avantage concurrentiel et octroyer aux employés et aux clients l'accès rapide, pratique et permanent auquel ils aspirent de nos jours.

ILLUSTRATION 1 L'ÉCONOMIE DES APPLICATIONS IMPOSE À LA SÉCURITÉ UN NOUVEAU RÔLE EN TANT QUE MOTEUR D'ACTIVITÉ.



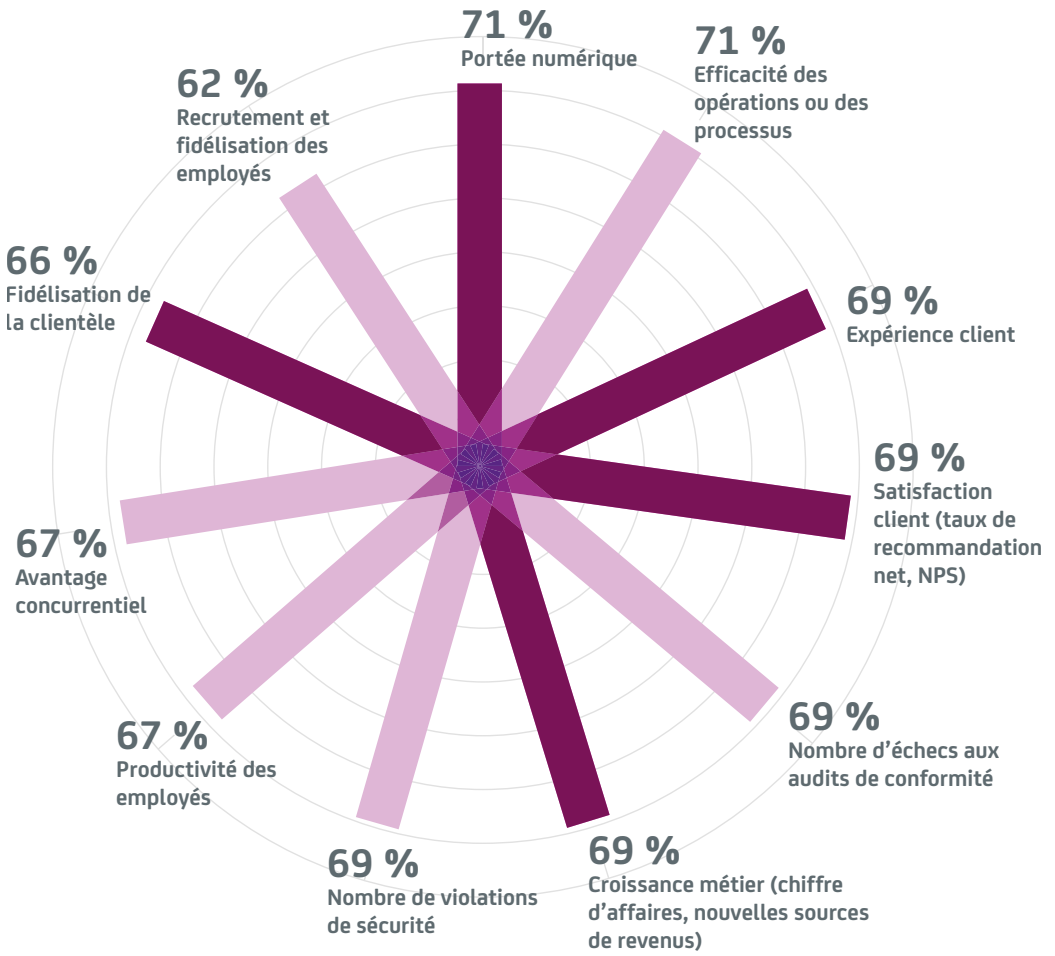
« Le juste équilibre est très difficile à trouver entre une sécurité robuste d'un côté, et l'interface avec les clients et les employés de l'autre »

Directeur IT, association de collectivités locales, États-Unis

Désormais, les entreprises considèrent clairement la sécurité IT comme un moyen de protéger les données, mais aussi comme un moteur d'activité essentiel. Cependant, certaines sautent des étapes essentielles sous la pression de l'économie des applications. Il est notamment inquiétant de constater que 68 % des entreprises interrogées admettent faire des concessions en matière de sécurité pour accélérer la mise à disposition de leurs applications sur le marché.

Ne pas faire passer la sécurité au premier plan dans l'économie des applications est un risque majeur. Gérer les identités et les accès sur plusieurs milliers d'applications, de services et de périphériques exige une approche bien plus sophistiquée que par le passé afin de protéger les identités et les données.

ILLUSTRATION 2 LES MÉTRIQUES MÉTIER EXTERNES FONT PARTIE DES PRINCIPAUX KPI UTILISÉS POUR MESURER L'IMPACT DE LA SÉCURITÉ IT.



02. Une nouvelle approche de la sécurité

Dans l'économie des applications, la difficulté consiste à vérifier des identités très distribuées provenant d'une grande variété de sources, telles que les applications, les systèmes, le Cloud et les plates-formes de réseaux sociaux.

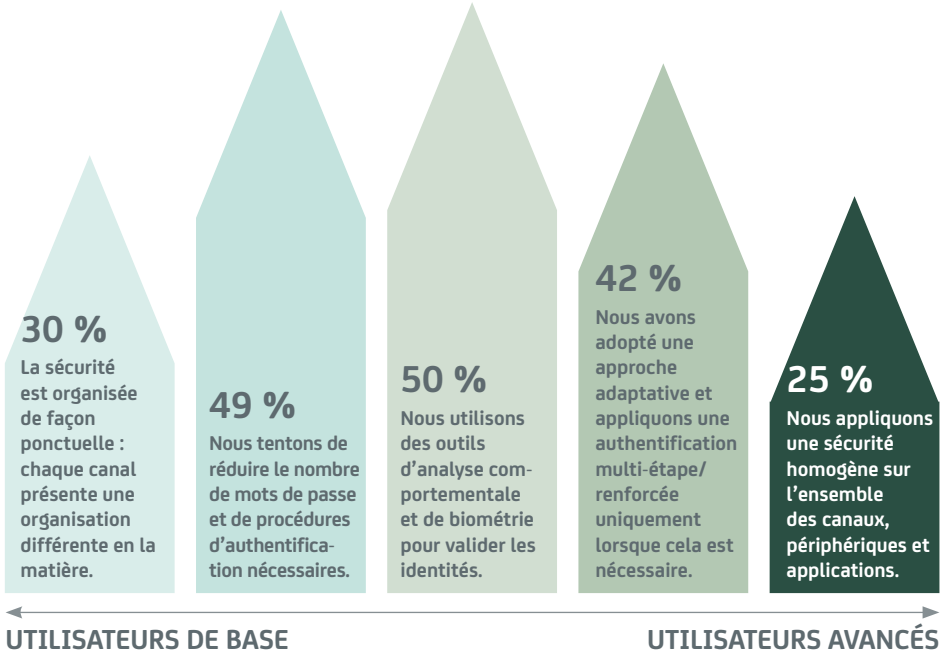
De plus, cette vérification doit passer inaperçue pour les utilisateurs. Les clients souhaitent une sécurité fiable et une expérience fluide. Des procédures d'inscription et d'authentification lourdes et hétérogènes auront vite fait de les décourager et entraveront les efforts visant à établir une relation numérique de confiance.

Une approche centrée sur l'identité vous aide à mettre en place des pratiques de sécurité qui n'affectent pas l'expérience globale de l'utilisateur. Elle vous oblige également à adopter des contrôles plus adaptatifs en matière de gestion des identités et des accès (Identity and Access Management, IAM) et une approche plus proactive et prédictive pour la prévention et la détection des violations de données.

Nous avons créé un modèle de maturité permettant d'évaluer où se situe une organisation en termes d'adoption et d'usage des trois éléments clés d'une sécurité centrée sur l'identité :

1. **Expérience client** (voir illustration 3).
   Des approches de sécurité homogènes sur les différents canaux, via des techniques adaptatives et des outils d'analyse comportementale, offrent une sécurité moins intrusive. Seul un quart des entreprises actuelles utilisent une sécurité homogène sur l'ensemble des canaux, périphériques et applications, dans le but d'offrir une expérience client de qualité. Une minorité d'entre elles (42 %) adopte une approche adaptative, et la moitié utilise des outils d'analyse comportementale.

ILLUSTRATION 3 DES APPROCHES DE SÉCURITÉ HOMOGÈNES ENTRE LES DIFFÉRENTS CANAUX GARANTISSENT UNE EXPÉRIENCE CLIENT DE QUALITÉ, MAIS RARES SONT LES ENTREPRISES À AVOIR ADOPTÉ CE PRINCIPE.



« La sécurité est devenue plus conviviale, sans perte d'efficacité. La clé consiste à pouvoir déterminer avec certitude si un utilisateur est un client, un employé ou un pirate, protéger les données des clients et des employés et s'assurer que les transactions ne sont pas entravées. »

Vice-président de la technologie et de la conformité, institution bancaire américaine

2. **Gestion des identités et des accès** (voir illustration 4). Une sécurité centrée sur l'identité exige aussi une approche plus adaptative en matière de contrôles pour la gestion des identités et des accès. Près de 70 % des entreprises se servent de contrôles IAM centralisés et automatisés, mais seul un dixième d'entre elles sont capables de les adapter en fonction des risques.

« La gestion des identités et des accès sera la principale problématique de sécurité à l'avenir. »

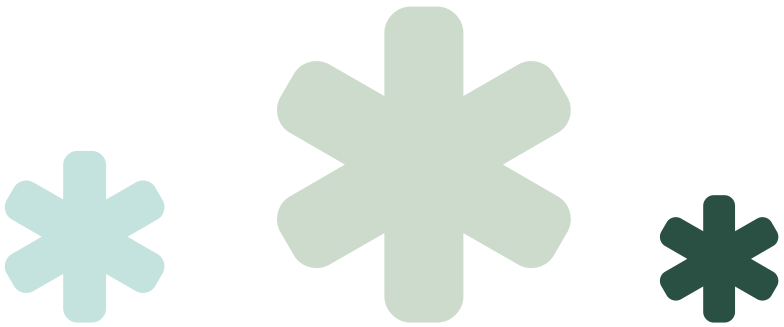
Directeur marketing, opérateur télécom européen

3. **Détection des violations de sécurité** (voir illustration 5). Des processus proactifs et prédictifs peuvent grandement améliorer la capacité d'une organisation à détecter et à prévenir les violations de données. Pourtant, seulement 37 % des entreprises utilisent des outils d'analyse pour détecter et prévenir proactivement les violations de données ; moins de la moitié de ces dernières (soit 16 %) sont à même de prévoir le risque de violations avant que celles-ci se produisent.

Après avoir posé aux participants des questions sur ces trois éléments clés de la sécurité centrée sur l'identité, nous avons attribué une note à leurs réponses. Sur la base des résultats obtenus, nous avons classé les organisations dans l'une des catégories suivantes en fonction de leur degré d'usage d'une sécurité centrée sur l'identité : utilisateurs avancés, utilisateurs de base ou utilisateurs limités.

Résultat, seulement 25 % des entreprises sont considérées comme des utilisateurs avancés. La majorité d'entre elles (64 %) sont des utilisateurs de base, et un peu plus du dixième (11 %) présentent une capacité de sécurité orientée identité limitée (voire nulle).

ILLUSTRATION 4 DES CONTRÔLES ADAPTATIFS EN MATIÈRE DE GESTION DES IDENTITÉS ET DES ACCÈS AMÉLIORENT LA SÉCURITÉ CENTRÉE SUR L'IDENTITÉ, MAIS RARES SONT LES ENTREPRISES À AVOIR ADOPTÉ CETTE APPROCHE.



20 %
Contrôles principalement manuels

69 %
Contrôles principalement centralisés et automatisés

11 %
Contrôles adaptatifs basés sur les risques.

UTILISATEURS DE BASE — **UTILISATEURS AVANCÉS**

ILLUSTRATION 5 DES OUTILS D'ANALYSE PROACTIFS ET PRÉDICTIFS AIDENT À DÉTECTER ET À PRÉVENIR LES VIOLATIONS DE DONNÉES, MAIS RARES SONT LES ENTREPRISES À AVOIR ADOPTÉ CETTE APPROCHE.

13 %
Vérification occasionnelle uniquement du reporting d'activité

34 %
Quelques analyses avec alertes et reporting intelligents

37 %
Méthode proactive : analyse approfondie avec réponse en temps réel aux événements et aux incidents

16 %
Méthode prédictive : capacité à anticiper les risques avant qu'une violation de sécurité se produise

UTILISATEURS DE BASE — **UTILISATEURS AVANCÉS**

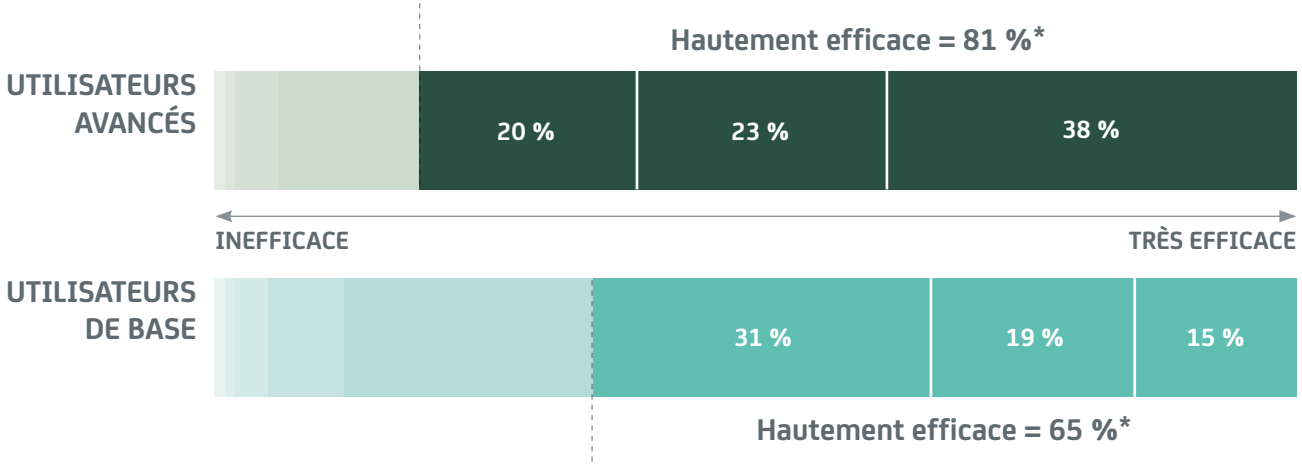
03. L'impact métier significatif de la sécurité centrée sur l'identité

À l'étape suivante de notre analyse, nous avons tenté de déterminer s'il existait une corrélation entre une utilisation mature de la sécurité centrée sur l'identité et des résultats métier. Pour ce faire, nous avons comparé les performances métier des utilisateurs avancés et des utilisateurs de base.

Le résultat de cette analyse est que les utilisateurs avancés sont beaucoup plus susceptibles de croire que leur approche de sécurité les distingue de la concurrence. Près de 81 % d'entre eux affirment que leur stratégie de sécurité est un facteur de différenciation, contre 65 % pour les utilisateurs de base (voir illustration 6).

Les utilisateurs avancés accordent également une plus grande priorité à l'ensemble des objectifs de sécurité sur lesquels nous les avons interrogés (voir page 8). Plus significatif encore, ils sont davantage susceptibles que les utilisateurs de base de mettre à profit leur approche de sécurité pour établir de nouvelles relations commerciales et mettre en place de nouvelles initiatives métier (55 % contre 34 %).

ILLUSTRATION 6 UNE UTILISATION AVANCÉE DE LA SÉCURITÉ CENTRÉE SUR L'IDENTITÉ AMÉLIORE LA DIFFÉRENCIATION CONCURRENTIELLE.

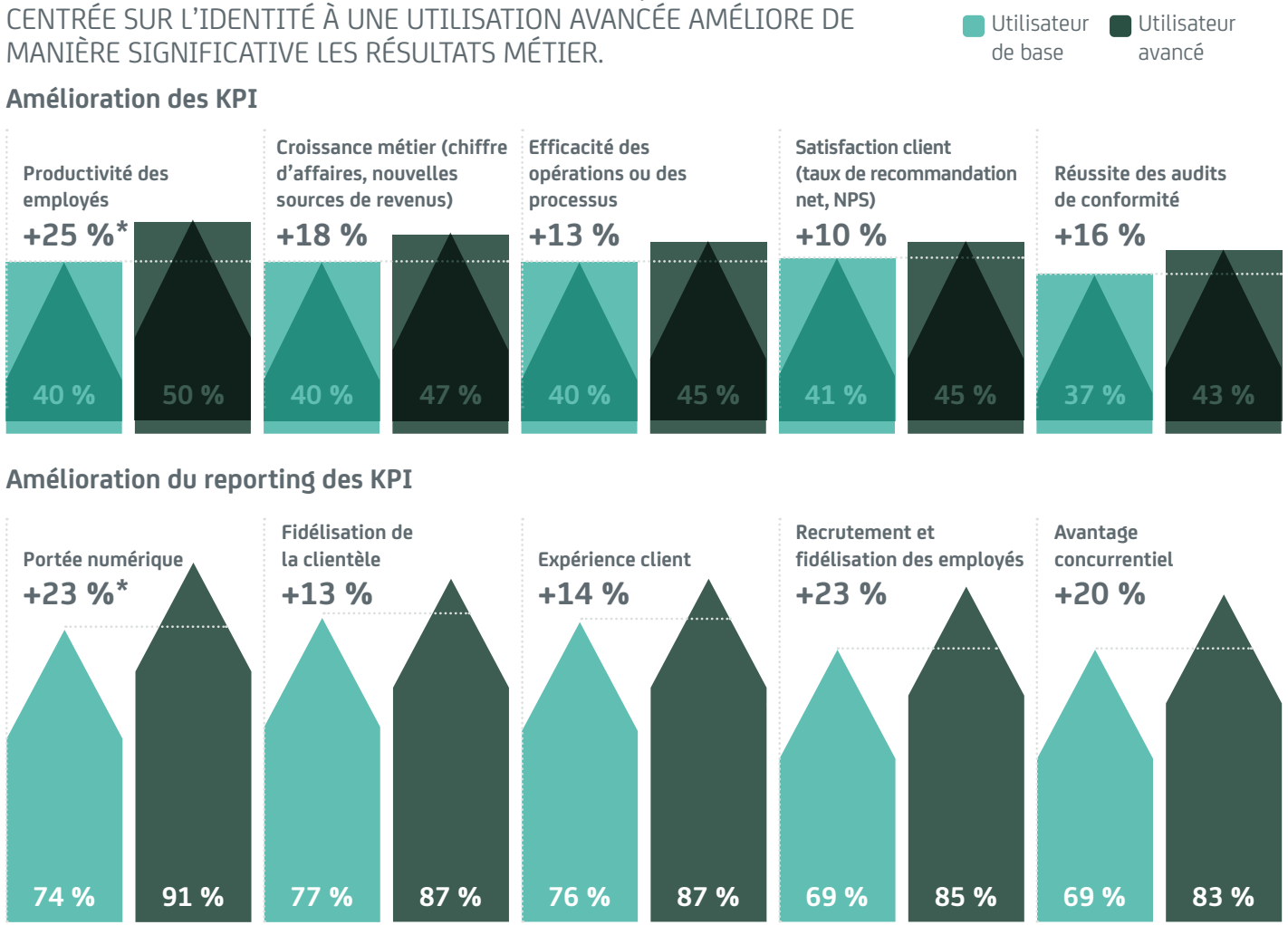


* Pourcentage total des 3 principaux groupes d'utilisateurs pour un classement allant de 1 (inefficace) à 10 (très efficace)

Une conclusion similaire s'impose si nous observons l'impact de la sécurité IT sur les indicateurs clés de performance (KPI) utilisés pour l'évaluation. Les utilisateurs avancés d'une sécurité centrée sur l'identité lui attribuent davantage d'améliorations, sur toutes les mesures métier et de sécurité pour lesquelles nous les avons interrogés.

La différence entre les utilisateurs avancés et les utilisateurs de base va de 10 % à près de 25 % (voir illustration 7). Par exemple, 87 % des utilisateurs avancés observent une amélioration significative en matière d'expérience client, contre 76 % pour les utilisateurs de base. L'impact observé est encore plus important dans le domaine du recrutement et de la fidélisation des employés : 85 % des utilisateurs avancés observent une amélioration, contre 69 % pour les utilisateurs de base.

ILLUSTRATION 7 PASSER D'UNE UTILISATION BASIQUE DE LA SÉCURITÉ CENTRÉE SUR L'IDENTITÉ À UNE UTILISATION AVANCÉE AMÉLIORE DE MANIÈRE SIGNIFICATIVE LES RÉSULTATS MÉTIER.



* % d'amélioration des KPI entre un utilisateur de base et un utilisateur avancé

En termes de protection des données, alors que près du tiers de l'ensemble des utilisateurs observe encore une hausse des violations de sécurité, il est significatif de voir que les utilisateurs avancés sont presque deux fois plus nombreux que les utilisateurs de base à avoir obtenu une réduction du nombre de violations de données. Les deux cinquièmes (41 %) des utilisateurs avancés sont parvenus à réduire le nombre de violations au cours de l'année écoulée, malgré un climat de sécurité de plus en plus difficile. Ce chiffre descend à 21 % pour les utilisateurs de base (voir illustration 8).

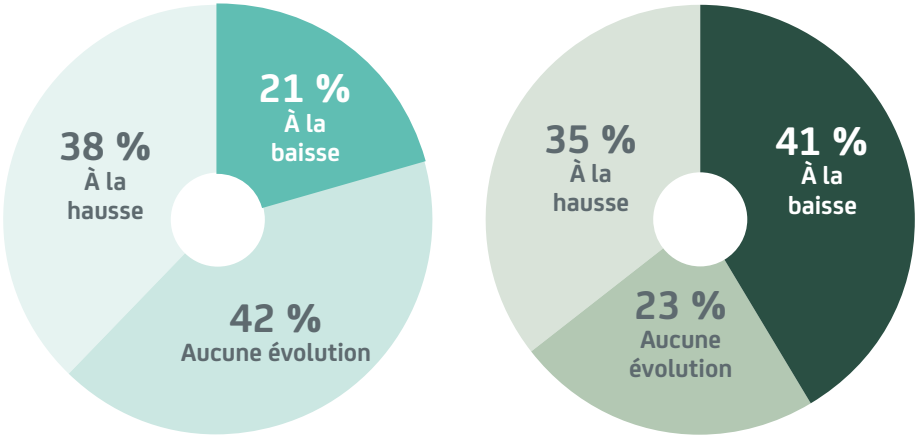
Fiche d'évaluation de l'impact de la transformation numérique sur l'activité

Nous avons également évalué l'impact d'une approche de sécurité orientée identité sur les efforts des entreprises interrogées en matière de transformation numérique.

Pour ce faire, nous avons utilisé la fiche d'évaluation de l'impact de la transformation numérique sur l'activité, que nous avions établie lors de notre enquête sur la transformation numérique des entreprises. Cette fiche évalue l'impact global des initiatives numériques d'une organisation, sur la base de 14 indicateurs clés de performance (KPI) métier, essentiels pour garantir le succès de la transformation numérique.

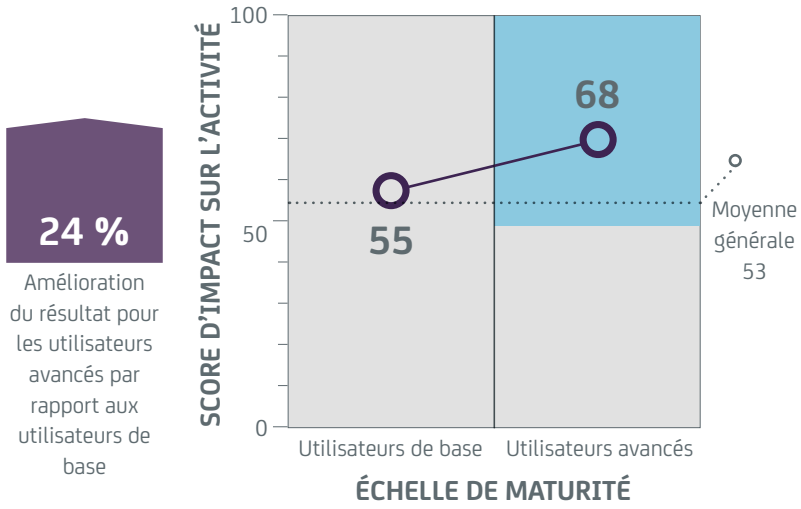
Nous avons comparé les résultats de cette fiche d'évaluation pour les utilisateurs avancés et les utilisateurs de base d'une sécurité centrée sur l'identité. Le score moyen des utilisateurs avancés était de 68 sur 100, contre 55 pour les utilisateurs de base, soit une amélioration de 24 % (voir illustration 9).

ILLUSTRATION 8 PASSER D'UNE UTILISATION BASIQUE DE LA SÉCURITÉ CENTRÉE SUR L'IDENTITÉ À UNE UTILISATION AVANCÉE RÉDUIT LE NOMBRE DE VIOLATIONS DE DONNÉES.



Pourcentage des entreprises indiquant que le nombre de violations de données a augmenté, est resté inchangé ou a diminué.
(La somme totale des pourcentages mentionnés n'est pas égale à 100 du fait de l'arrondi.)

ILLUSTRATION 9 UNE UTILISATION AVANCÉE DE LA SÉCURITÉ CENTRÉE SUR L'IDENTITÉ AMÉLIORE LES RÉSULTATS MÉTIER DE LA TRANSFORMATION NUMÉRIQUE.



04. Les leçons à tirer des utilisateurs avancés de la sécurité centrée sur l'identité

Le constat est clair : les entreprises ayant adopté de façon mature une approche de sécurité centrée sur l'identité bénéficient de meilleurs résultats métier dans tous les domaines. Que font ces utilisateurs avancés pour que leur sécurité soit bien plus efficace ?

Tout d'abord, ils prennent la sécurité IT bien plus au sérieux : 81 % des utilisateurs avancés investissent davantage dans la prévention des violations de sécurité, contre 55 % pour les utilisateurs de base. Par ailleurs, ils ont moins tendance à accepter des concessions en termes de sécurité : 58 % des utilisateurs avancés tolèrent des compromis en matière de sécurité pour accélérer la mise à disposition de leurs applications sur le marché, contre 70 % chez les utilisateurs de base.

Ils sont également plus susceptibles de faire appel aux approches « DevSecOps ». Une majorité d'utilisateurs avancés en matière de sécurité centrée sur l'identité (54 %) appliquent ces pratiques, contre 33 % pour les utilisateurs de base.

Les pratiques DevSecOps sont essentielles dans l'économie des applications. Lorsque votre activité repose sur les technologies numériques, vous devez intégrer la sécurité à vos applications dès le début et ne pouvez pas la traiter comme une notion accessoire. De même que l'approche DevOps intègre la production IT plus tôt dans le cycle de développement logiciel, les pratiques DevSecOps incluent la sécurité plus tôt dans le processus de développement. De cette façon, vous êtes sûr que la sécurité est intégrée à vos applications numériques dès le départ.

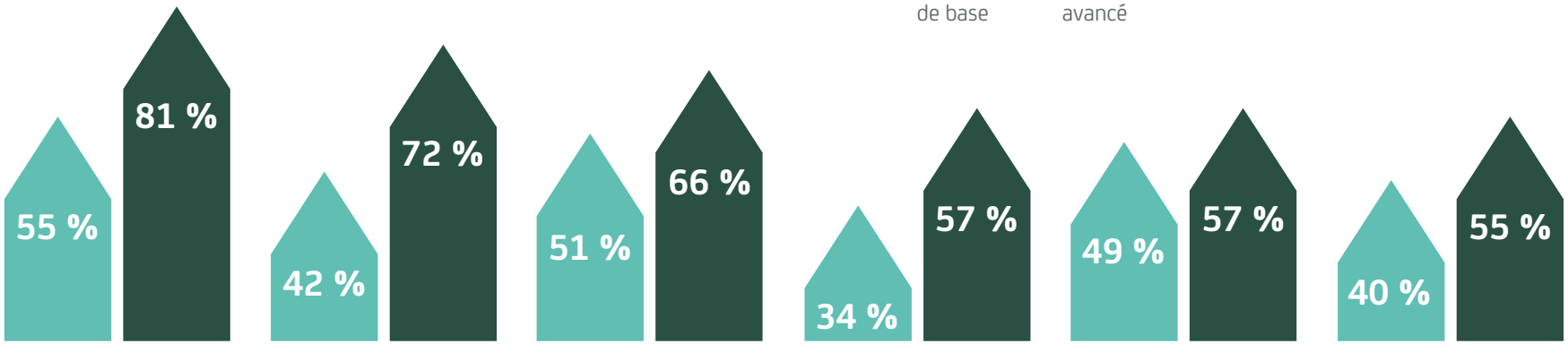
Enfin, les utilisateurs avancés s'efforcent davantage d'aligner leur approche en matière de prévention des violations de sécurité sur les réalités de l'économie des applications (voir illustration 10).

Ils sont bien plus susceptibles de mettre en place une sécurité dédiée pour les applications et les périphériques mobiles (72 contre 42 %), de reconfigurer leurs pratiques de sécurité pour protéger les zones à haut risque, telles que les identités à forts privilèges (57 contre 34 %), de déployer une authentification renforcée (66 contre 51 %) et de restructurer leur activité pour responsabiliser davantage les utilisateurs en matière de sécurité (55 contre 40 %).

« Notre principal casse-tête en matière de sécurité est l'accès distant, qui est devenu monnaie courante pour les utilisateurs aujourd'hui. Notre sécurité IT a donc été centrée ces deux dernières années sur l'authentification. »

Directeur R&D, société pharmaceutique américaine

ILLUSTRATION 10 RAISONS DE LA BAISSE DES VIOLATIONS DE SÉCURITÉ.

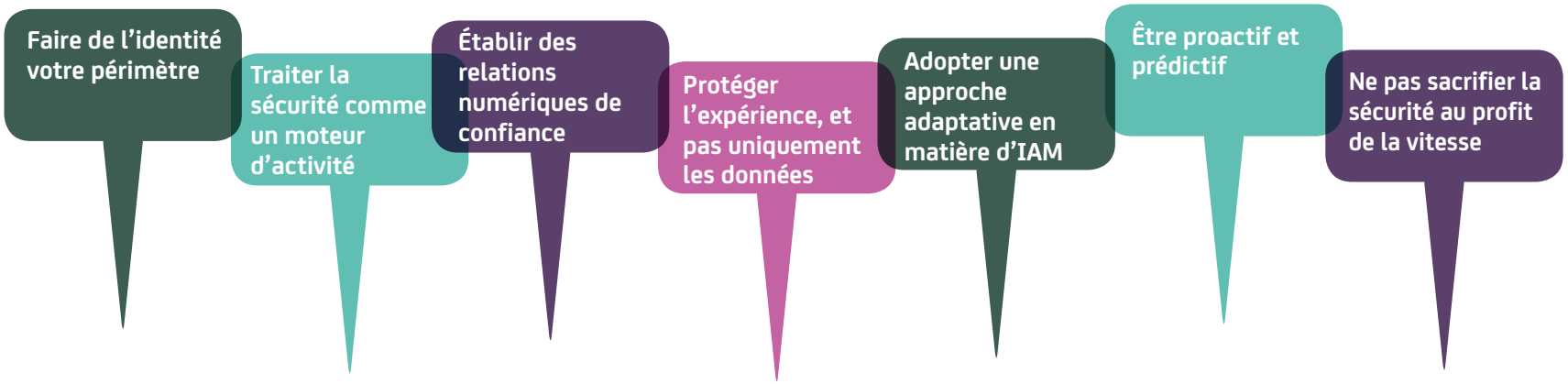


05. Feuille de route pour une sécurité orientée identité efficace

Les résultats de notre enquête plaident clairement en faveur de l'adoption d'une approche de sécurité centrée sur l'identité. Mais par où commencer ? Comment faire en sorte que cette approche fonctionne pour votre entreprise ? Et comment garantir qu'elle améliore réellement les performances et favorise la croissance de votre activité ?

D'après notre expérience, les actions suivantes sont cruciales pour mener à bien une sécurité centrée sur l'identité :

1. **Faire de l'identité votre périmètre.** Les frontières du périmètre de sécurité sont aujourd'hui définies par les utilisateurs, qui accèdent à votre réseau quand et où ils le souhaitent. Vous devez vous assurer que chaque utilisateur est bien celui qu'il prétend être, et qu'il accède uniquement aux informations et aux services qui le concernent. Cela implique une authentification basée sur les risques, associée à une approche analytique pour l'évaluation des identités.
2. **Traiter la sécurité comme un moteur d'activité.** Dans l'économie des applications, la sécurité ne consiste pas uniquement à réduire les risques ; elle génère également une croissance de l'activité. Notre enquête indique qu'une approche de sécurité centrée sur l'identité peut engendrer des avantages ayant pour résultat une amélioration du chiffre d'affaires. Il est donc recommandé d'intégrer à votre cadre d'évaluation de la sécurité des indicateurs de performance métier.
3. **Se consacrer à établir des relations numériques de confiance**. Votre meilleur atout est la relation numérique que vous établissez individuellement avec chaque client. En effet, les clients doivent avoir la certitude que vous comprenez leurs besoins lors de toute interaction avec votre entreprise et que vous protégez leur identité et leurs données de la façon la plus transparente possible.
4. **Protéger l'expérience, et pas uniquement les données**. La sécurité doit être robuste, mais sans friction. Les clients recherchent des interactions rationalisées et des expériences de qualité ; toute perturbation risque de les détourner de vous. Cela implique d'offrir un accès avec authentification unique, des fonctionnalités en self-service et des mécanismes d'authentification homogènes, mais flexibles, lorsque les utilisateurs basculent entre différents périphériques et applications.
5. **Adopter une approche adaptative en matière de gestion des identités et des accès (IAM)**. Les résultats de notre enquête indiquent que les utilisateurs matures d'une sécurité centrée sur l'identité disposent de contrôles IAM pouvant être facilement adaptés en fonction des risques, pour une expérience utilisateur nettement améliorée.
6. **Être proactif et prédictif**. Des outils d'analyse avancée peuvent vous aider à vous prémunir contre les risques de sécurité, au lieu d'être en permanence en mode réactif. Ils permettent en outre de passer à un stade de sécurité supérieur, en vous aidant à détecter, réagir et adapter les processus de sécurité pour faire face aux risques de violations avant que celles-ci se produisent.
7. **Ne pas sacrifier la sécurité au profit de la vitesse**. L'économie des applications a accru la pression sur les entreprises pour que celles-ci livrent leurs nouvelles applications plus rapidement. Il est toutefois plus important que jamais de garantir que la sécurité est intégrée dès le départ, et qu'elle n'est pas compromise à la fin. Vous pouvez notamment envisager une approche DevSecOps pour vous assurer que toutes les problématiques de sécurité ont été traitées à un stade précoce du processus de développement.



Informations complémentaires

Méthodologie de recherche

CA Technologies a demandé au cabinet Coleman Parkes Research de réaliser une enquête auprès de cadres concernant l'étendue et l'impact de l'activité de transformation numérique au sein de leur organisation.

Dans le cadre de cette enquête, nous avons interrogé 1 770 décideurs métier et IT (y compris 106 CSO/CISO) travaillant dans de grandes entreprises situées dans 21 pays différents issus des régions Amériques, Europe, Moyen-Orient, Afrique (EMEA) et Asie-Pacifique, Japon (APJ). Les organisations ayant participé à l'étude enregistrent des revenus annuels supérieurs à 1 milliard de dollars (ou 0,5 milliard dans les économies de plus petite taille).

Les pays étudiés étaient les suivants :

Amériques	**EMEA**	**APJ**
Brésil	Afrique du Sud	Australie
États-Unis	Allemagne	Chine
	Espagne	Corée
	France	Hong Kong
	Italie	Inde
	Pays-Bas	Indonésie
	Royaume-Uni	Japon
	Suède	Malaisie
	Suisse	Singapour
		Thaïlande

Les secteurs d'activité étudiés étaient les suivants :

- Automobile
- Services bancaires et financiers
- Énergie et services publics
- Santé
- Production industrielle
- Médias et divertissements
- Secteur public national
- Commerce de détail
- Télécommunications
- Transport et logistique

L'étude et les analyses ont été conduites en mai et juin 2016.

À propos de CA Technologies

CA Technologies (NASDAQ : CA) fournit les logiciels qui aident les entreprises à opérer leur transformation numérique. Dans tous les secteurs, les modèles économiques des entreprises sont redéfinis par les applications. Partout, une application sert d'interface entre une entreprise et un utilisateur. CA Technologies aide ces entreprises à saisir les opportunités créées par cette révolution numérique et à naviguer dans « l'Économie des applications ». Grâce à ses logiciels pour planifier, développer, gérer la performance et la sécurité des applications, CA Technologies aide ainsi ces entreprises à devenir plus productives, à offrir une meilleure qualité d'expérience à leurs utilisateurs et leur ouvre de nouveaux relais de croissance et de compétitivité sur tous les environnements : mobile, Cloud, distribué ou mainframe. www.ca.com/fr

À propos de Coleman Parkes Research

Spécialisée dans le recrutement et les interviews de cadres supérieurs, Coleman Parkes Research intervient sur de multiples marchés mondiaux, secteurs d'activité et domaines fonctionnels pour le compte de divers clients. Nous faisons tout : recherches autour du leadership éclairé pour les relations publiques et les campagnes marketing, analyse des opportunités de pertes/gains, test des messages de produits, interviews approfondies de cadres supérieurs. Coleman Parkes Research travaille en collaboration avec les clients pour formuler des stratégies éprouvées qui procurent des informations sur le marché en fonction de besoins spécifiques et d'hypothèses clés. colemanparkes.com/

À propos de Grist

Services éditoriaux et créatifs. Grist est une agence B2B primée, spécialisée dans le leadership éclairé et le marketing de contenu. Forts de l'héritage éditorial de The Economist et The Financial Times, nous offrons une vision claire du futur numérique. www.gristonline.com