STATE OF DIGITAL TRUST

PILLARS OF TRUST

C- LEVEL, DIRECTOR
MANAGER INSIGHTS

DIGITAL TRUST READINESS
SCORE
1245.56°
753234.72°

IDENTITY

AUTOMATION
433.6°
24567.76°

ID 7021.4

THREATS

XX
SECURITY ALERT

ZERO TRUST

NOVEMBER 2022

ENTERPRISES
EMPLOYEES
CUSTOMERS
6578.854°
6785.77°

GLOBAL STUDY

digicert®

CONFIANCE NUMÉRIQUE : RAPPORT D'ENQUÊTE DIGICERT 2022

La transformation numérique et la pandémie ont accéléré notre transition d'un monde physique et analogue vers un univers digital hyperconnecté, soulevant par là même une question essentielle : comment établir la confiance dans ce nouvel écosystème ?
Comment…

- vérifier la légitimité des personnes (et des appareils) avec lesquels nous communiquons ?
- savoir que les données que nous consommons sont sûres ?
- veiller à ne pas être l'objet de compromissions ou d'attaques par déni de service (DoS) ?
- s'assurer de la protection et de l'intégrité des services et applications que nous utilisons ?

La tâche n'est pas simple, car ce nouveau monde a considérablement élargi les surfaces d'attaque, tandis que le coût de la moindre faille de sécurité a explosé. Surtout qu'au-delà des dépenses liées aux aspects juridiques, réglementaires et de remédiation, l'entreprise a souvent beaucoup plus à perdre en termes de perte de clients et d'érosion de l'image de marque. Selon un rapport Forbes Insights, près de la moitié (46 %) des entreprises ont été victimes d'une compromission qui a porté atteinte à leur réputation et leur image de marque[1].

Ce constat a propulsé la question de la confiance numérique au premier plan. Selon Jennifer Glenn, Directrice de recherche pour IDC, la confiance numérique est la base d'un monde connecté sûr et sécurisé. Elle représente donc un élément indispensable à toute entreprise qui cherche à rassurer ses clients, collaborateurs et partenaires quant à la fiabilité de ses processus et interactions en ligne.

Bref, la confiance numérique permet d'être un acteur à part entière du monde digital.

Leader de la confiance numérique, DigiCert apporte aux entreprises et aux particuliers les outils qui leur permettront d'échanger et de communiquer de façon sereine et sécurisée dans l'univers du digital. C'est pourquoi nous nous engageons à mieux comprendre comment les entreprises perçoivent la confiance numérique et quel est leur niveau de maturité dans ce domaine.

Le rapport DigiCert 2022 sur la confiance numérique dresse un état de lieux du niveau d'adoption et d'appropriation de ce concept au niveau des entreprises, des salariés et des consommateurs du monde entier.

[1]The Reputational Impact of IT Risk – Forbes Insights

Qu’est-ce que la confiance numérique ?

Selon Jennifer Glenn, Directrice de recherche pour IDC, la confiance numérique est la base d’un monde connecté sûr et sécurisé. Elle représente donc un élément indispensable à toute entreprise qui cherche à rassurer ses clients, collaborateurs et partenaires quant à la fiabilité de ses processus et interactions en ligne.

La confiance numérique s’articule autour de quatre piliers :

1. Les standards, qui permettent de définir les exigences pour la confiance en une technologie ou un secteur donné.
2. La conformité et les opérations, qui génèrent ou vérifient les certificats numériques établissant la confiance numérique (sous-tendues par les trois éléments essentiels que sont l’identité, l’intégrité et le chiffrement), dans le respect des standards établis par les organismes normatifs.
3. La gestion de la confiance, garante de la bonne gouvernance des entreprises sur tout le cycle de vie des certificats, et ce grâce à une visibilité et à un contrôle centralisés sur leur utilisation.
4. La confiance connectée, qui permet d’étendre la confiance au sein de supply chains plus complexes (typiques des logiciels, équipements et contenus).

C’est sur ces quatre grands piliers que repose la confiance numérique. Les entreprises peuvent soit faire appel à des tiers pour tout ou partie de ces activités, soit en assurer la gestion en interne.

DE L'IMPORTANCE DE LA CONFIANCE NUMÉRIQUE

La confiance numérique s'est révélée être un sujet sensible pour les participants à notre étude, puisque 100 % des entreprises la considèrent comme importante et la plupart (90 %) comme très importante. À tel point que près de deux tiers d'entre elles déclarent s'être séparées de fournisseurs ayant perdu leur confiance. Et presque toutes (99 %) pensent que leurs clients pourraient se tourner vers la concurrence si elles ne parvenaient pas à garder leur confiance. Près de la moitié (47 %) considèrent même cette éventualité comme probable.

Les salariés des entreprises sont également très impliqués dans les questions de confiance numérique. Tous (100 %) la considèrent comme importante, et 86 % comme très importante. Dans le cadre de leurs missions au sein de l'entreprise, 99 % affirment qu'ils seraient prêts à rompre leur relation avec un fournisseur en qui ils n'ont plus confiance. Environ la moitié (51 %) estiment cette rupture comme « probable ».

Enfin, la confiance numérique est considérée comme importante pour deux tiers (68 %) des consommateurs, et très importante pour un tiers (36 %) d'entre eux. La moitié (47 %) déclare que par le passé, ils ont déjà rompu une relation avec une entreprise en qui ils n'avaient plus confiance. Ils sont 84 % à dire qu'ils envisageraient une telle rupture, et 57 % à l'estimer probable dans ce cas de figure. L'importance accordée à la confiance numérique semble aussi augmenter avec le niveau de revenus des consommateurs (58 % des consommateurs aux revenus supérieurs à la moyenne accordent de l'importance à la confiance numérique).

Méthodologie

En septembre 2022, Eleven Research, un spécialiste des études de marché basé à Dallas, a dressé un état des lieux de la confiance numérique. L'enquête a été menée par téléphone et par e-mail auprès de 400 entreprises et 400 consommateurs du monde entier.

Entreprises

Au total, 400 responsables (IT, sécurité de l'information, DevOps) et dirigeants d'entreprises de 1 000 salariés et plus ont été interrogés : figure A (voir p. 5)

Consommateurs

Nous avons interrogé 400 consommateurs (provenant des mêmes régions) de différents âges, sexes, orientations politiques et catégories sociodémographiques : figure B (voir p. 5)

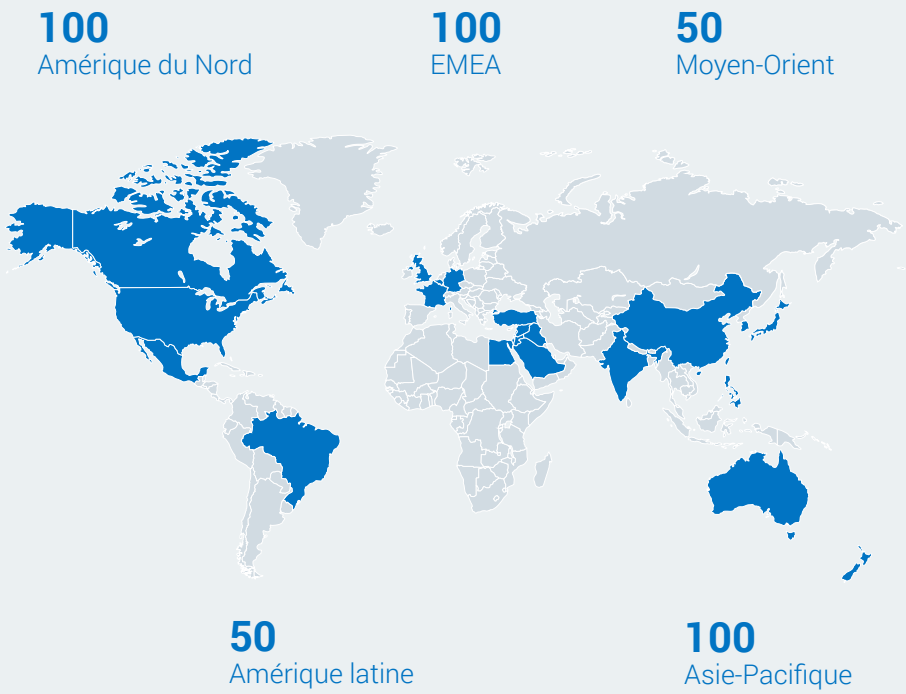


Figure A.

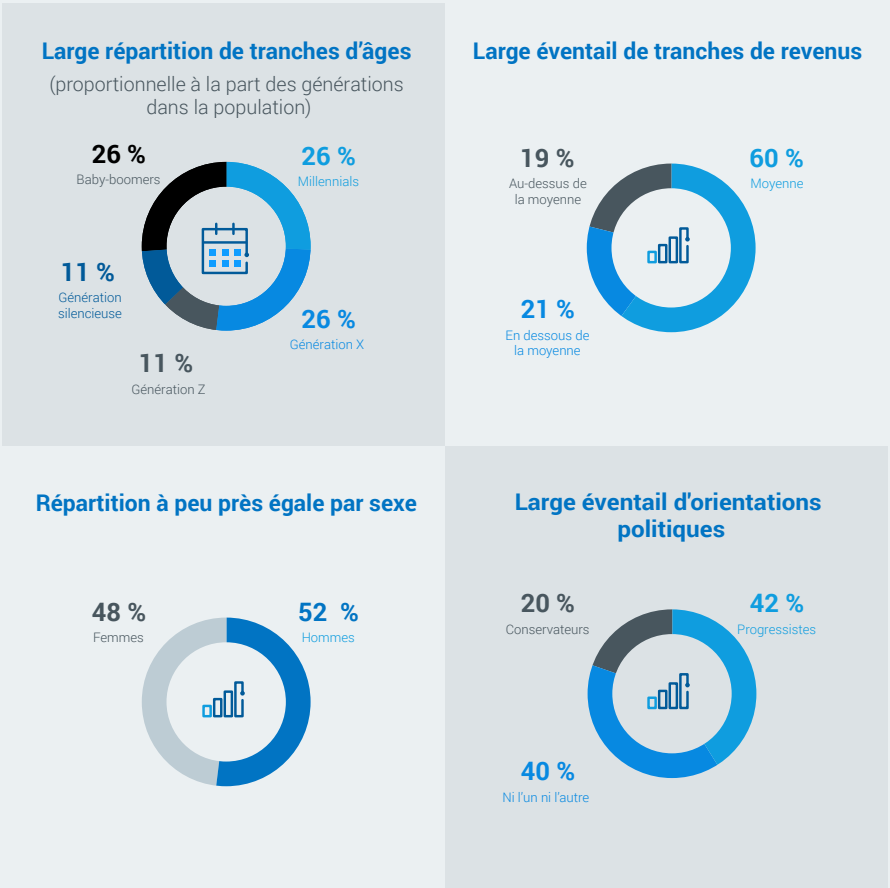
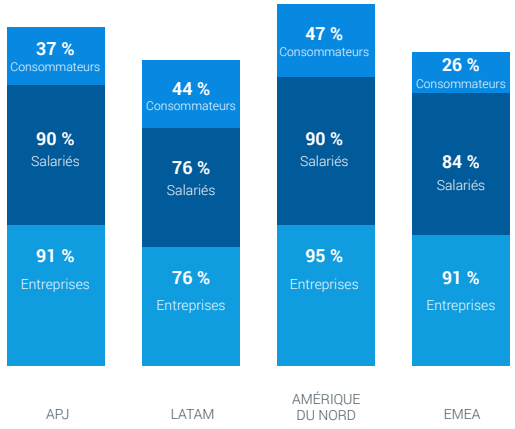


Figure B.

CONFIANCE NUMÉRIQUE : UNE IMPORTANCE À GÉOGRAPHIE VARIABLE

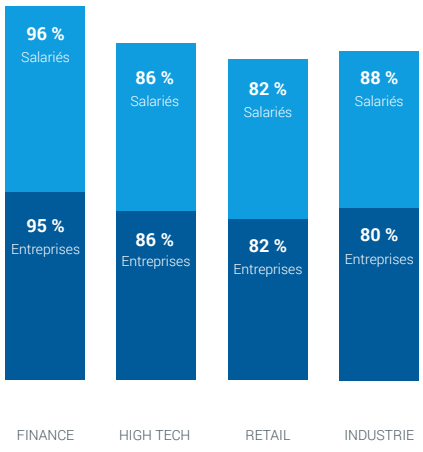
Entreprises, salariés et consommateurs sont unanimes quant à l'importance de la confiance numérique. Toutefois, le niveau d'importance dépend d'une variété de paramètres.

CONFIANCE NUMÉRIQUE CONSIDÉRÉE COMME TRÈS IMPORTANTE (PAR RÉGION)



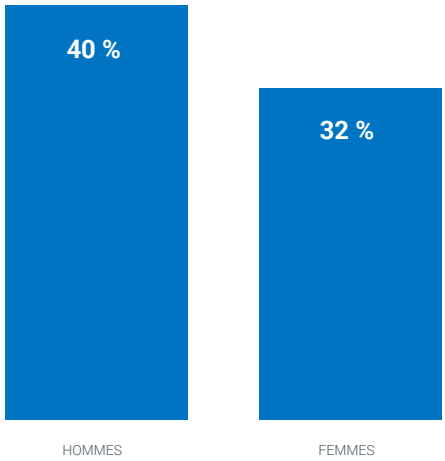
Côté entreprises et salariés, l'Amérique latine compte moins de participants déclarant accorder une très grande importance à la confiance numérique. Même verdict pour les consommateurs des régions APJ et EMEA. Concrètement, les consommateurs EMEA ne sont que 26 % à accorder beaucoup d'importance à la confiance numérique, ce qui paraît assez étonnant compte tenu de la promulgation du RGPD en 2018.

CONFIANCE NUMÉRIQUE CONSIDÉRÉE COMME TRÈS IMPORTANTE (PAR SECTEUR D'ACTIVITÉ)



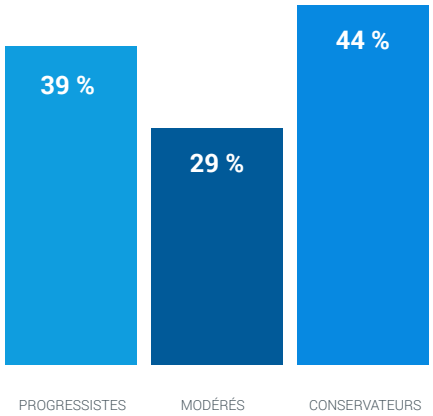
Sans surprise, les établissements financiers sont les plus susceptibles de considérer la confiance numérique comme très importante.

CONFIANCE NUMÉRIQUE CONSIDÉRÉE COMME TRÈS IMPORTANTE (SELON LE SEXE DES CONSOMMATEURS)



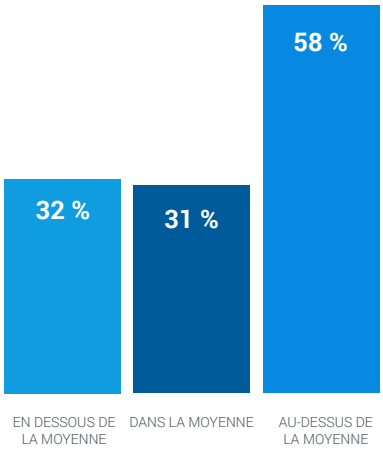
Côté consommateurs, les hommes accordent davantage d'importance à la confiance numérique que les femmes.

CONFIANCE NUMÉRIQUE CONSIDÉRÉE COMME TRÈS IMPORTANTE (SELON L'AFFILIATION POLITIQUE DES CONSOMMATEURS)



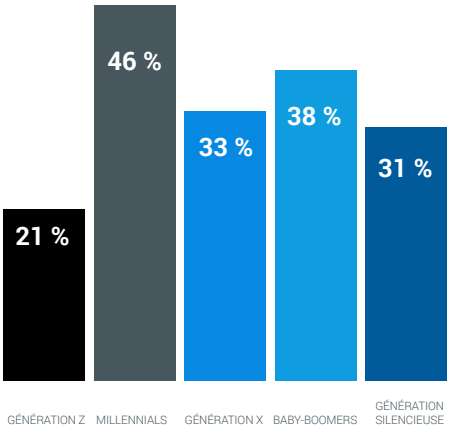
Enfin, sur le plan des opinions politiques, la confiance numérique rallie progressistes et conservateurs. Les uns comme les autres sont nombreux à la considérer comme très importante.

CONFIANCE NUMÉRIQUE CONSIDÉRÉE COMME TRÈS IMPORTANTE (SELON LES REVENUS DES CONSOMMATEURS)



Les consommateurs dont les revenus se situent au-dessus de la moyenne accordent également beaucoup plus d'intérêt à cette question.

CONFIANCE NUMÉRIQUE CONSIDÉRÉE COMME TRÈS IMPORTANTE (SELON LA GÉNÉRATION DES CONSOMMATEURS)



Fait intéressant, les deux plus jeunes générations de consommateurs (et les seules à se situer dans la catégorie « digital-native ») sont respectivement les moins et les plus susceptibles d'accorder une très grande importance à la confiance numérique.

LES RESSORTS DE L'INTÉRÊT POUR LA CONFIANCE NUMÉRIQUE

Tout le monde s'intéresse à la confiance numérique. Toutefois, les facteurs qui suscitent cet intérêt sont multiples.

Explosion de la data. Selon les sondés, il s'agit du principal facteur. Pourquoi ? Parce qu'aujourd'hui, les volumes de données augmentent de 23 % par an[2]. Pour vous donner une meilleure idée, alors qu'il a fallu 70 ans pour amasser 97 Zo de données dans le monde fin 2021, ce chiffre aura presque doublé fin 2025, soit seulement quatre ans après, pour atteindre 174 Zo. L'équivalent de plus de 20 000 Go pour chaque être humain d'ici 2025 !

Au-delà des volumes de données, l'enjeu se situe également au niveau de l'importance de ces données. Ce que nous achetons, les sites que nous visitons, nos dossiers médicaux, nos réseaux sociaux, nos photos… toutes ces données constituent un véritable gisement d'informations à caractère personnel (PII).

Élargissement de la surface d'attaque. Les entreprises ont transformé leurs réseaux relativement statiques, organisés autour de structures internes (data centers, bureaux et sites distants), en des réseaux hybrides beaucoup plus complexes. Ces nouvelles infrastructures connectent non seulement les data centers, bureaux et sites distants existants, mais aussi des milliers d'environnements de télétravail, de multiples clouds, équipements numériques, réseaux de périphérie (edge) et appareils IoT.

Dans ce nouvel espace sans périmètre, les points d'attaque sont légion.

Attentes des consommateurs. Comme nous l'avons vu dans la section précédente, 100 % des entreprises et 68 % des consommateurs accordent de l'importance à la confiance numérique. Dans une catégorie comme dans l'autre, chacun est prêt à passer à la concurrence s'il perd confiance en une entreprise, ce qui hisse la confiance numérique au rang des facteurs qui peuvent faire et défaire une entreprise.

Multiplication des attaquants. Le nombre d'attaquants augmente chaque année :

- Black hats
- Cybercriminels
- Cyberterroristes
- Hacktivistes
- Ennemis de l'intérieur
- Groupes étatiques
- Trolls et hackers récréatifs

Cette croissance est prouvée par le nombre de plaintes record recueillies par l'Internet Crime Complaint Center (IC3) en 2021 : 847 376, soit 7 % de plus qu'en 2020[3].

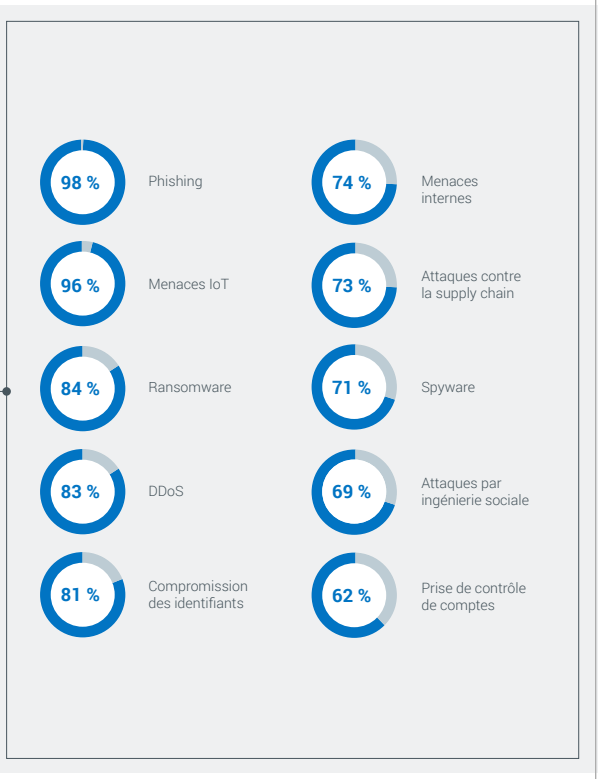
[2]Big Growth Forecasted for Big Data – IDC
[3]FBI Internet Crime Complaint Center (IC3)

LES ENJEUX

Que protègent les entreprises ? La fidélité client est citée comme un enjeu majeur par toutes les entreprises (100 %) interrogées. Ceci est somme toute logique quand on considère qu'un client peut vite passer à la concurrence s'il perd confiance en une entreprise.

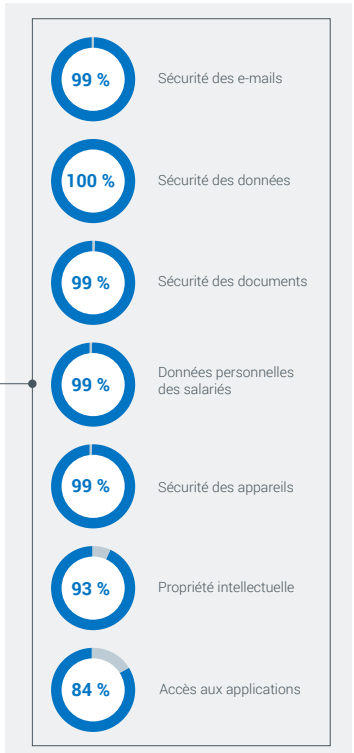
Les types d'attaque que les sondés craignent le plus sont les suivants (dans cet ordre) :

POUR LES ENTREPRISES…



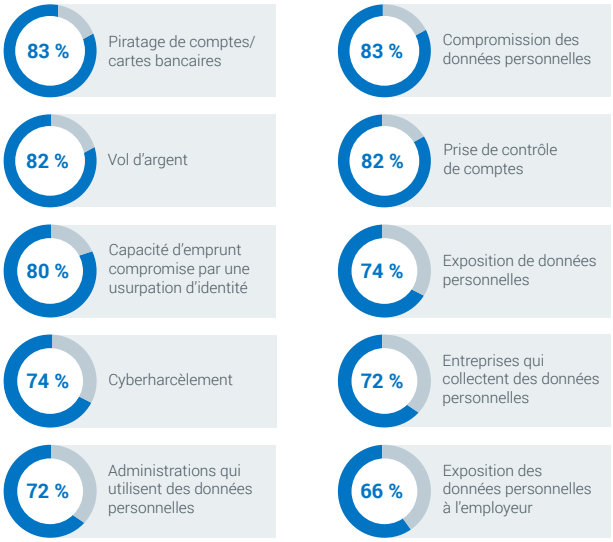
Les salariés, eux, ont une tout autre préoccupation : leurs données personnelles.

POUR LES SALARIÉS…

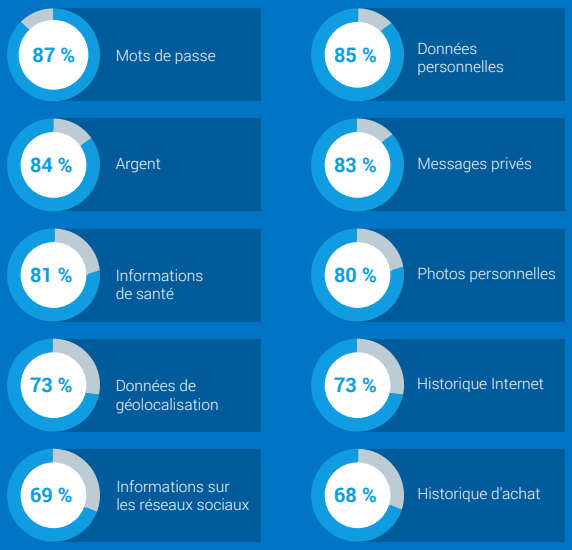


Enfin, les préoccupations des consommateurs sont multiples :

LES CONSOMMATEURS CRAIGNENT…

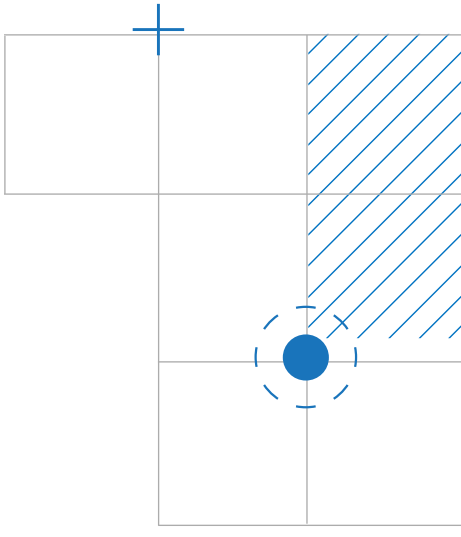


LES CONSOMMATEURS VEULENT PROTÉGER…



Nous avons cherché à savoir si les entreprises étaient en phase avec les consommateurs sur la protection des ressources qui comptent le plus pour eux (mots de passe, données personnelles, etc.). Quasiment toutes les attaques qui compromettent les données des consommateurs commencent par un e-mail[4]. Ceci dit, malgré tout ce qu'elles mettent en œuvre pour protéger les consommateurs, les entreprises classent leur protection anti-phishing en avant-dernière position en termes de performances, et ce alors même qu'elles considèrent ce type d'attaque comme le plus préoccupant.

Par conséquent, malgré toute la bonne volonté affichée par les entreprises pour répondre aux besoins prioritaires des consommateurs, elles ont encore beaucoup à faire pour atteindre le niveau de sécurité attendu par ces derniers.

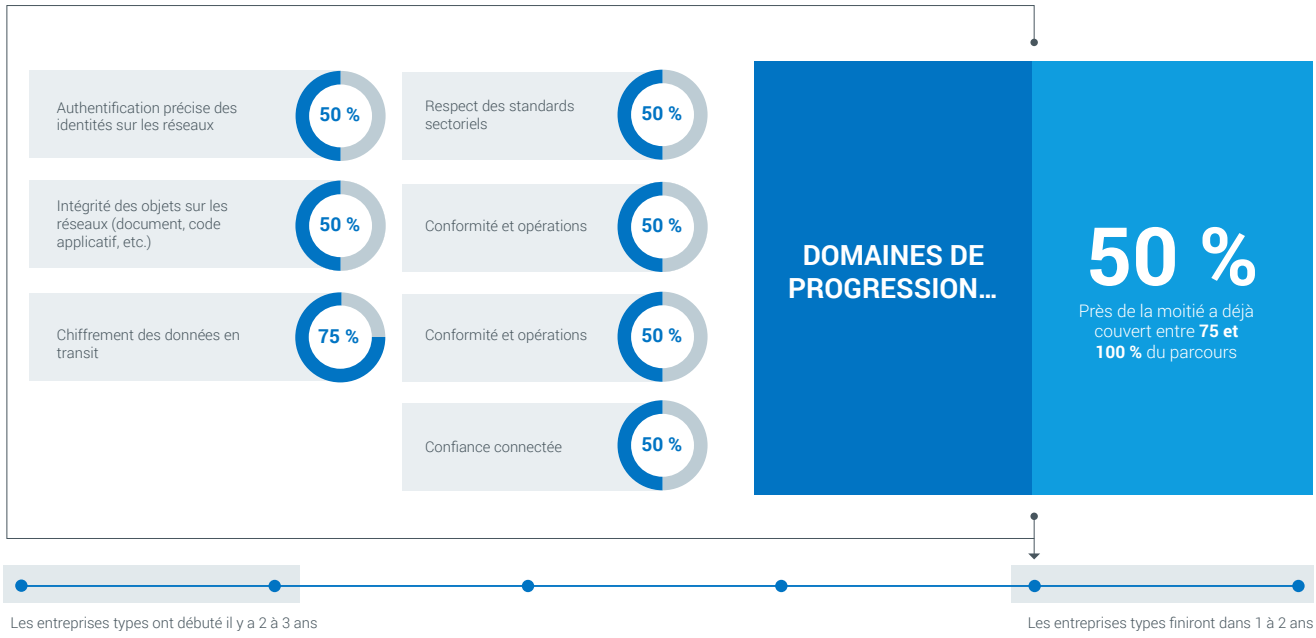


[4]Why Your Business Needs Better Email Security – Guardian Digital

COMMENT LES ENTREPRISES OPTIMISENT-ELLES LA CONFIANCE NUMÉRIQUE ?

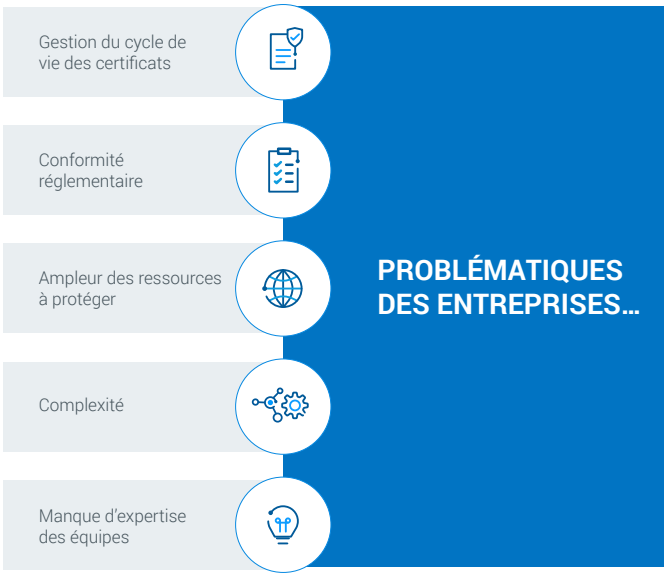
La confiance numérique fait partie des engagements déjà pris par les entreprises. Une entreprise type aura ainsi entamé son parcours il y a deux ou trois ans, et couvert 75 % (ou plus) du processus à l'heure actuelle, avec un achèvement prévu à un horizon de un à deux ans.

La confiance numérique comporte de multiples facettes. Nous avons analysé plus en détail l'état d'avancement des entreprises sur chacune d'entre elles.



Objectifs de confiance numérique : pour les entreprises interrogées, la fidélité client apparaît clairement comme le principal objectif en matière de confiance numérique. Toutes (100 %) l'ont qualifié d'important, ce qui le place largement en tête. Il est pourtant loin d'être le seul objectif des entreprises…

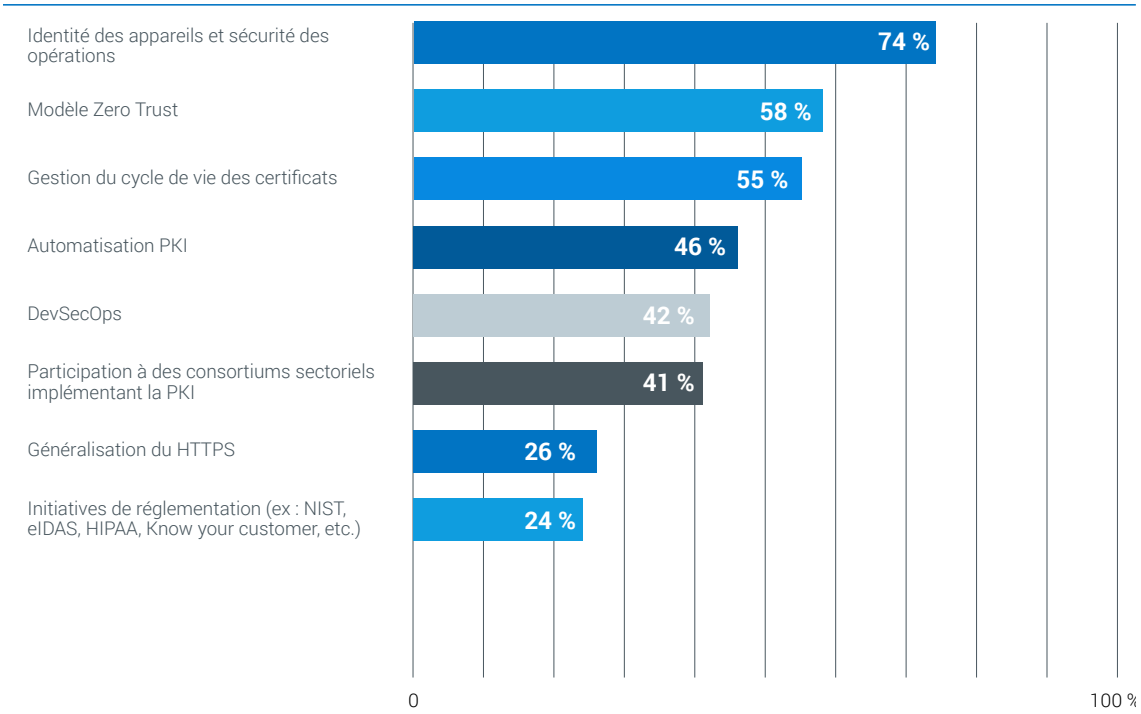
Obstacles à la confiance numérique : les entreprises sont certes bien avancées dans leur parcours vers une confiance numérique totale, mais le cheminement n'a pas été de tout repos. En tête des problématiques citées par les équipes IT se trouve la gestion des certificats numériques, considérée comme importante par 100 % des entreprises. La conformité réglementaire et l'étendue massive des ressources à protéger arrivent en deuxième position, à 99 %. Viennent ensuite la complexité liée à la sécurisation d'un réseau multifournisseur complexe et dynamique, et le manque d'expertise interne.



Pratiques de confiance numérique : un grand nombre d'initiatives peuvent sous-tendre la confiance numérique d'une entreprise. Ces initiatives étant à des stades plus ou moins avancés d'une entreprise à l'autre, nous avons jugé utile de faire le point.

En tête se trouve la sécurité des opérations et les identités des appareils, une initiative aujourd'hui pleinement mise en œuvre par 74 % des entreprises. Viennent ensuite les politiques Zero Trust, qui ne sont cependant pleinement mises en œuvre que par 58 % des entreprises. La seule autre initiative déployée par plus de la moitié des entreprises (55 %) est la gestion du cycle de vie des certificats. Voici le classement complet :

Q22 : Quelle est votre implication dans les pratiques de confiance numérique suivantes ?
(Déploiement terminé)

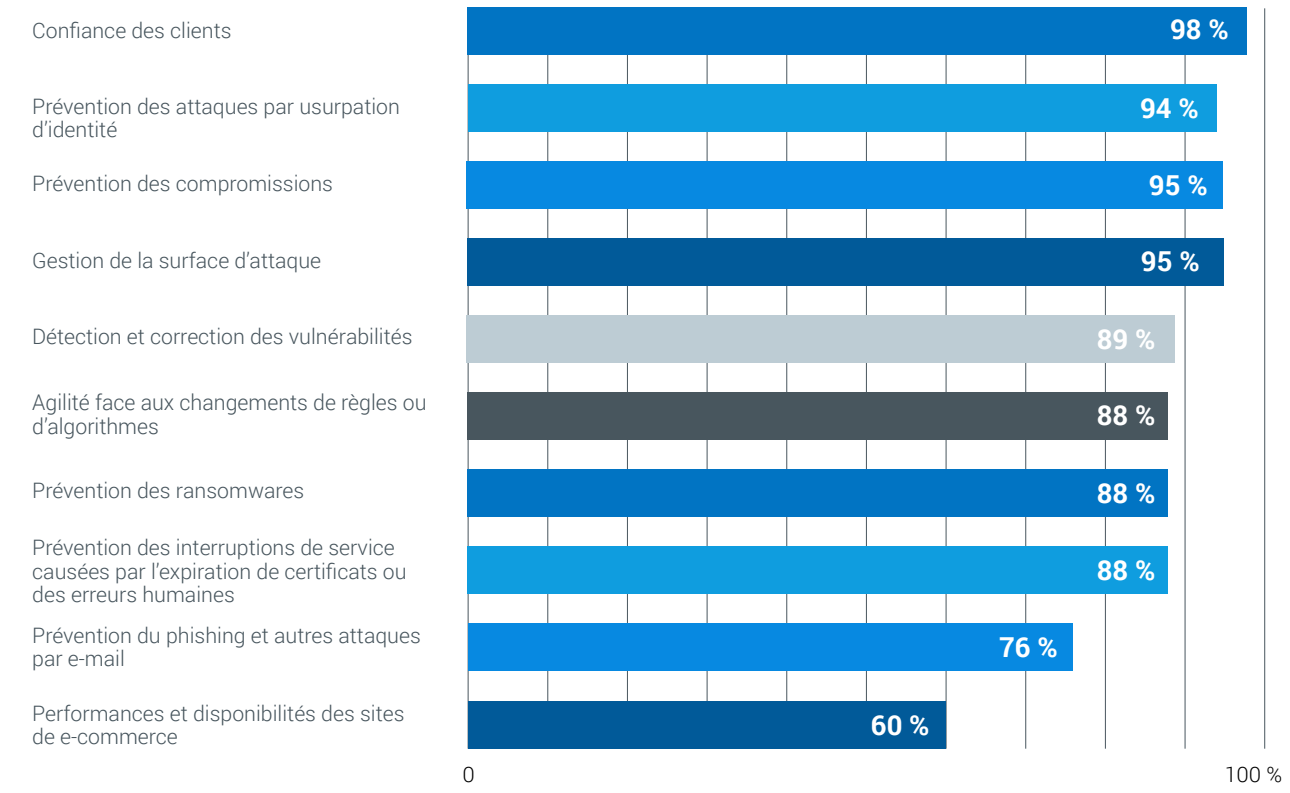


MÉTRIQUES DE CONFIANCE NUMÉRIQUE DANS LES ENTREPRISES

Les entreprises s'en sortent plutôt bien sur un large éventail de métriques relatives aux objectifs de confiance numérique. Par exemple, sur leur objectif principal (la fidélité client), 98 % des entreprises s'en sortent bien (dont 61 % extrêmement bien). Elles obtiennent également de bons résultats sur la prévention des compromissions (95 %, avec de très bons résultats pour 51 %) et les attaques par usurpation d'identité (94 %, avec de très bons résultats pour 50 %).

En fait, au moins sept entreprises sur huit déclarent obtenir de bons scores sur huit des dix métriques étudiées. Elles accusent cependant un certain retard dans la prévention du phishing et des attaques par e-mail d'une part, et les performances et la disponibilité des sites de e-commerce d'autre part (76 % et 60 %, respectivement).

Q23 : Quel est votre niveau de performance pour chacune des métriques de confiance numérique suivantes ?
(Haut/Très haut)



Les clients constatent des améliorations

Toutes les entreprises (100 %) déclarent que la confiance numérique est importante pour leurs clients, et même très importante pour 91 % d'entre elles.

D'où la nécessité de faire un point sur la manière dont ces clients perçoivent le niveau de confiance numérique des entreprises. Les nouvelles sont plutôt bonnes de côté-là, avec 99 % d'entreprises qui affirment que leur cote de confiance numérique est aujourd'hui plus élevée auprès de leurs clients. Et près des trois quarts (73 %) déclarent qu'elle est beaucoup plus élevée.

Qu'en est-il du côté des clients B2B ? Partagent-ils l'optimisme des fournisseurs ? On peut dire que oui puisque les chiffres sont quasiment identiques. En effet, lorsqu'il leur a été demandé d'évaluer leur confiance envers les autres entreprises avec lesquelles elles interagissent, 98 % déclarent que cette confiance est plus forte aujourd'hui que par le passé, et 76 % la disent beaucoup plus forte.

Ceci ne concerne toutefois que les interactions B2B. Qu'en est-il du B2C ? À ce niveau, les chiffres sont beaucoup plus mitigés. En effet, moins de la moitié des sondés déclarent que leur confiance numérique vis-à-vis des entreprises avec lesquelles ils traitent est plus élevée qu'auparavant, tandis que 54 % déclarent qu'il y a encore matière à s'améliorer.

Amérique du Nord

L'Amérique du Nord (États-Unis et Canada) se situe en tête des régions qui accordent une très grande importance à la confiance numérique et ce, toutes catégories confondues : entreprises, salariés et consommateurs.

Les consommateurs nord-américains sont notamment les plus préoccupés par les cybermenaces (par ex., piratage de comptes ou de cartes bancaires et vol d'argent) que ceux du reste du monde, à l'exception de l'Asie-Pacifique. (91 % des consommateurs APAC sont préoccupés par ces menaces contre 85 % pour l'Amérique du Nord, et respectivement 77 % et 78 % pour les régions EMEA et LATAM).

Tout ceci se reflète dans le score élevé que les consommateurs attribuent aux entreprises nord-américaines. Concernant les effets positifs de la confiance numérique, 31 % des consommateurs nord-américains déclarent avoir beaucoup plus confiance dans les entreprises avec lesquelles ils traitent. Ceux de la région APAC se situent au milieu avec 19 %, entre l'Amérique latine (24 %) et la région EMEA (15 %).

APAC

Dans l'ensemble, l'Asie-Pacifique considère la confiance numérique comme très importante. Avec l'Amérique du Nord, il s'agit de la région la plus soucieuse de ces questions.

Cette tendance s'explique en partie par le fait que les consommateurs APAC sont davantage préoccupés par les cybermenaces (par ex., piratage de comptes ou de cartes bancaires et vol d'argent) que ceux du reste du monde. (91 % des consommateurs APAC sont préoccupés par ces menaces contre 85 % pour l'Amérique du Nord, et respectivement 77 % et 78 % pour les régions EMEA et LATAM).

Concernant les effets positifs de la confiance numérique, 19 % des consommateurs APAC déclarent faire aujourd'hui beaucoup plus confiance aux entreprises avec lesquelles ils traitent. Ce chiffre se situe à 31 % pour l'Amérique du Nord, 24 % pour l'Amérique latine et tout juste 15 % pour la région EMEA.

LATAM

De manière générale, les sondés d'Amérique latine sont moins nombreux à considérer la confiance numérique comme très importante.

Ce constat s'explique en partie par le fait que les consommateurs latino-américains sont moins préoccupés par les cybermenaces (par ex., piratage de comptes ou de cartes bancaires et vol d'argent) que la plupart des autres. (Seulement 78 % des consommateurs LATAM sont préoccupés par ces menaces, contre 91 % en région APAC, 85 % en Amérique du Nord et 77 % en région EMEA).

Côté confiance numérique, les effets sur les consommateurs LATAM semblent relativement élevés, puisque 24 % d'entre eux déclarent avoir aujourd'hui beaucoup plus confiance dans les entreprises avec lesquelles ils traitent. En Amérique du Nord, 31 % des consommateurs partagent cet avis. Ils sont respectivement 19 % et 15 % dans les régions APAC et EMEA.

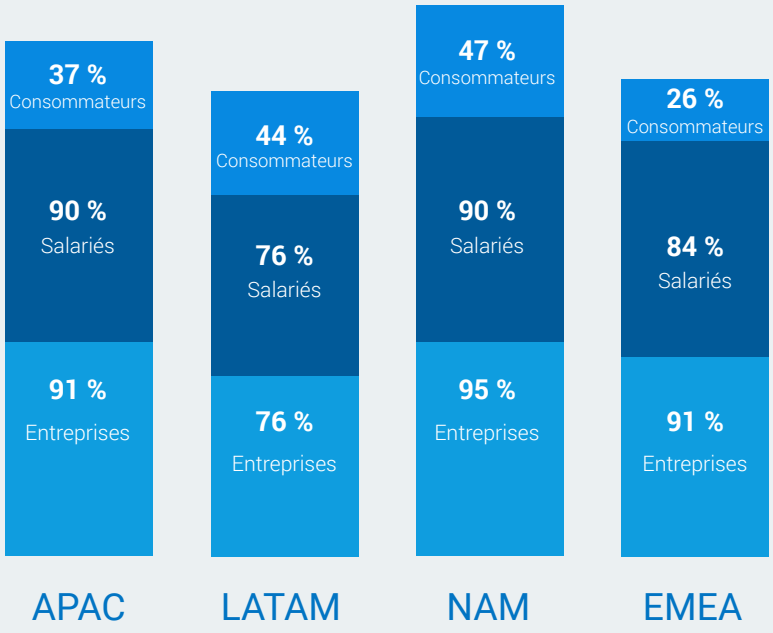
EMEA

Pour la région du globe qui applique l'une des réglementations les plus strictes en matière de protection de la vie privée (RGPD), les consommateurs EMEA semblent étonnamment détachés des questions de confiance numérique. Sur l'ensemble, l'EMEA se classe en troisième position sur l'importance accordée à la confiance numérique. À y regarder de plus près, on constate un fort intérêt des entreprises et un intérêt moyen des salariés de cette région. Quant aux consommateurs, ils sont quasiment la moitié, par rapport à ceux d'Amérique du Nord, à accorder de l'importance à la confiance numérique.

Ce chiffre renvoie directement aux préoccupations concernant les cybermenaces. En effet, les consommateurs EMEA sont les moins préoccupés par les cybermenaces telles que le piratage de comptes bancaires ou de cartes de crédit et le vol d'argent. Seulement 77 % se disent préoccupés par ces menaces, contre 78 % des consommateurs LATAM, 85 % de l'Amérique du Nord et 91 % de la région APAC.

On observe également une corrélation avec le pourcentage relativement faible (15 %) de consommateurs EMEA qui affirment que leur confiance dans les entreprises avec lesquelles ils traitent a augmenté ces dernières années. Là encore, l'EMEA se place derrière les autres régions : APAC (19 %), LATAM (24 %) et Amérique du Nord (31 %).

CONFIANCE NUMÉRIQUE CONSIDÉRÉE COMME TRÈS IMPORTANTE (PAR RÉGION)



LEÇONS DU « DIGITAL TRUST COGNOSCENTI »

Comme nous l'avons vu, les entreprises affichent de plutôt bons résultats dans leurs initiatives de confiance numérique. Nous avons tout de même voulu voir s'il s'agit d'une tendance universelle, ou si certaines entreprises s'en sortent mieux, voire beaucoup mieux que d'autres.

Pour cela, nous avons noté leurs réponses aux questions concernant les métriques :

Guide des scores

- Très faible -2
- Faible -1
- Neutre 0
- Haut +1
- Très haut +2

Nous avons ensuite ajouté trois scores individuels pour créer un score total pour chaque sondé. Et nous avons réparti les participants en trois niveaux :

Niveaux de confiance numérique des entreprises

- Niveau supérieur (scores situés dans le tiers haut)
- Niveau intermédiaire (scores situés dans le tiers médian)
- Niveau inférieur (scores situés dans le tiers bas)

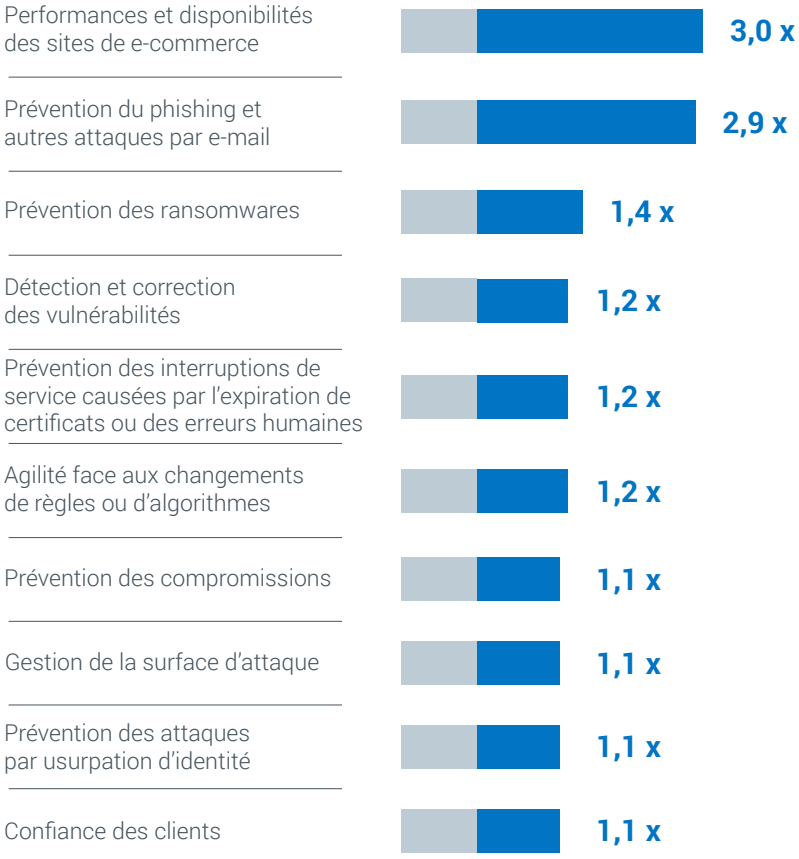
Cette hiérarchisation a révélé des différences considérables entre les entreprises les plus performantes (niveau supérieur) et les moins performantes (niveau inférieur).

Quels écarts ?

Il va de soi que les entreprises du niveau supérieur affichent de meilleures métriques de confiance numérique, puisque c'est sur ce critère que nous avons initialement réparti les participants. Mais ce qui est intéressant, c'est d'analyser les écarts de performances entre les entreprises du niveau supérieur et celles du niveau inférieur. Par exemple, trois fois plus d'entreprises du niveau supérieur déclarent obtenir de bons résultats en termes de performances et de disponibilité de leurs sites e-commerce. De même, elles sont 2,9 fois plus nombreuses à faire état d'une bonne prévention contre les attaques par phishing ou autres attaques par e-mail. Concrètement, elles affichent des résultats 10 % à 300 % meilleurs sur chaque métrique :

LES CLIENTS DES ENTREPRISES DU **NIVEAU SUPÉRIEUR** SONT BEAUCOUP PLUS NOMBREUX À LEUR FAIRE CONFIANCE QUE LES CLIENTS DES ENTREPRISES DU **NIVEAU INFÉRIEUR**.

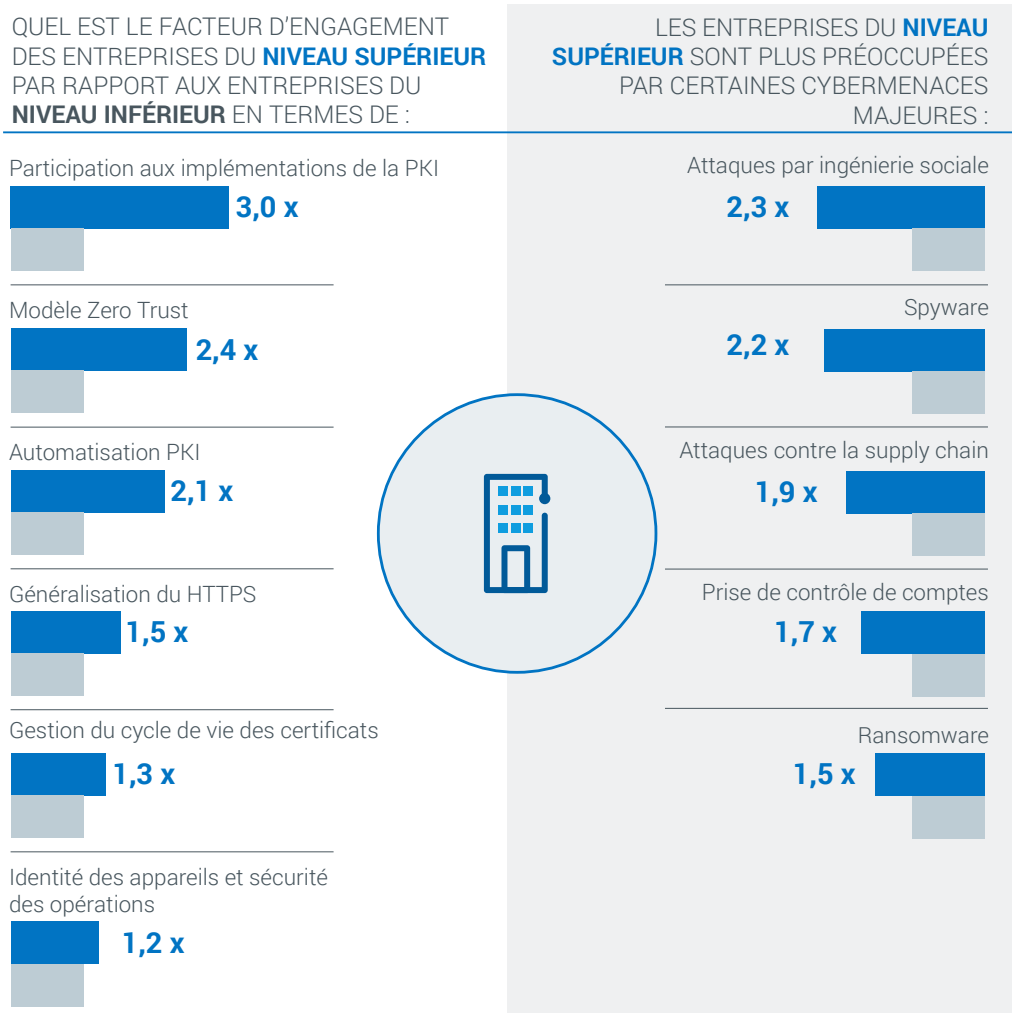
LES ENTREPRISES DE NIVEAU SUPÉRIEUR OBTIENNENT DE **BIEN MEILLEURS** RÉSULTATS QUE CELLES DE NIVEAU INFÉRIEUR EN TERMES DE CONFIANCE NUMÉRIQUE



Pourquoi les entreprises du niveau supérieur affichent-elles une telle avance ?

Les écarts importants observés en matière de confiance numérique s'expliquent par plusieurs différences entre les entreprises du niveau supérieur et celles du niveau inférieur :

- Attitudes : les entreprises du niveau supérieur sont 4,5 fois plus nombreuses à croire qu'une perte de confiance d'un client entraînera la perte de ce client. Elles sont également plus nombreuses à croire en l'influence de la confiance numérique sur leur marque, leurs ventes et leurs marges. Par ailleurs, elles sont 5,6 fois plus nombreuses à dire qu'elles rompraient toute relation avec un partenaire si elles perdaient confiance en ce dernier.
- Adoption précoce : les entreprises leaders sont plus avancées dans leur parcours vers la confiance numérique et termineront celui-ci beaucoup plus tôt que les retardataires.
- Préoccupation plus forte concernant les cybermenaces : les leaders prennent les cybermenaces beaucoup plus au sérieux. Ils sont ainsi 1,5 à 2,3 fois plus nombreuses à se dire préoccupées par les cybermenaces.
- Plus grand engagement dans les mesures de cyberprotection courantes : les entreprises du niveau supérieur sont jusqu'à trois fois plus nombreuses à appliquer d'importantes mesures de sécurité.



À qui la responsabilité de la confiance numérique ?

Désigner le pôle en charge de la confiance numérique dans une entreprise est une décision importante. Sur cette question, les opinions divergent énormément entre les entreprises des niveaux supérieur et inférieur.

Pour la grande majorité des premières, le DSI devrait être la personne en charge de la confiance numérique. Les secondes estiment quant à elle que cette mission devrait être confiée aux opérations de sécurité (SecOps).

Le but de cette comparaison n'est pas de minorer le rôle de ces équipes SecOps, dont on connaît l'importance vitale, mais bien de montrer que la sphère d'influence des DSI s'étend à toute l'empreinte IT d'une organisation et de rappeler à quel point la confiance numérique est essentielle à la réussite des entreprises à dominante technologique. Ainsi, ces résultats ne font que refléter l'approche stratégique des entreprises du niveau supérieur sur la question de la confiance numérique.

LE POINT DE VUE DE DIGICERT

Leader et pionnier de la confiance numérique, DigiCert apporte aux entreprises et aux particuliers les outils qui leur permettront d'échanger et de communiquer de façon sereine et sécurisée dans l'univers du digital. Nous conseillons aux entreprises souhaitant emboîter le pas des acteurs du « Digital Trust Cognoscenti » d'envisager les cinq actions suivantes :

Faire de la confiance numérique un impératif stratégique. Ce point est l'un des facteurs qui différencient clairement les entreprises du niveau supérieur des autres. Celles-ci reconnaissent en effet l'impact de la confiance numérique sur des marqueurs importants comme l'image de marque, la fidélisation des clients, le chiffre d'affaires et les marges.

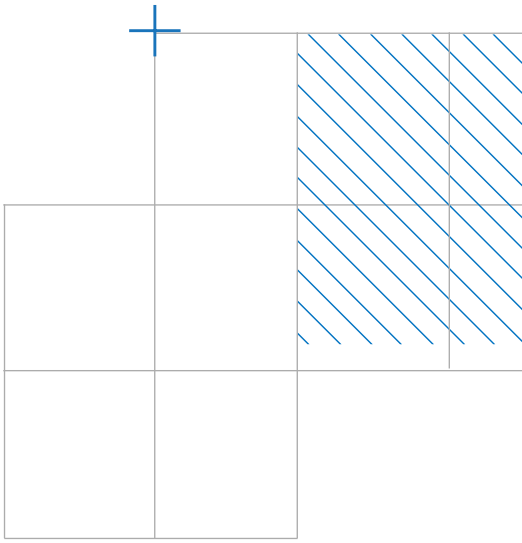
Mettre en place un Digital Trust Office dirigé par un responsable doté d'un pouvoir décisionnaire.

Reconnaître que vos utilisateurs, y compris les consommateurs, sont de plus en plus conscients des questions liées à la confiance numérique, et que le succès et la réputation de votre entreprise sont directement liés à votre capacité à garantir cette confiance.

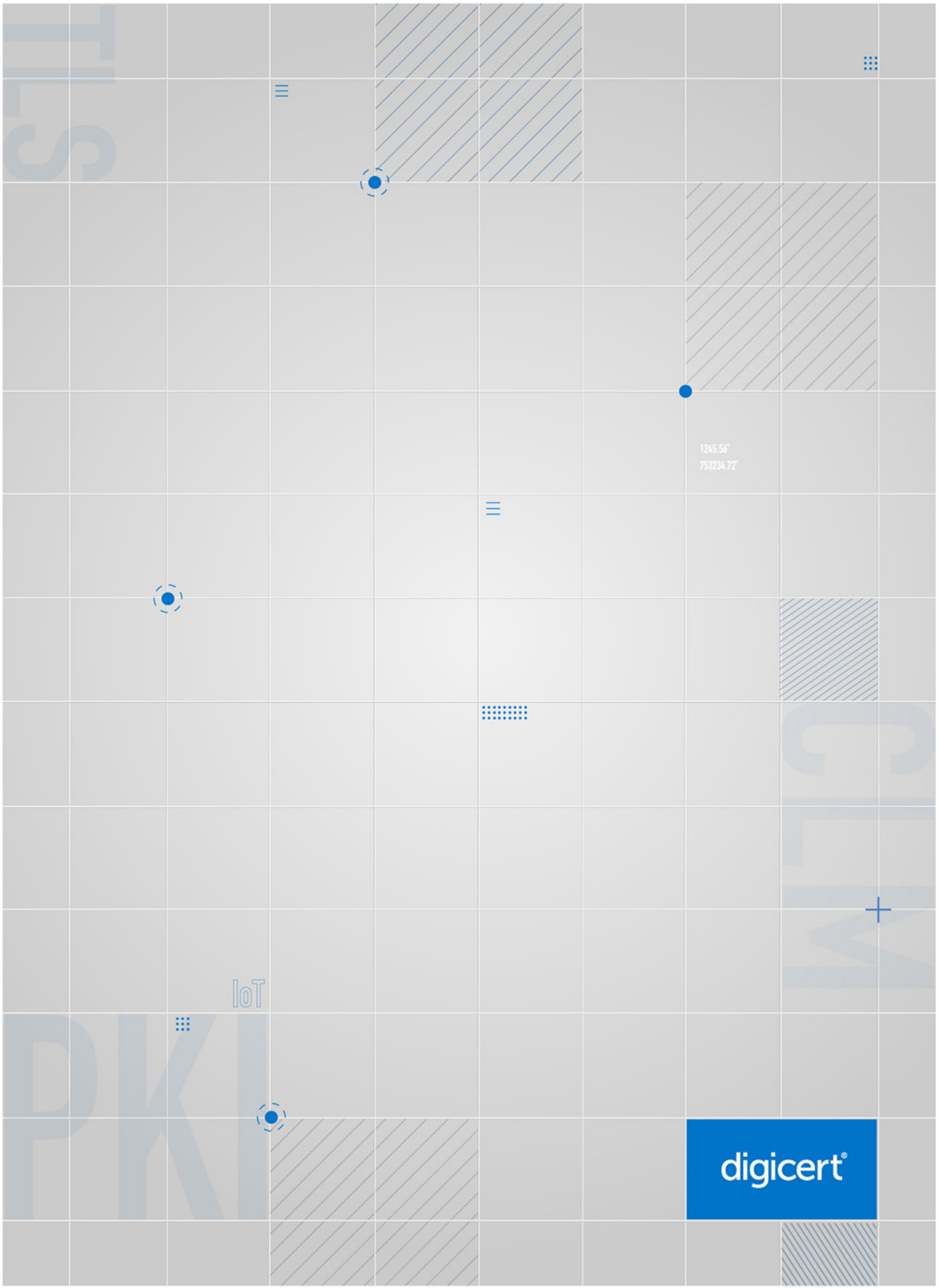
Vous faire accompagner par des experts dans votre parcours vers la confiance numérique. L'une des problématiques de confiance numérique citées par les entreprises est le manque d'expertise en interne. Assurez-vous que les partenaires que vous engagez disposent d'un portefeuille complet couvrant les piliers de la confiance numérique, sans oublier des solutions de gestion unifiée de la confiance couvrant l'ensemble de votre organisation.

Ne jamais oublier que vos clients prennent la confiance numérique très au sérieux. Communiquez avec eux de façon claire, en leur expliquant non seulement votre engagement dans le domaine de la confiance numérique, mais également les progrès réalisés à ce jour.

Cela rejoint une célèbre étude de Bain & Company[5] selon laquelle une hausse de 5 % du taux de fidélisation des clients augmenterait les bénéfices de 25 % à 95 %. Compte tenu de la propension des clients à se tourner vers la concurrence dès qu'ils perdent confiance en une entreprise, la confiance numérique s'impose d'elle-même comme un impératif absolu.



[5]Prescription for Cutting Costs – Bain & Company


TLS
1245.56
753234.72
IoT
PKI
digicert®