

Livre blanc

L'avenir de la vérification d'identité dans le monde

Comment les grandes entreprises
concilient sécurité numérique et
expérience utilisateur

Alors que les cas d'usurpation d'identité se multiplient, les entreprises du monde entier cherchent de nouveaux moyens de vérifier et d'authentifier l'identité de leurs clients. Les solutions de vérification d'identité (IDV) et d'authentification apportent ce niveau de sécurité essentiel. Une meilleure compréhension du déploiement de ces solutions par les grandes organisations et une prise de conscience des zones les plus vulnérables du parcours client permettent aux entreprises de mieux se protéger contre des risques croissants.

DocuSign, qui a lancé Intelligent Agreement Management, et Onfido, une société du groupe Entrust, ont corédigé ce rapport afin de comprendre l'état de l'usurpation d'identité dans le monde et le rôle que joue l'IDV pour y faire face. Le rapport met en exergue les étapes du parcours client où se produisent les usurpations d'identité et analyse la manière dont les équipes réagissent à cette menace croissante. Il liste également les défis rencontrés par les organisations au niveau régional et sectoriel.

Principales conclusions

1 Les incidents d'usurpation d'identité sont en augmentation, ce qui coûte du temps, de l'argent et des ressources humaines aux entreprises.

Globalement, une part importante des entreprises interrogées perdent plus de 900 000 euros chaque année en coûts directs et indirects liés à l'usurpation d'identité, des dépenses qui devraient augmenter avec les progrès de l'intelligence artificielle (IA). Malgré ces enjeux, certaines entreprises hésitent à mettre en place des mesures de prévention, de peur qu'elles ne nuisent à l'expérience client. En France, 56% estiment que l'expérience client et la prévention de l'usurpation d'identité sont des priorités concurrentes. Pourtant, dans la pratique, de nombreuses entreprises du monde entier constatent qu'elles n'ont pas à faire de compromis : selon notre enquête, celles qui utilisent l'IDV sont deux fois plus satisfaites que celles qui ne l'utilisent pas.

2 L'usurpation d'identité se produit tout au long du parcours client, mais le plus souvent lorsque les clients se connectent et autorisent des paiements.

Néanmoins, elle ne se limite pas au parcours client et se manifeste de bien des manières. Les formes les plus courantes, tous secteurs confondus, sont le vol d'identité, la création frauduleuse de comptes, la falsification de documents numériques et la fraude par rétrofacturation. La méthode d'authentification la plus souvent associée à l'usurpation d'identité reste le nom d'utilisateur et le mot de passe. Une analyse plus approfondie du comportement au sein des entreprises françaises révèle que 69% d'entre elles appliquent différents niveaux d'authentification pour chaque interaction avec les clients, en fonction soit du profil de risque de ces derniers, soit du type d'interaction.

3 En plus de constituer une ligne de défense très efficace contre l'usurpation d'identité, l'IDV peut représenter un avantage concurrentiel.

En effet, elle permet de détecter les fraudes plus tôt et plus fréquemment dans le parcours client. C'est ainsi que 28% des entreprises de l'Hexagone qui utilisent l'IDV ont économisé entre 900 000 et 4,5 millions d'euros. Au niveau international, 63% de celles qui ont investi davantage que leurs homologues dans ce domaine estiment que les mesures prises ont eu une incidence positive sur leur marque.

4 La plupart des entreprises considèrent la technologie comme la solution pour résoudre ou atténuer la fraude au client.

Quelque 70% des entreprises interrogées estiment qu'investir massivement dans des solutions technologiques est le meilleur moyen d'atténuer le risque financier lié à l'usurpation d'identité. L'IDV figure donc parmi leurs principales priorités, et 74% d'entre elles prévoient d'y investir davantage.

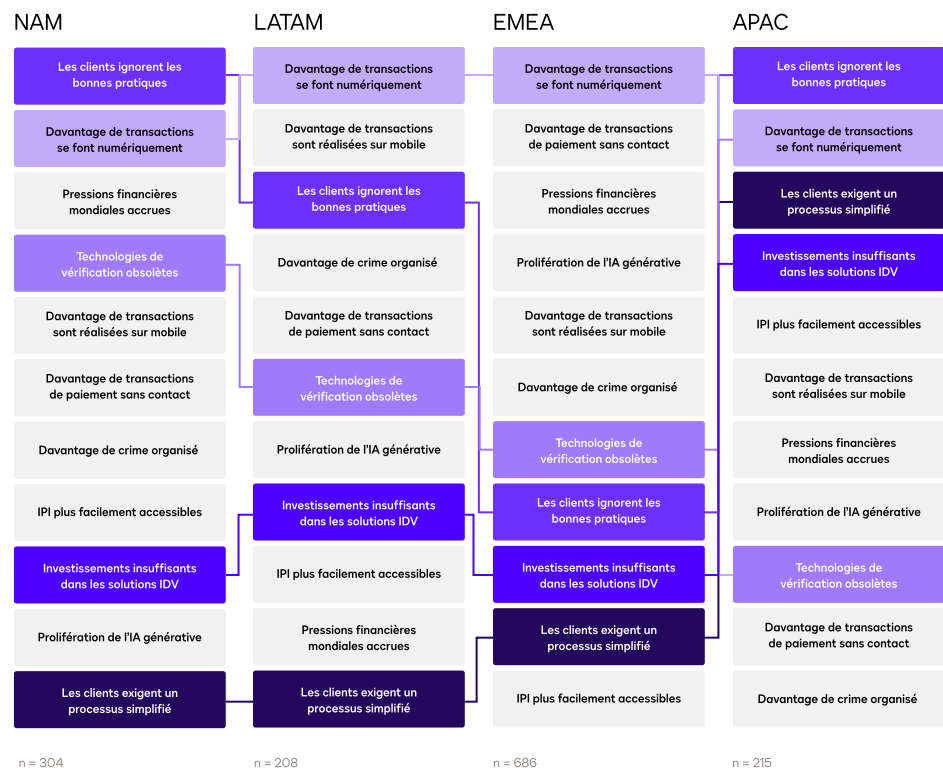
Les calculs ont été effectués en USD et convertis en monnaie locale le 21 mars 2025 à USD = EUR 0,924488.

L'usurpation d'identité est une préoccupation croissante, de même que les coûts élevés et les attentes croissantes des clients.

Parmi les entreprises interrogées, 69% s'accordent à dire que les tentatives d'usurpation d'identité sont en augmentation. Si la majorité des entreprises à travers le monde sont confrontées à ce défi, leurs opinions sur les causes de cette progression diffèrent selon les secteurs d'activité et les régions. Cependant, deux raisons ressortent de notre étude :

- Les transactions numériques sont aujourd'hui plus nombreuses.
- Les clients méconnaissent les bonnes pratiques à adopter pour protéger leurs identifiants de connexion et autres données sensibles.

Le manque de sensibilisation des clients aux bonnes pratiques et l'augmentation des transactions numériques sont les principales raisons de la hausse des tentatives de fraude

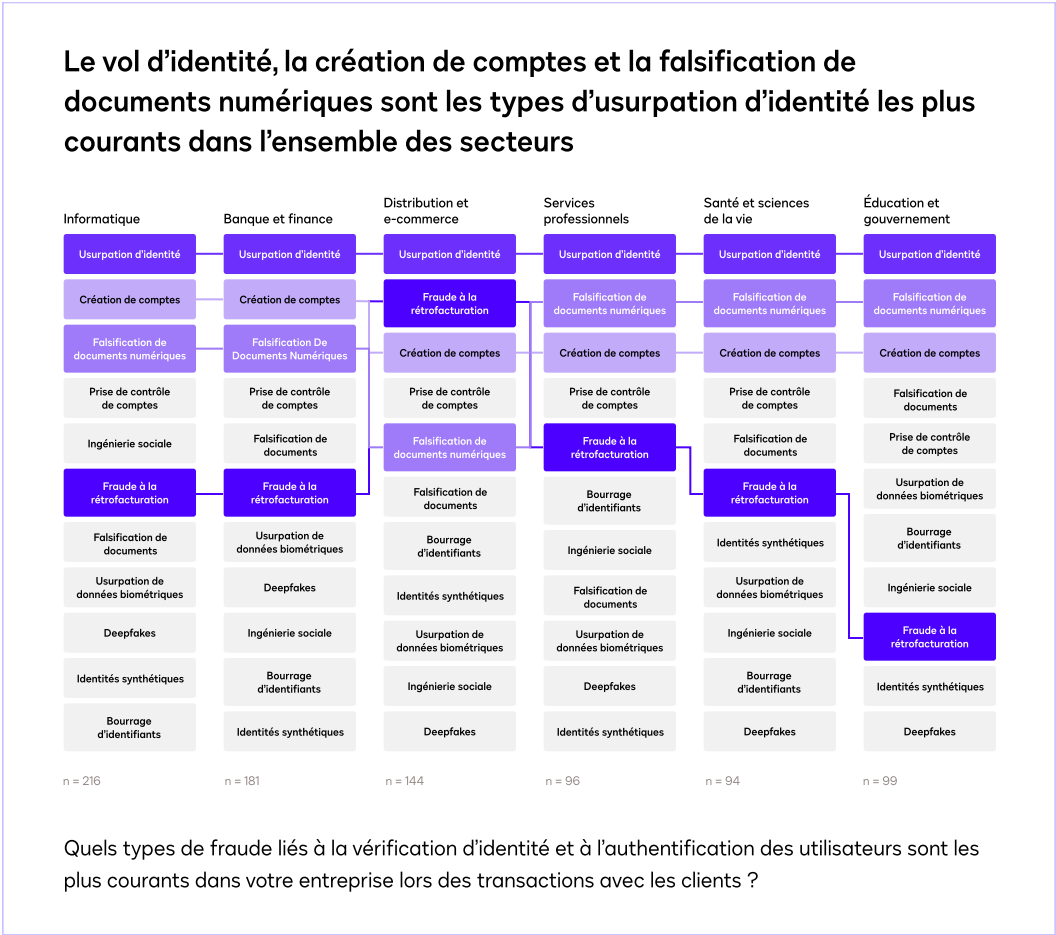


Selon vous, quelles sont les principales raisons de l'augmentation des tentatives de fraude ?

Bien que peu d'entreprises aient désigné l'IA comme l'un des principaux facteurs de fraude dans cette enquête, d'autres recherches indiquent qu'elle pourrait contribuer fortement à l'évolution du paysage de la sécurité. Le rapport Entrust 2025 sur l'usurpation d'identité révèle que la falsification de documents numériques, souvent réalisée à l'aide de l'IA générative, **a augmenté de 244% au cours de l'année écoulée**. Les « deepfakes » représentent désormais 40% des fraudes biométriques. Pourtant, de nombreuses entreprises considèrent l'IA comme un outil essentiel pour lutter contre l'usurpation d'identité : au niveau international, 82% des personnes interrogées estiment que l'IA générative sera plus efficace que leurs méthodes actuelles pour réduire le risque de fraude au client.

On observe également des tendances dans les différentes formes d'usurpation d'identité. Dans l'ensemble des secteurs français, le vol d'identité est le plus fréquemment signalé, suivi de la création frauduleuse de comptes et de la falsification de documents numériques. La distribution et l'e-commerce sont les seuls secteurs qui comptent un autre type de fraude dans leur top 3 : la fraude par rétrofacturation (lorsque des clients contestent intentionnellement une transaction pour obtenir un remboursement tout en conservant le produit ou le service). Cela s'explique par la place prépondérante qu'occupent les achats effectués par les consommateurs dans ces secteurs.

Ces résultats montrent que la plupart des usurpations d'identité se produisent à des moments critiques, lorsque les clients interagissent activement avec une entreprise, que ce soit pour créer un compte pour la première fois, réinitialiser leur mot de passe ou saisir des informations de paiement. Afin de protéger ces étapes critiques du parcours client, les entreprises doivent proposer des moyens permettant d'ouvrir des comptes en toute sécurité et de vérifier en permanence l'identité des utilisateurs tout au long du cycle de vie client.



Résultats par région

Pourcentage d'entreprises dont les coûts directs de l'usurpation d'identité dépassent 900 000 euros

Pays affichant le pourcentage le plus élevé

- 55% Allemagne
- 65% Australie

Pays affichant le pourcentage le plus faible

- 30% Royaume-Uni
- 29% Brésil

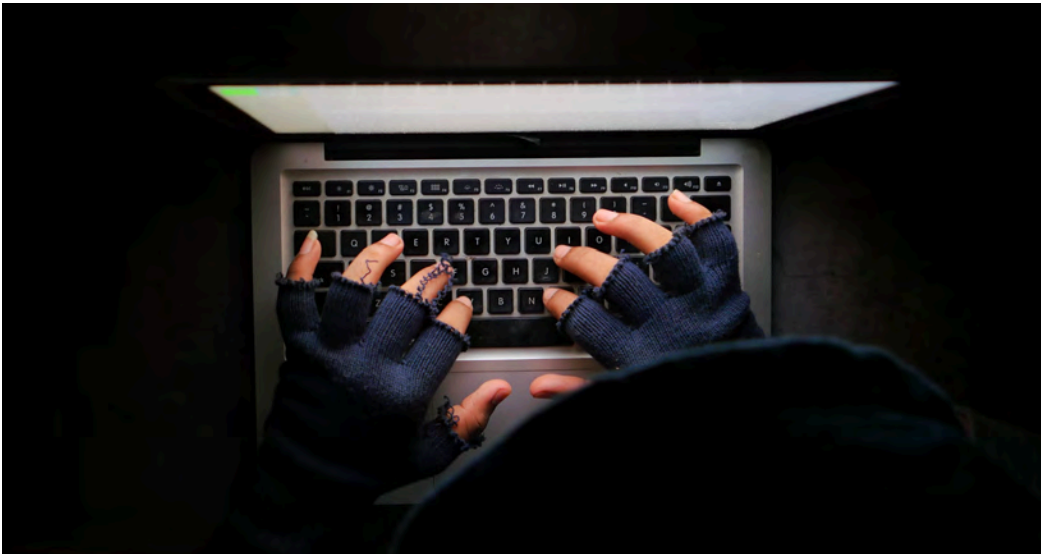
Pourcentage d'entreprises dont les coûts indirects de l'usurpation d'identité dépassent 900 000 euros

Pays affichant le pourcentage le plus élevé

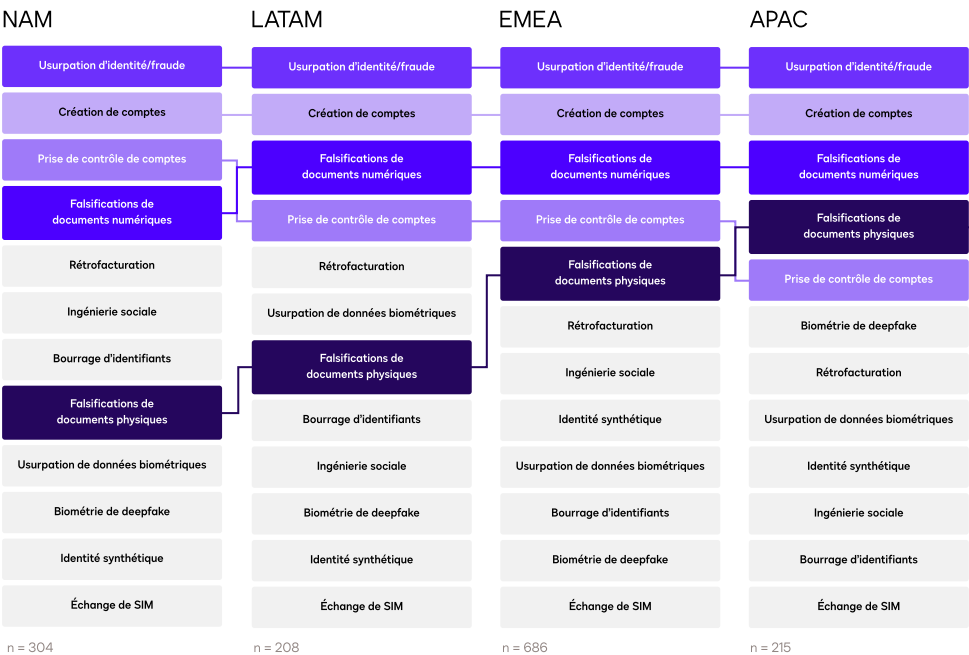
- 24% Brésil
- 29% Australie

Pays affichant le pourcentage le plus faible

- 6% Mexique



Le vol d'identité, la création de comptes et la falsification de documents numériques sont les types d'usurpation d'identité les plus courants dans la zone EMEA



Quels types de fraude liés à la vérification d'identité et à l'authentification des utilisateurs sont les plus courants dans votre entreprise lors des transactions avec les clients ? Veuillez sélectionner jusqu'à trois types de fraude qui se produisent régulièrement en cliquant dessus et en commençant par le plus fréquent.

Résultats par secteur

C'est dans le secteur de la banque et de la finance que les coûts directs liés à l'usurpation d'identité sont les plus élevés (51% ont déclaré des coûts directs annuels supérieurs à 900 000 euros).

C'est dans le secteur des services professionnels que les coûts indirects liés à l'usurpation d'identité sont les plus élevés (20% ont déclaré des coûts indirects annuels supérieurs à 900 000 euros).

L'usurpation d'identité coûte en moyenne plus de 6 millions d'euros par an aux entreprises

De nombreuses entreprises du monde entier estiment que les coûts associés à l'usurpation d'identité sont simplement le prix à payer pour exercer leur activité, mais ce prix ne cesse d'augmenter. Certaines d'entre elles doivent régulièrement faire face à des dépenses supérieures à sept chiffres en raison des coûts directs liés aux rétrofacturations, aux remboursements et autres pertes financières. S'ajoutent à cela les coûts indirects des ressources humaines affectées à l'identification et à la régularisation des transactions frauduleuses, ou à la réparation des dommages réputationnels. Notre étude révèle que :

41%

des entreprises enregistrent un coût annuel direct lié à l'usurpation d'identité supérieur à 900 000 euros.

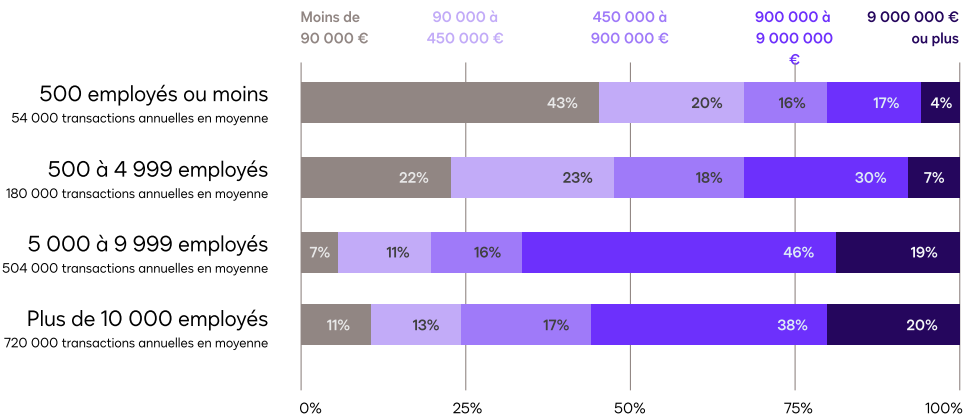
15%

des entreprises enregistrent un coût annuel indirect lié à l'usurpation d'identité supérieur à 900 000 euros.

Les grandes entreprises, qui gèrent davantage de clients, de données et de chiffre d'affaires, supportent des coûts encore plus élevés.

- Parmi les entreprises de plus de 5 000 salariés le coût annuel direct moyen de l'usurpation d'identité est de 12 millions d'euros. 28% enregistrent un coût annuel indirect lié à l'usurpation d'identité supérieur à 900 000 euros.
- Ces coûts s'accroissent de manière exponentielle à mesure que la taille des entreprises augmente. Parmi celles qui comptent plus de 10 000 employés, 20% affichent des coûts annuels (directs ou indirects) liés à l'usurpation d'identité supérieurs à 46 millions d'euros.

Les grandes entreprises enregistrent des coûts directs liés à l'usurpation d'identité plus élevés



À combien estimeriez-vous le coût financier annuel direct de l'usurpation d'identité pour votre entreprise ? Par coût financier direct, nous entendons le montant d'argent perdu pour cause de fraude, sans tenir compte des éventuelles indemnités versées par les assurances.

Au niveau sectoriel, la banque et la finance sont confrontées aux coûts directs les plus élevés. En effet, les fraudeurs créent de faux comptes au début du parcours client, ce qui leur permet d'accéder à des services monétaires ou à des comptes légitimes à un stade ultérieur et de vider ces comptes de leurs fonds. Dans les deux cas, l'entreprise ciblée perd directement de l'argent ou doit rembourser le véritable client.

Le secteur des services professionnels enregistre les coûts indirects les plus élevés. L'usurpation d'identité porte davantage atteinte à la réputation de la marque et à la confiance des clients, ce qui entraîne une baisse des revenus futurs et des coûts indirects substantiels.

56%

des entreprises françaises interrogées estiment que l'expérience client et la prévention de l'usurpation d'identité sont des priorités concurrentes.

45%

des entreprises mondiales interrogées privilégient l'expérience client plutôt que la prévention de la fraude.

56%

des entreprises françaises interrogées craignent de contrarier les clients et d'augmenter les taux d'abandon si elles renforcent la prévention de l'usurpation d'identité.

Résultats par région

La région EMEA est moins préoccupée par les frictions entre l'expérience client et la prévention de l'usurpation d'identité,

47%

des entreprises s'accordant à dire qu'elles n'ont pas de difficultés à trouver le juste équilibre.

Les clients s'attendent de plus en plus à des expériences harmonieuses.

79% des entreprises interrogées à l'échelle mondiale s'accordent à dire que l'expérience client est très importante pour leur réussite.

Les entreprises doivent offrir des expériences numériques simples, pratiques et compétitives tout en assurant la sécurité des informations client. Par exemple, de nombreux clients s'attendent à des expériences personnalisées, à des transactions adaptées aux appareils mobiles et à des formulaires préremplis avec les informations qu'ils ont déjà fournies, tout en supposant que leurs données seront protégées tout au long de ces interactions. Or, de nombreuses entreprises ont du mal à concilier ces objectifs.

Cependant, les approches visant à trouver un équilibre entre prévention de l'usurpation d'identité et expérience client varient selon les régions, les secteurs d'activité et les générations. Les secteurs des technologies de l'information ainsi que de la banque et de la finance sont plus susceptibles de soumettre leurs clients à des mesures d'authentification rigoureuses en vue de protéger les données confidentielles et les transactions à forte valeur, même lorsque ces mesures créent davantage de frictions.

Les décideurs issus des générations Y et Z, qui sont plus habitués aux contrôles de vérification d'identité numériques, attendent que les transactions numériques offrent un niveau exceptionnel d'expérience utilisateur et de sécurité, ce qui les pousse à innover en matière de technologie.

Dans l'ensemble, les entreprises qui utilisent l'IDV sont deux fois plus satisfaites que celles qui n'y ont pas recours et ont tendance à trouver leurs méthodes de prévention de la fraude nettement plus efficaces.

Point à retenir

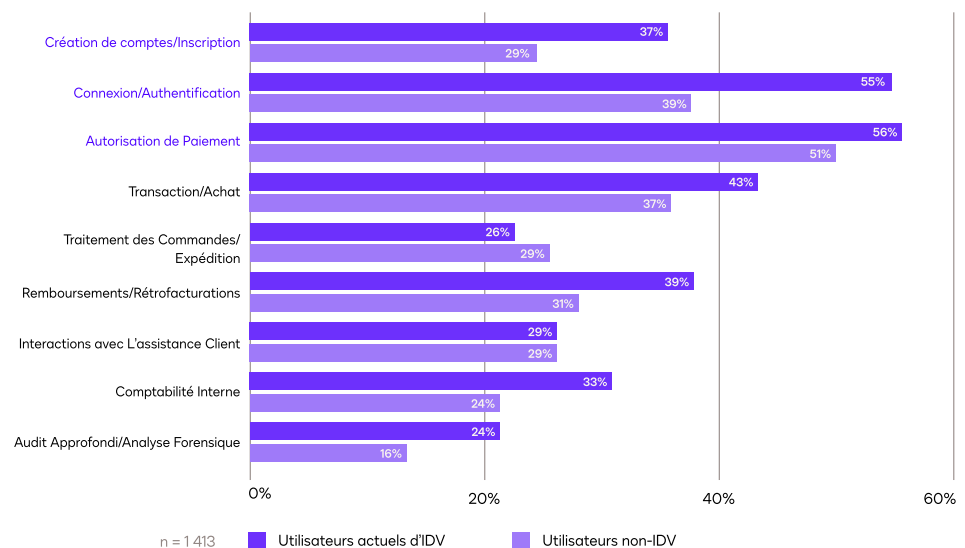
Faire face à l'augmentation des tentatives d'usurpation d'identité tout en offrant une expérience harmonieuse est un défi croissant que l'IDV relève. Les entreprises qui utilisent des technologies obsolètes ou insuffisantes pour atténuer ce risque auront du mal à se défendre contre les fraudes les plus sophistiquées et à suivre le rythme de menaces constamment mises à jour.

L'usurpation d'identité se produit tout au long du parcours client

L'usurpation d'identité se produit tout au long du parcours client, mais les entreprises la détectent le plus souvent aux premières étapes de la connexion et de l'autorisation des paiements.

Les entreprises qui utilisent l'IDV sont encore plus susceptibles d'être informées des tentatives d'usurpation d'identité dès le début des transactions, ce qui améliore leurs chances de prévenir ou d'atténuer les dommages.

Les utilisateurs de l'IDV sont plus susceptibles que les autres de détecter la fraude aux premières étapes du parcours client



À quel moment du processus de transaction votre entreprise apprend-elle généralement qu'une transaction frauduleuse a eu lieu ? Les options énumérées ci-dessous sont classées par ordre décroissant, des premiers échanges avec le client au processus postérieur à l'engagement client.

Lorsqu'on leur a demandé quels outils d'authentification étaient les plus associés à l'usurpation d'identité, les entreprises ont désigné **l'authentification par nom d'utilisateur et mot de passe en tant que méthode la plus faible**. Cela peut s'expliquer par le fait que les noms d'utilisateur et les mots de passe sont facilement compromis, sujets aux violations de données et ne reposent pas sur une authentification multifacteur (AMF). En 2024, les identifiants volés, tels que le nom d'utilisateur et le mot de passe, ont été la source la plus courante d'incidents de violation de données¹.

¹ « 2024 Data Breach Investigations Report », Verizon Business.



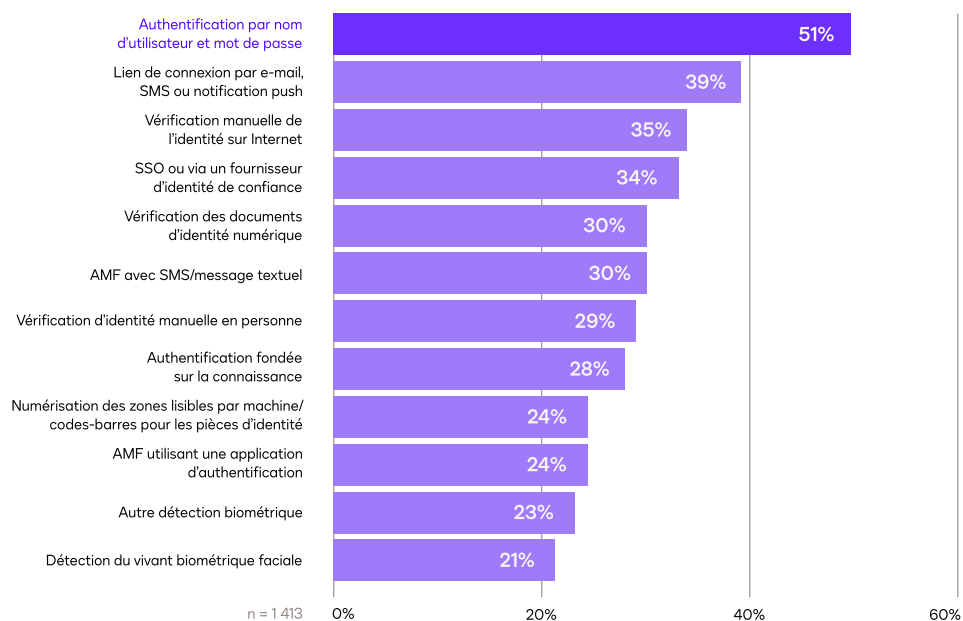
Les entreprises qui utilisent l'IDV détectent en moyenne les tentatives d'usurpation d'identité dans

20%

d'étapes supplémentaires du parcours client que les autres.

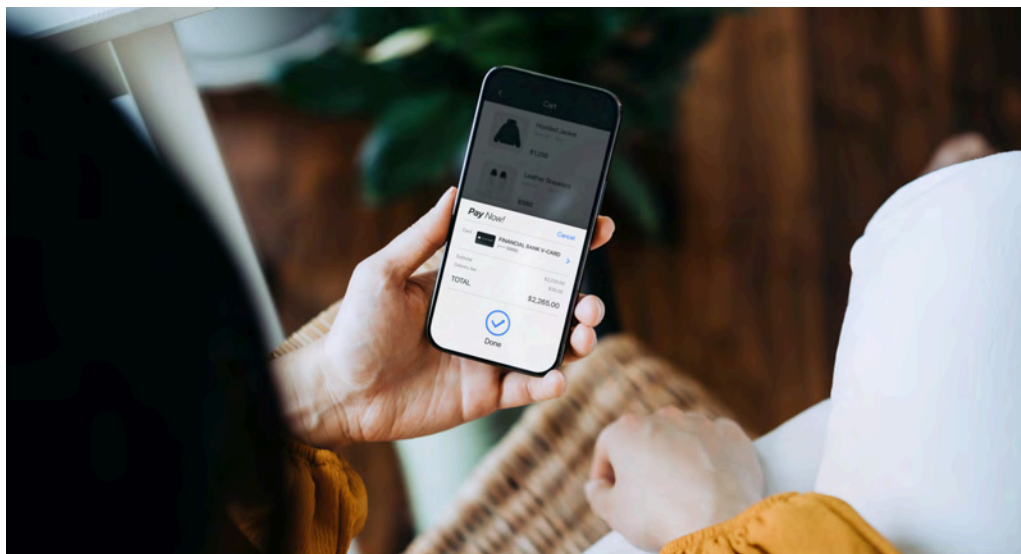
L'usurpation d'identité se produit le plus souvent lorsque le nom d'utilisateur et le mot de passe sont la seule méthode d'authentification

La fraude à l'identité est plus fréquente avec cette technique

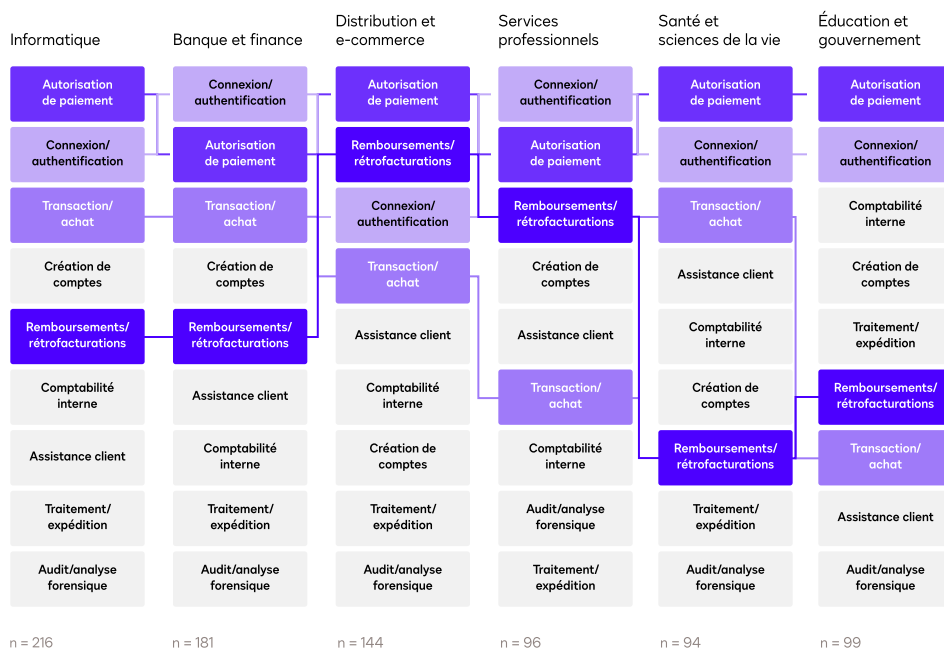


Pour chacun des types d'authentification utilisateur, veuillez indiquer la fréquence à laquelle vous constatez des fraudes par rapport aux autres types d'authentification.

L'enquête révèle également que plus une entreprise traite de transactions numériques, plus elle est susceptible de détecter des fraudes pour diverses méthodes d'authentification.



L'autorisation des paiements et la connexion sont les étapes les plus courantes pour détecter les fraudes dans tous les secteurs

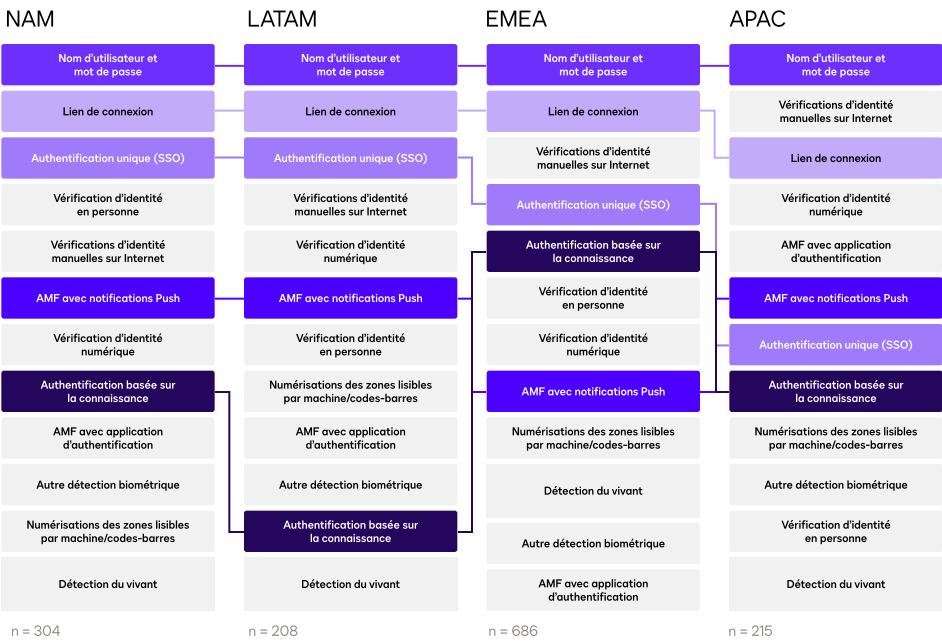


À quels moments du processus de transaction votre entreprise apprend-elle qu'une transaction frauduleuse a eu lieu ?

Résultats par génération

Parmi les décisionnaires informatiques et opérationnels, les cadres dirigeants issus des générations Y et Z sont plus enclins à utiliser l'IDV que les baby-boomers ou ceux issus de la génération X. Ils sont également plus susceptibles de qualifier de « très bonne » l'approche de leur entreprise en matière de lutte contre la fraude.

L'authentification par nom d'utilisateur et mot de passe est la méthode associée au plus grand nombre de fraudes dans toutes les régions



La fraude est beaucoup plus fréquente que la moyenne avec cette technique.

Point à retenir

L'authentification par nom d'utilisateur et mot de passe est la méthode la plus vulnérable, mais même l'AMF n'est pas suffisante pour se protéger contre les tentatives d'usurpation d'identité de plus en plus complexes. Les formes avancées d'IDV telles que l'authentification biométrique et la vérification de documents sont essentielles pour garder une longueur d'avance sur les fraudeurs.

Investir largement dans l'IDV donne des résultats concrets

28% des entreprises de l'Hexagone ont économisé

**entre
900 000
euros et 4,5
millions d'euros**

au total en prévenant la fraude grâce à une solution d'IDV.

Les données montrent que l'IDV est un investissement rentable. En mettant en œuvre une solution de ce type, 52% de l'ensemble des entreprises ont économisé plus de 900 000 euros au total.

Cependant, le déploiement d'une solution d'IDV n'est que la première étape. Les entreprises qui obtiennent les meilleurs résultats accordent une attention particulière à leur sécurité en investissant beaucoup plus que leurs homologues dans l'IDV. En outre, celles qui investissent davantage sont moins attrayantes pour les fraudeurs, ce qui leur confère un avantage concurrentiel.

Les entreprises qui déclarent investir beaucoup plus que leurs homologues dans l'IDV :

Économisent davantage

1,5 fois

plus susceptibles d'avoir économisé plus de 900 000 euros au total par rapport à leurs pairs.

2,2 fois

plus susceptibles d'avoir économisé plus de 900 000 euros au total par rapport à leurs pairs.

Réduisent le nombre de fraudes à l'identité

1,7 fois

plus susceptibles d'avoir réussi à réduire considérablement le nombre de fraudes à l'identité.

Continuent d'investir dans l'IDV

2,8 fois

plus susceptibles de prévoir d'investir davantage dans l'IDV.

Présentent une plus grande satisfaction interne et client

4 fois

plus susceptibles d'être très satisfaites des solutions d'IDV qu'elles utilisent.

1,6 fois

plus susceptibles d'observer une incidence positive sur leur marque.

Sont plus compétitives

2,7 fois

plus susceptibles d'estimer qu'elles disposent d'un avantage concurrentiel.

Les données indiquent que les clients font davantage confiance aux entreprises qui font tout leur possible pour protéger leurs données personnelles.

77%

des entreprises qui ont investi davantage que leurs homologues dans les technologies de vérification d'identité ont

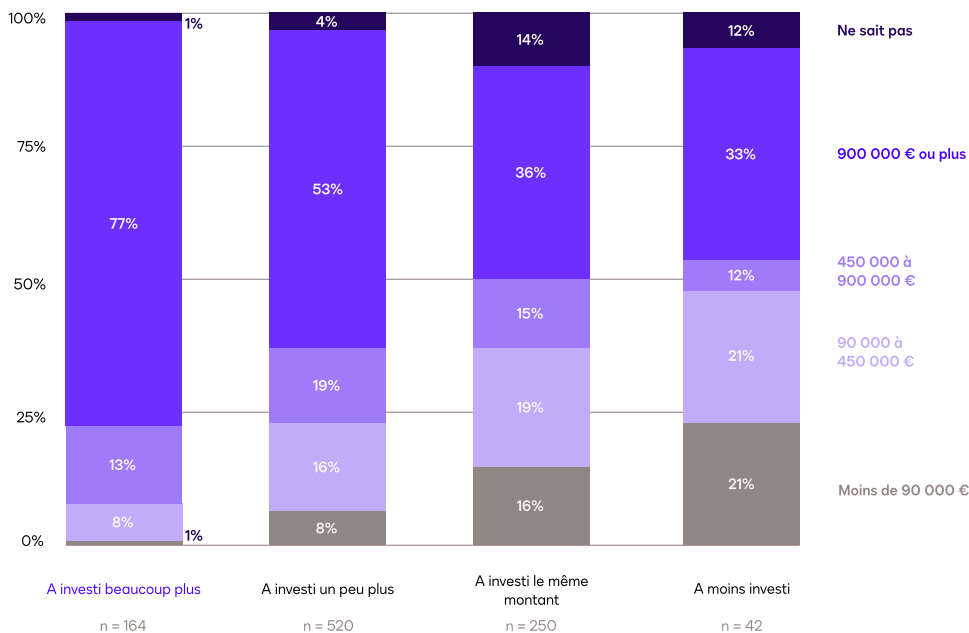
économisé plus de 900 000 euros

au total, contre 36% de celles ayant investi au même niveau que leurs homologues.



Les entreprises qui ont investi beaucoup plus que leurs homologues dans l'IDV étaient plus susceptibles d'économiser 900 000 euros ou plus au total

Économies réalisées avec les solutions IDV actuelles



À combien estimeriez-vous le montant total des économies réalisées par votre entreprise grâce à la prévention de la fraude au client et l'utilisation de vos solutions actuelles de vérification d'identité et d'authentification des utilisateurs ?

Les grandes entreprises investissent davantage dans l'IDV et génèrent un retour sur investissement (ROI) nettement plus élevé.

Pour les entreprises confrontées à un nombre considérable de fraudes à l'identité, investir dans l'IDV permet d'augmenter le ROI. Les données mondiales montrent que les grandes entreprises qui subissent des coûts d'usurpation d'identité plus élevés, ont tendance à investir beaucoup plus dans les solutions d'IDV que leurs homologues et à obtenir un ROI nettement plus élevé.

78%

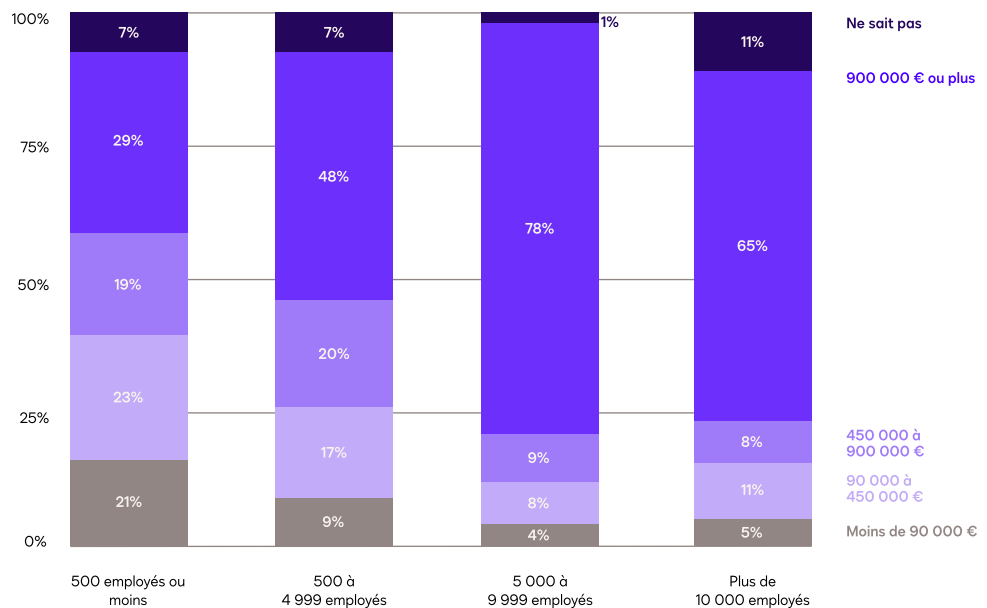
des entreprises de 5 000 à 9 999 employés ont économisé au total 900 000 euros ou plus grâce à l'IDV.

65%

des entreprises de plus de 10 000 employés ont économisé au total 900 000 euros ou plus grâce à l'IDV.

Les grandes entreprises réalisent davantage d'économies grâce aux solutions d'IDV

Économies réalisées avec les solutions IDV actuelles

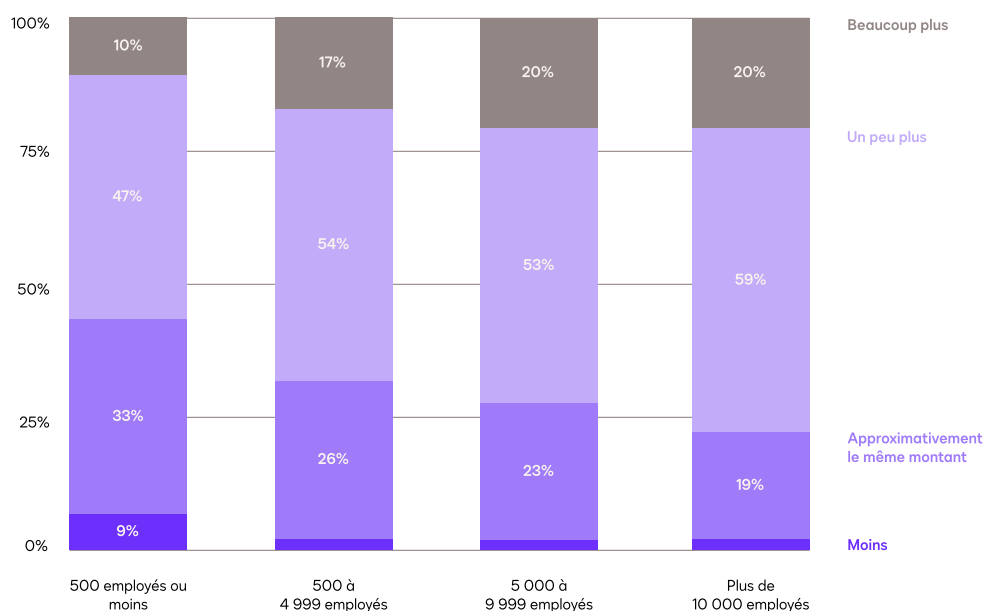


Parmi les propositions suivantes, laquelle décrit le mieux l'investissement actuel de votre entreprise dans les solutions ou les méthodes de vérification d'identité et d'authentification des utilisateurs ?



Les grandes entreprises investissent beaucoup plus que leurs homologues dans l'IDV

Comparaison des investissements d'IDV par rapport aux pairs du secteur



À combien estimeriez-vous le montant total des économies réalisées par votre entreprise grâce à la prévention de la fraude au client et l'utilisation de vos solutions actuelles de vérification d'identité et d'authentification des utilisateurs ?

Point à retenir

Les entreprises qui investissent massivement dans l'IDV en retirent de nombreux avantages, notamment des économies plus importantes, une diminution des cas d'usurpation d'identité, une meilleure perception de la marque, une amélioration de l'expérience client et un avantage sur la concurrence.

Les grandes entreprises se tournent vers la technologie pour lutter contre la fraude.

70%

estiment que le meilleur moyen d'atténuer le risque financier de l'usurpation d'identité est d'investir massivement dans la technologie.

On observe de grandes disparités dans la confiance des entreprises en leur capacité à gérer l'usurpation d'identité. Un peu plus de la moitié (53%) pense pouvoir atténuer la fraude, mais ne jamais la résoudre complètement, tandis que 40% estiment pouvoir la résoudre complètement avec la bonne technologie. Les grandes entreprises de plus de 10 000 employés ont tendance à privilégier une approche d'atténuation.

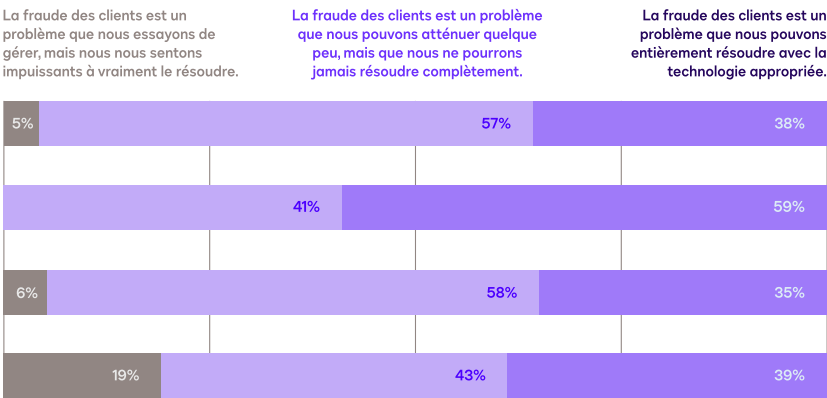
Si les perceptions diffèrent sur la question elle-même, la plupart des entreprises s'accordent sur une solution :

Cet intérêt pour l'investissement technologique éclipse d'autres approches, telles que l'investissement dans le personnel et les talents (18%) et l'investissement dans l'assurance contre la criminalité en vue de compenser les coûts de la fraude (11%), des options réactives qui cherchent à réparer les dommages plutôt qu'à se défendre proactivement contre les menaces.

Résultats par génération

Les dirigeants d'entreprise issus des générations Y et Z ont plus tendance à croire que la fraude peut être complètement résolue grâce à la bonne technologie que ceux de la génération X ou des baby-boomers.

Les entreprises d'Amérique latine sont les plus optimistes quant à la résolution complète de la fraude



Avec laquelle des propositions suivantes seriez-vous le plus d'accord ?

L'outil d'IDV le plus populaire est l'authentification multifacteur

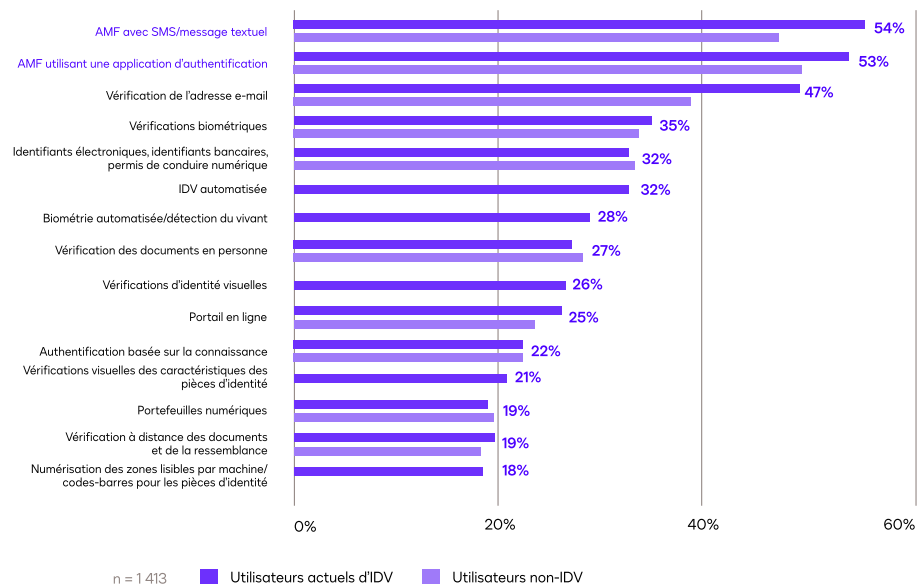
Les entreprises utilisent les outils d'IDV à différents moments du parcours client, mais le plus souvent lors de l'authentification par nom d'utilisateur et mot de passe, étape où elles signalent le plus de fraudes.

L'authentification multifacteur est l'outil le plus couramment utilisé par les entreprises pour vérifier les identités et authentifier les utilisateurs, que ce soit par SMS ou par une application d'authentification.

La popularité de l'AMF ne doit rien au hasard : c'est l'une des plus anciennes méthodes d'identification numérique, et les clients y sont habitués, ce qui réduit les frictions tout en offrant une couche de sécurité essentielle.

L'AMF est l'outil de vérification d'identité et d'authentification le plus courant

Types d'IDV et d'authentification utilisateur actuellement utilisés



Parmi les types de vérification d'identité et d'authentification des utilisateurs suivants, lesquels votre entreprise utilise-t-elle actuellement ? Veuillez sélectionner toutes les réponses qui s'appliquent.

L'authentification multifacteur via une application ou par SMS plus couramment utilisée dans la zone EMEA



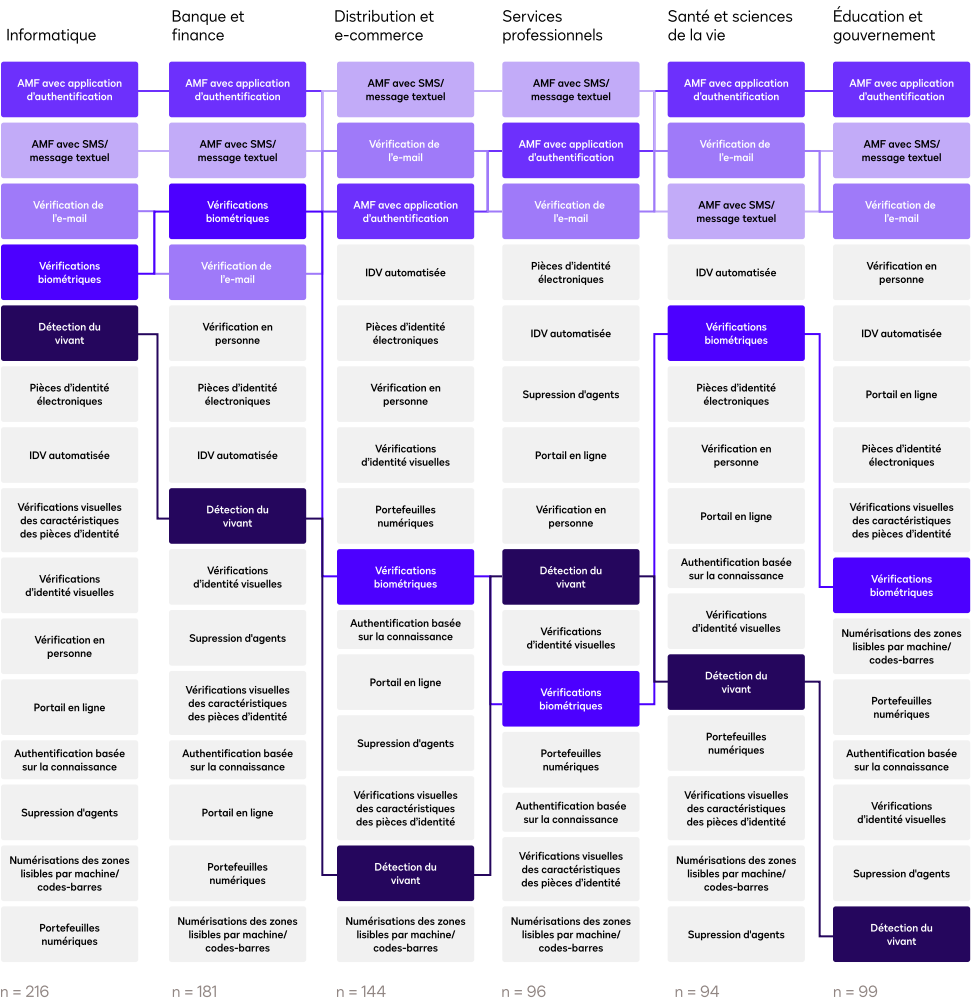
Parmi les types de vérification d'identité et d'authentification des utilisateurs suivants, lesquels votre entreprise utilise-t-elle actuellement ?

Les décisionnaires en France et en Allemagne adoptent les outils biométriques et la détection du vivant à un rythme plus lent que les décisionnaires au Royaume-Uni et dans d'autres régions.

Résultats sectoriels

Les dirigeants d'entreprise issus des générations Y et Z considèrent la biométrie comme un élément important de l'authentification en ligne. Selon une **étude d'IDEX Biometrics**, 47% d'entre eux ont utilisé des méthodes de sécurité biométriques au cours du mois dernier. Parmi ce groupe, 52% préfèrent l'authentification biométrique aux autres méthodes.

Les secteurs de la banque/finance et des technologies de l'information sont les plus susceptibles d'utiliser les contrôles biométriques

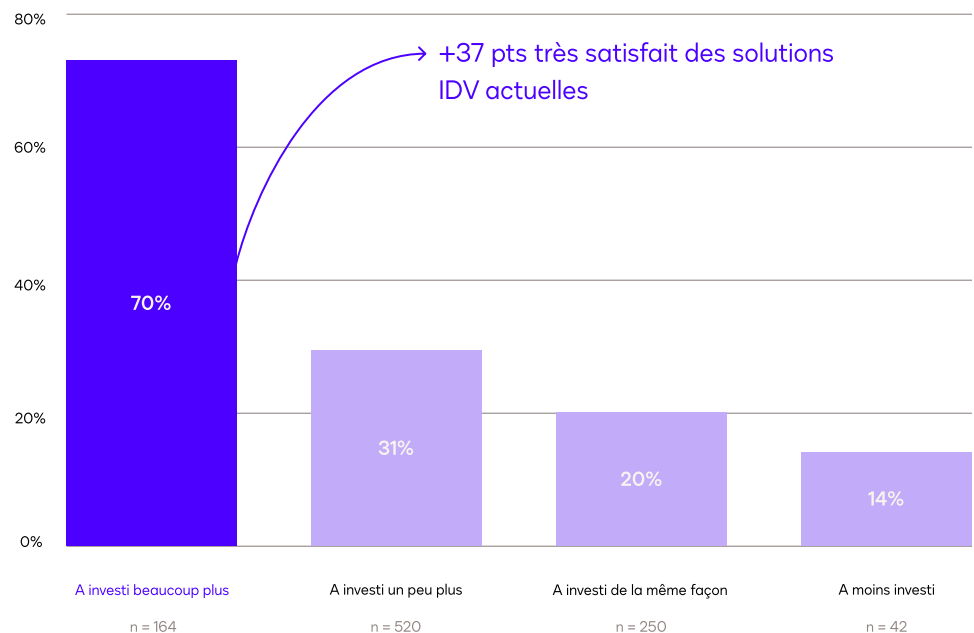


Parmi les types de vérification d'identité et d'authentification des utilisateurs suivants, lesquels votre entreprise utilise-t-elle actuellement ?

Les entreprises qui investissent davantage dans l'IDV se déclarent plus satisfaites des outils d'IDV.

Bien que l'AMF soit l'outil le plus courant, les entreprises qui investissent davantage se distinguent en mettant en œuvre des mesures supplémentaires. Par exemple, les grands investisseurs sont plus susceptibles de déployer des outils sophistiqués, tels que les contrôles biométriques et les fonctionnalités d'identification visuelle au point de connexion. Ces efforts supplémentaires sont corrélés à une plus grande satisfaction des clients à l'égard des solutions d'IDV.

Un investissement plus important dans l'IDV par rapport aux homologues est corrélé à une plus grande satisfaction



Quel est le degré de satisfaction de votre entreprise à l'égard de la solution de vérification d'identité et d'authentification des utilisateurs que vous utilisez actuellement ?

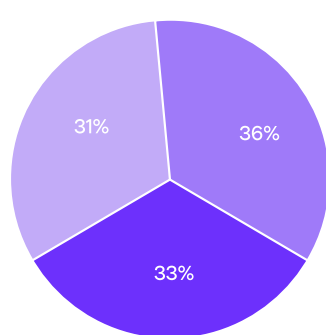
80%

des entreprises sont prêtes à soumettre leurs clients à des niveaux d'authentification élevés, même si cela augmente les frictions.

Les entreprises utilisent diverses méthodes pour déterminer le niveau d'authentification approprié pour chaque client.

Plus de deux entreprises sur trois utilisent actuellement des niveaux d'authentification dans leurs processus de sécurité. Autrement dit, elles peuvent mettre en place des moyens d'authentification supplémentaires pour les clients considérés à haut risque en raison de critères, tels que leur adresse IP, leur distance par rapport à l'expéditeur ou leur pays. Elles peuvent également mettre en œuvre d'autres mesures pour des types d'interactions précis avec les clients, tels que l'ouverture d'un nouveau compte ou l'accès aux finances.

La majorité des entreprises adaptent les niveaux d'authentification à chaque transaction en fonction du profil de risque ou du type de demande du client



Niveau d'authentification

- 36% Nous utilisons différents niveaux d'authentification selon le type d'interaction ou de demande que les clients effectuent
- 31% Nous utilisons différents niveaux d'authentification selon le profil de risque calculé du client
- 33% Nous gérons toutes les interactions liées aux questions d'identité numérique avec les clients en utilisant le même niveau d'authentification

Laquelle des affirmations suivantes décrit le mieux la manière dont votre organisation gère la prévention de la fraude ?

Les entreprises utilisent différents critères pour déterminer le niveau d'authentification approprié pour chaque interaction client, et 62% d'entre elles déclarent qu'il est difficile de choisir ce niveau. Elles se réfèrent le plus souvent à des politiques internes et aux profils de risque des clients, mais considèrent **la valeur des transactions et l'analyse coûts-avantages comme les critères les plus importants** pour évaluer le risque.

62%

des personnes disent qu'il est difficile de trouver le niveau approprié.

Résultats par région

La valeur estimée de la transaction est le critère le plus populaire pour déterminer les niveaux d'authentification en France (20%). Elle est également plus couramment utilisées en Allemagne (25%) qu'au Royaume-Uni (14%).

Résultats par secteur

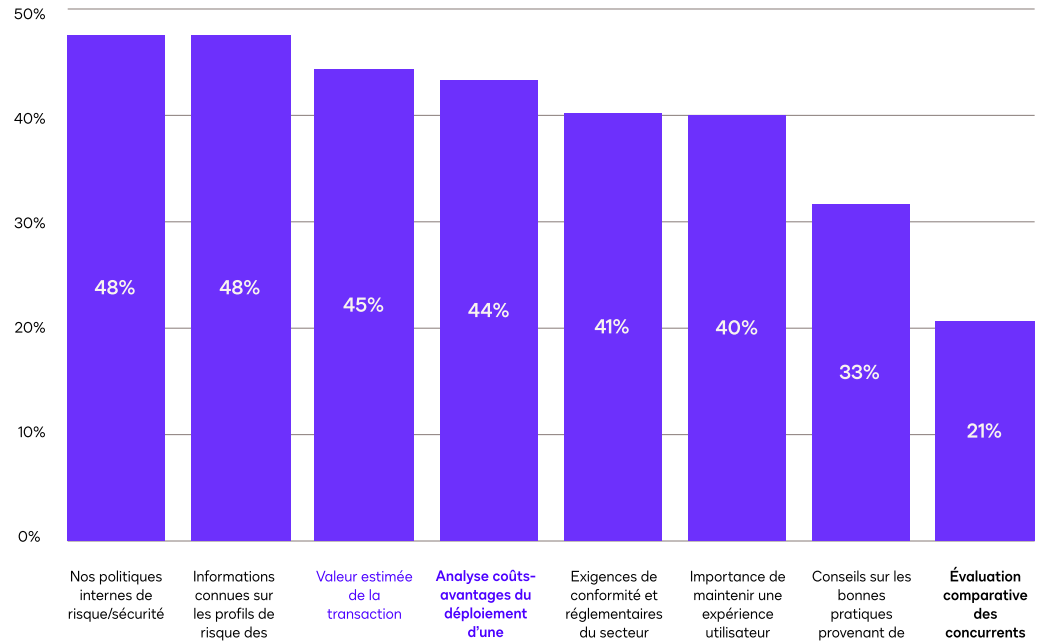
Les exigences réglementaires sont la méthode la plus populaire pour déterminer les niveaux d'authentification dans le secteur de la santé (29%). Elles sont également plus couramment utilisées dans l'immobilier (25%) et dans le secteur bancaire et financier (20%) que dans d'autres secteurs.

Les politiques internes et les profils de risque des clients sont les méthodes les plus courantes pour déterminer le niveau d'authentification

La valeur des transactions et l'analyse coûts-avantages sont considérées comme les critères les plus importants

Comment décidez-vous du niveau approprié ?

Méthodes les plus utilisées pour déterminer le niveau d'authentification



La valeur de la transaction (17%)
+
l'analyse coûts-avantages (19%)
sont les critères les plus importants.

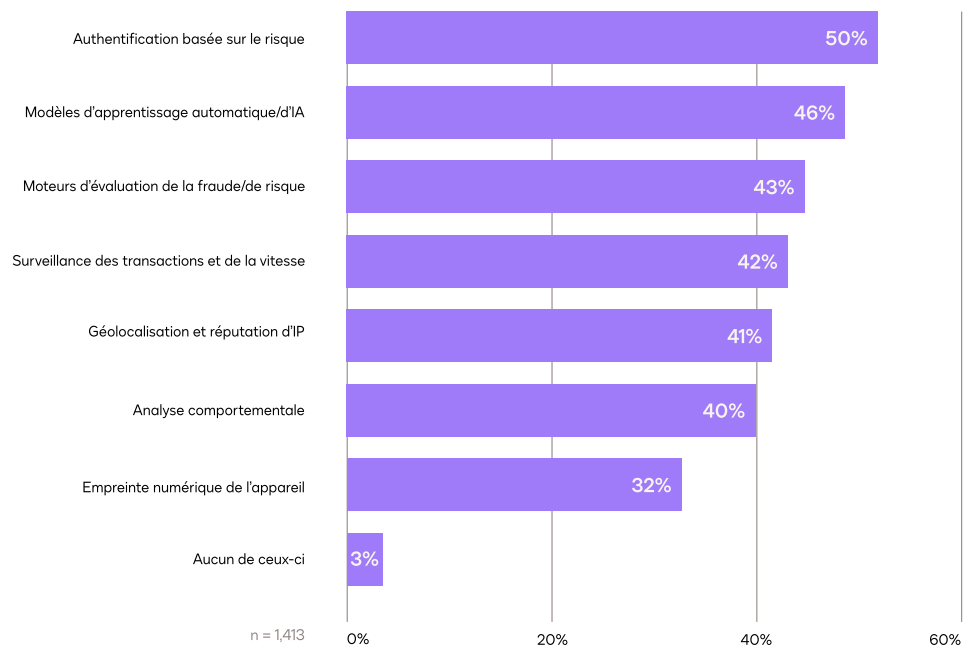
Sur quoi vous basez-vous pour établir le niveau d'authentification requis d'un utilisateur lors d'une interaction particulière ?

En plus de suivre diverses méthodes pour évaluer le risque lié aux clients, les entreprises utilisent une panoplie d'outils. Les plus populaires sont les outils d'authentification basés sur les risques, qui ajustent automatiquement le niveau de vérification d'identité pour chaque interaction en fonction du risque attribué au client. Un client à haut risque, par exemple, peut déclencher une vérification biométrique, tandis qu'un autre à faible risque peut ne faire l'objet que d'une AMF.



L'authentification basée sur les risques est l'outil le plus populaire pour évaluer le risque lié aux clients

Outils pour évaluer le risque d'authentification



Parmi les éléments suivants, lesquels votre entreprise utilise-t-elle pour évaluer le risque associé à une interaction particulière ?

78%

des entreprises
prévoient d'investir
davantage dans les
solutions d'IDV à
l'avenir.



Les entreprises prévoient d'investir continuellement dans l'IDV.

Le paysage de l'usurpation d'identité étant en pleine évolution, les entreprises continuent de se pencher sur les stratégies et les outils d'évaluation des risques et de prévention de la fraude. Quel que soit leur secteur d'activité, leur taille ou leur région, elles restent fermement convaincues que la technologie est la clé pour faire face à ce problème croissant.

Les décideurs s'intéressent particulièrement au rôle que joueront la biométrie et l'IA générative dans la lutte contre la fraude. En comparaison avec leurs méthodes actuelles d'authentification et de vérification des utilisateurs :

84%

des personnes interrogées
estiment que l'authentification
biométrique sera plus efficace
pour réduire le risque de fraude
au client.

82%

des personnes interrogées
estiment que l'IA générative
sera plus efficace pour
réduire le risque de fraude
au client.

78%

des personnes interrogées
estiment que l'évaluation
basée sur le risque sera plus
efficace pour réduire le risque
de fraude au client.

Parmi ces trois solutions, l'IA générative est considérée comme la plus attrayante pour les clients, mais de nombreux répondants craignent toujours une réaction négative. Alors que 51% des entreprises françaises, 47% des entreprises allemandes et 46% des entreprises britanniques s'accordent à dire que leurs clients seront frustrés ou mécontents si elles adoptent l'IA générative dans le cadre de leur processus d'IDV, 59% estiment au niveau mondial qu'elles connaîtront une augmentation significative de la fraude si elles ne l'adoptent pas.

Conclusion

Les entreprises du monde entier sont confrontées à l'émergence de nouveaux risques. L'essor de l'IA générative et l'adoption généralisée des transactions numériques, associés à la méconnaissance des bonnes pratiques de sécurité par les clients, ont créé un environnement propice à l'usurpation d'identité. Face à cette menace croissante, les plus grandes entreprises du monde investissent dans des outils de pointe, tels que la vérification d'identité pour se protéger.

Notre enquête a mis en évidence une conclusion majeure :
La technologie est essentielle pour détecter l'usurpation d'identité tout au long du parcours client et réduire les dépenses inutiles.

Avec l'IDV, les entreprises peuvent mettre en place des défenses efficaces pour protéger leur réputation et leurs résultats. Même dans des environnements d'affaires contraignants, investir dans l'IDV permet de réduire les risques et d'obtenir un retour sur investissement élevé à long terme. Les clients, quant à eux, ont l'esprit tranquille en sachant que leurs informations personnelles sont sécurisées alors qu'ils continuent de bénéficier d'une expérience numérique fluide.

Les coûts de l'usurpation d'identité ne feront qu'augmenter à mesure que l'IA progressera. Pour les entreprises qui cherchent à protéger leurs clients, à défendre leur réputation et à séduire les jeunes générations plus habituées aux outils de vérification d'identité numérique, il n'a jamais été aussi important d'adopter une attitude proactive et d'investir dans les technologies de lutte contre la fraude.

Principales recommandations

Réévaluez vos défenses anti-fraude.

Ce n'est pas pour rien que 74% des entreprises évaluent de nouvelles solutions au moins une fois par an. En effet, les fraudeurs apprennent et adoptent constamment de nouvelles techniques. Les entreprises doivent donc mettre à jour leurs défenses en conséquence. Le moyen le plus simple d'y parvenir est de rechercher des fournisseurs qui perfectionnent régulièrement leurs propres outils de défense contre les dernières tactiques et menaces, et de travailler en permanence avec ces prestataires.

Investissez dans la technologie basée sur l'IA.

Selon la majorité des décideurs interrogés, le meilleur moyen d'atténuer le risque financier lié à l'usurpation d'identité est d'investir massivement dans la technologie. Plutôt que de mobiliser de précieuses ressources sur des mesures réactives (comme l'assurance ou le recrutement intensif), investir dans des solutions d'IDV basées sur l'IA offre le meilleur levier pour lutter contre l'usurpation d'identité, notamment face à des menaces sophistiquées, comme celles résultant de l'IA générative.

Identifiez les étapes les plus vulnérables du cycle de vie client.

Selon notre enquête, la création de comptes, la connexion et l'autorisation des paiements sont les étapes les plus exposées à l'usurpation d'identité. Il peut être utile initialement de concentrer vos efforts dans ces domaines, mais nous vous recommandons de travailler avec une équipe qualifiée afin de cartographier le parcours de vos clients et d'identifier les risques les plus importants pour votre entreprise.

Dépassez le faux dilemme opposant protection contre la fraude et expérience utilisateur.

Les répondants les plus avisés de notre enquête ont noté que l'amélioration des mesures de lutte contre la fraude ne nécessite pas de compromettre l'expérience utilisateur. Au contraire, l'IDV peut compléter l'expérience client et améliorer la réputation de la marque. Pour offrir la meilleure expérience d'IDV et assurer une mise en œuvre harmonieuse, il convient d'encourager la collaboration entre vos équipes chargées des risques, des produits et de la croissance et de privilégier les produits conviviaux intégrant des fonctions d'automatisation.

Calculez le retour de vos investissements dans la lutte contre la fraude.

Les entreprises qui ont investi beaucoup plus que leurs homologues dans l'IDV ont tendance à économiser davantage que celles qui ont investi autant. Pour obtenir un retour similaire, évaluez un certain nombre de facteurs lorsque vous recherchez de nouvelles technologies, notamment la diminution attendue du coût de la fraude, les économies de personnel grâce à l'automatisation, la baisse des coûts d'acquisition de clients et les gains de chiffre d'affaires provenant des nouveaux clients.

Tenez compte des attentes des jeunes consommateurs.

Les décisionnaires des générations Y et Z sont plus susceptibles de comprendre l'intérêt des outils d'IDV lorsqu'il s'agit d'améliorer la perception de la marque et la sécurité. Il en va de même pour les clients : les nouvelles générations préfèrent les technologies innovantes, telles que l'authentification biométrique, aux autres méthodes. Les entreprises peuvent être certaines qu'en adoptant des technologies de pointe, elles gagneront le respect de leurs jeunes clients et employés, et assureront ainsi leur réussite, aujourd'hui comme demain.

Apprenez-en plus sur **Docusign Identify** et **Entrust**.

Annexe : Méthodologie

Le rapport intitulé *L'avenir de la vérification d'identité dans le monde* est basé sur des données recueillies lors d'une enquête quantitative mondiale en ligne qui a été menée du 6 novembre au 4 décembre 2024. Au cours du processus de collecte des données, notre équipe de recherche² a échangé avec des décisionnaires dans les domaines opérationnel et informatique de différents secteurs et régions. Les décisionnaires interrogés dans le cadre de ce rapport travaillaient dans des entreprises comptant entre 150 et plus de 10 000 employés et rencontraient le même défi, à savoir celui de vérifier l'identité de leurs clients.

Total		N = 1 413	
Public		Taille de l'organisation	
Utilisateurs actuels d'IDV	N = 976	150 – 499	N = 254
Authentification utilisateur / utilisateurs numériques mais pas d'IDV	N = 309	500 – 999	N = 266
Authentification manuelle / utilisateurs non-IDV	N = 128	1 000 – 2 499	N = 274
Marché*		2 500 – 4 999	N = 204
États-Unis et Canada NAM	N = 304	5 000 – 9 999	N = 213
Royaume-Uni EMEA	N = 227	Plus de 10 000	N = 202
Allemagne EMEA	N = 233		
France EMEA	N = 226		
Mexique LATAM	N = 104		
Brésil LATAM	N = 104		
Australie APAC	N = 102		
Japon APAC	N = 113		
* Chaque marché a été traité dans sa langue principale			

Secteurs d'activité couverts par l'enquête		Rôles couverts par l'enquête	
Banque	Produits pharmaceutiques	Opérations informatiques et service informatique	Gestion des risques et conformité
Services professionnels	Distribution et e-commerce	Sécurité informatique	Analyse de la fraude
Éducation	Construction et ingénierie	Gestion des achats et de la chaîne d'approvisionnement	Ressources humaines
Services financiers	Fabrication industrielle	Opérations	Service client
Santé	Immobilier	Expérience client	Juridique
Assurance	Télécommunications	Gestion de produits	Ventes
Services informatiques	Énergie et services publics		
Sciences de la vie			

2 Docusign et Onfido ont mandaté TL;DR Insights, une société d'études de marché, pour mener l'enquête.



À propos de Docusign et de Entrust

Docusign donne vie aux contrats. Aujourd'hui, près d'1,7 million de clients et 1 milliard de personnes dans plus de 180 pays utilisent les solutions Docusign pour améliorer leur productivité et simplifier leur quotidien. Avec la gestion intelligente des accords, Docusign libère des données essentielles à l'entreprise qui sont enfermées dans les documents. Jusqu'à présent, ces données étaient déconnectées des autres systèmes, faisant perdre du temps, de l'argent et des opportunités. Grâce à la plateforme Intelligent Agreement Management de Docusign, les entreprises peuvent créer, formaliser et gérer leurs accords avec des solutions développées par le leader de la signature électronique et de la gestion du cycle de vie des contrats (CLM). Pour plus d'informations, rendez-vous sur docusign.com.

Entrust est un leader novateur dans le domaine des solutions de sécurité centrées sur l'identité, fournissant une plateforme intégrée de solutions de sécurité modulables basées sur l'IA. Nous permettons aux organisations de protéger leurs opérations, d'évoluer sans compromis et de protéger leurs interactions dans un monde interconnecté - pour qu'elles puissent transformer leurs activités en toute confiance. Entrust accompagne ses clients dans plus de 150 pays et travaille avec un réseau mondial de partenaires. Les organisations les plus fiables au monde nous font confiance.

Docusign France
9-15 rue Maurice Mallet
92130 Issy-les-Moulineaux
docusign.com

Pour plus d'informations
emea@docusign.com
+33 (0)9 75 18 13 31