Les PME mettent l'accent sur la sécurité à l'ère de la flexibilité au travail.

LONDON RESEARCH
Research Powered Content

En partenariat avec

Adobe

Sommaire

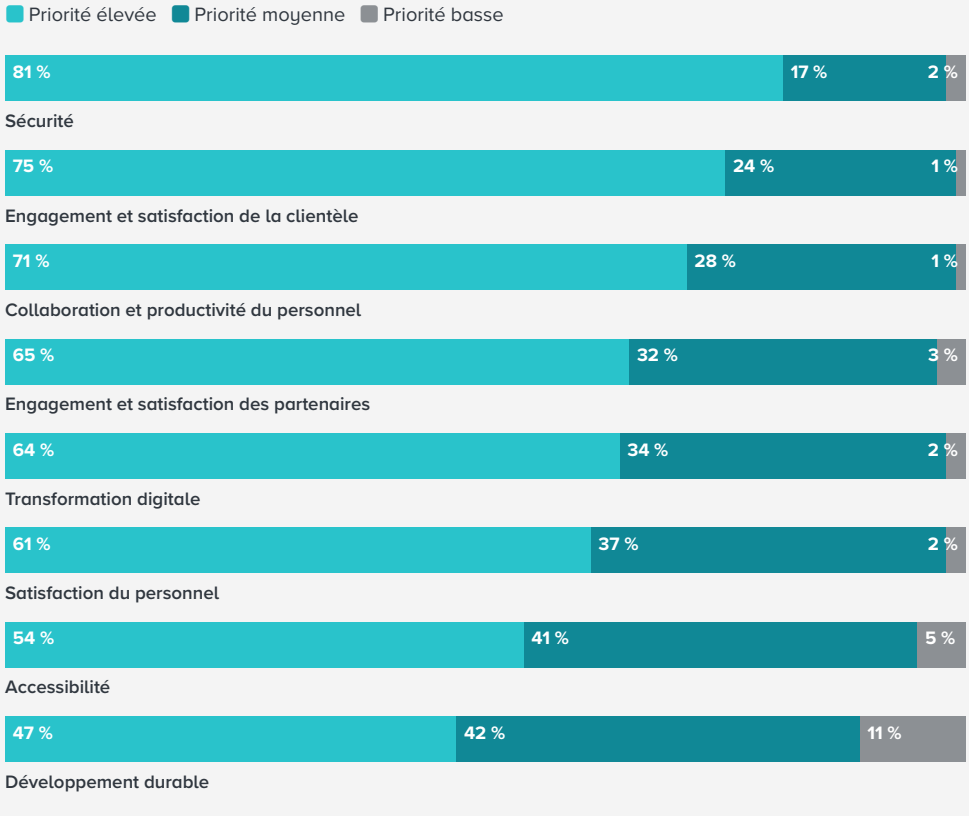
Introduction

Si la flexibilité au travail est aujourd'hui le pire casse-tête qui soit pour les responsables IT, ce n'est pas parce que leurs équipes sont libres de travailler où bon leur semble et aux horaires qui leur conviennent, mais parce que l'ensemble du personnel de l'entreprise adopte ces pratiques. Résultat, les problèmes de sécurité se multiplient. Dans une enquête réalisée en 2023 en partenariat avec Adobe auprès de responsables IT en poste dans de petites et moyennes entreprises (PME) dans la zone EMEA, quatre cadres IT sur cinq (83 %) affirment que les personnes en télétravail dans leur société sont aujourd'hui plus nombreuses qu'avant. Près des trois quarts (71 %) précisent que cet essor du télétravail expose leur entreprise à davantage de problèmes de sécurité.

De fait, 81 % des personnes interrogées considèrent la sécurité comme une priorité absolue (*Figure 1*), devant la satisfaction client (75 %), la productivité du personnel (71 %) ou la préparation de l'avenir digital (64 %). Pour la plupart d'entre elles (63 %), cette problématique est aussi devenue plus urgente ces 12 derniers mois.

FIGURE 1

Dans quelle mesure les domaines suivants constituent-ils une priorité pour votre DTI/DSI en 2023 ?

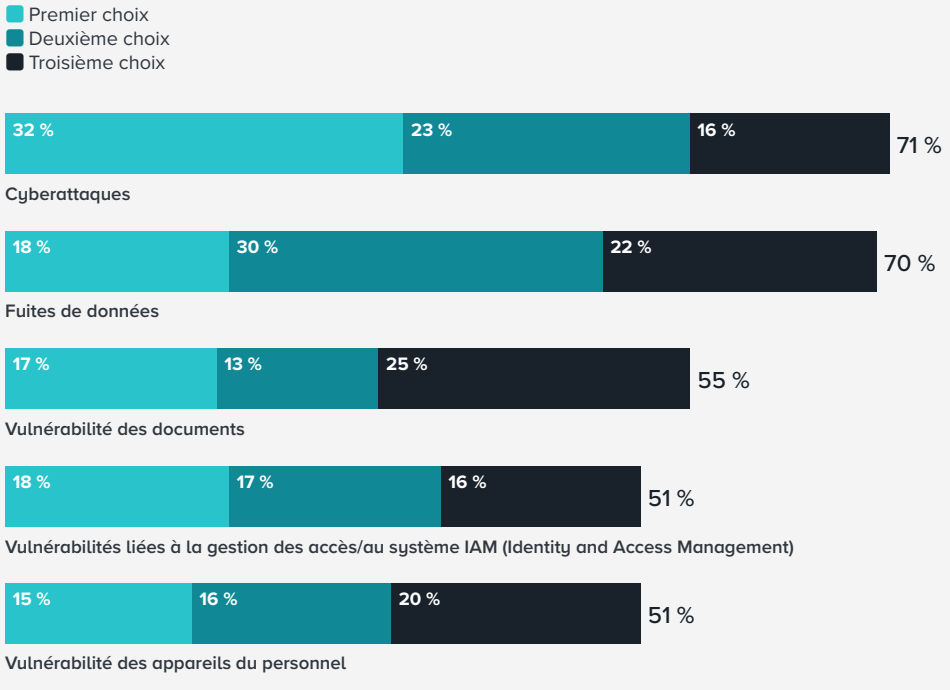


La raison est simple. Quelle que soit l'habileté dont vous faites preuve pour préserver la sécurité et l'intégrité de l'infrastructure IT de votre entreprise lorsque l'ensemble du personnel travaille à l'intérieur du pare-feu, votre mission se révèle infiniment plus difficile dès lors que les salariés se mettent à accéder aux serveurs depuis des réseaux non sécurisés ou à partir de leurs ordinateurs portables, leurs tablettes et leurs téléphones mobiles personnels.

Nous avons donc demandé aux responsables IT de ces PME de nous confier leurs principales préoccupations et force est de constater que la vulnérabilité des documents sensibles se classe dans le trio de tête, après les cyberattaques et les fuites de données (*Figure 2*).

FIGURE 2

Parmi les défis de sécurité suivants, lesquels vous préoccupent le plus ?



La gestion documentaire à l'ère de la flexibilité au travail
La sécurité des documents comprend trois volets essentiels :

Sécurité des utilisateurs et des utilisatrices

Fait-elle obstacle à l'accès frauduleux aux documents ?

Sécurité des contenus

Empêche-t-elle de partager des documents dans leur intégralité ou en partie, notamment en ce qui concerne certains passages sensibles, et permet-elle d'identifier des documents partagés falsifiés ?

Sécurité des systèmes

Protège-t-elle le parc de l'entreprise des tentatives malveillantes visant à réaliser des opérations en écriture ou en lecture dans le système de fichiers d'un ordinateur ?

En fait, plus de la moitié du groupe IT interrogé n'est pas certaine d'avoir réussi le pari d'une gestion documentaire sécurisée. L'un des grands défis à relever est celui de la collaboration. Aider le personnel en télétravail à collaborer est une priorité pour les services IT, comme nous l'avons vu. Or, la sécurisation des communications point à point entre les équipes de travail et les serveurs de l'entreprise est une chose, mais à partir du moment où tous les membres du personnel se mettent à partager, réviser et modifier des documents, les difficultés (et donc les risques) augmentent de façon exponentielle.

Comme le montre la *Figure 3*, seules 44 % des personnes interrogées sont tout à fait d'accord pour dire que les technologies de gestion documentaire utilisées assouplissent et sécurisent leurs méthodes de travail, et 36 % d'entre elles ont totalement confiance dans la sécurité de leurs documents, même s'ils sont créés et partagés à l'extérieur du pare-feu de l'entreprise. En revanche, 45 % reconnaissent avoir plutôt confiance dans la sécurité de leurs documents.

FIGURE 3

Dans quelle mesure êtes-vous d'accord avec les affirmations suivantes concernant la sécurité des pratiques de travail dans votre entreprise ?

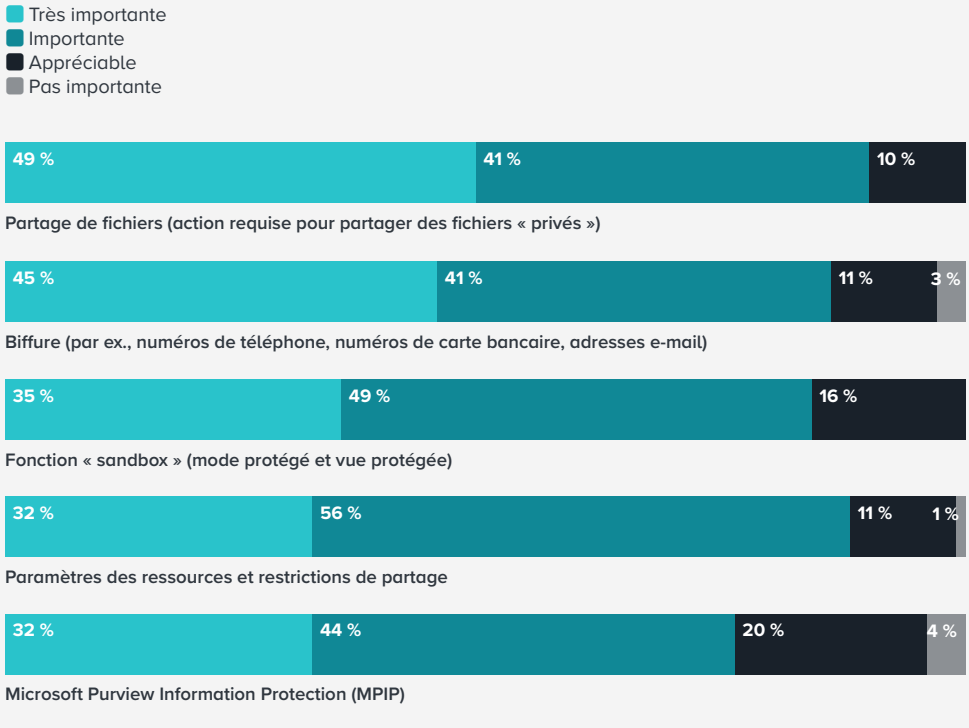
Du point de vue des responsables IT de ces PME, il est donc logique que les investissements dans la gestion documentaire soient motivés par une réduction des risques de sécurité, mais aussi une productivité accrue des salariés. Dans leur quête de technologies pour faciliter le télétravail, il est essentiel que les entreprises mesurent l'importance d'allier la souplesse et la sécurité qui n'ont aucune valeur l'une sans l'autre.

L'importance des fonctionnalités de gestion documentaire

Sur la liste des fonctionnalités de sécurité requises pour une application de gestion documentaire, les responsables IT des PME sondées en classent deux largement en tête : un partage de fichiers priorisant la confidentialité et la possibilité de biffer des informations sensibles ou confidentielles dans un document avant de le diffuser. Toutes deux sont jugées « très importantes » par respectivement 49 % et 45 % des personnes interrogées (*Figure 4*).

FIGURE 4

Dans quelle mesure les fonctionnalités de gestion documentaire sécurisée suivantes sont-elles importantes pour votre entreprise ?

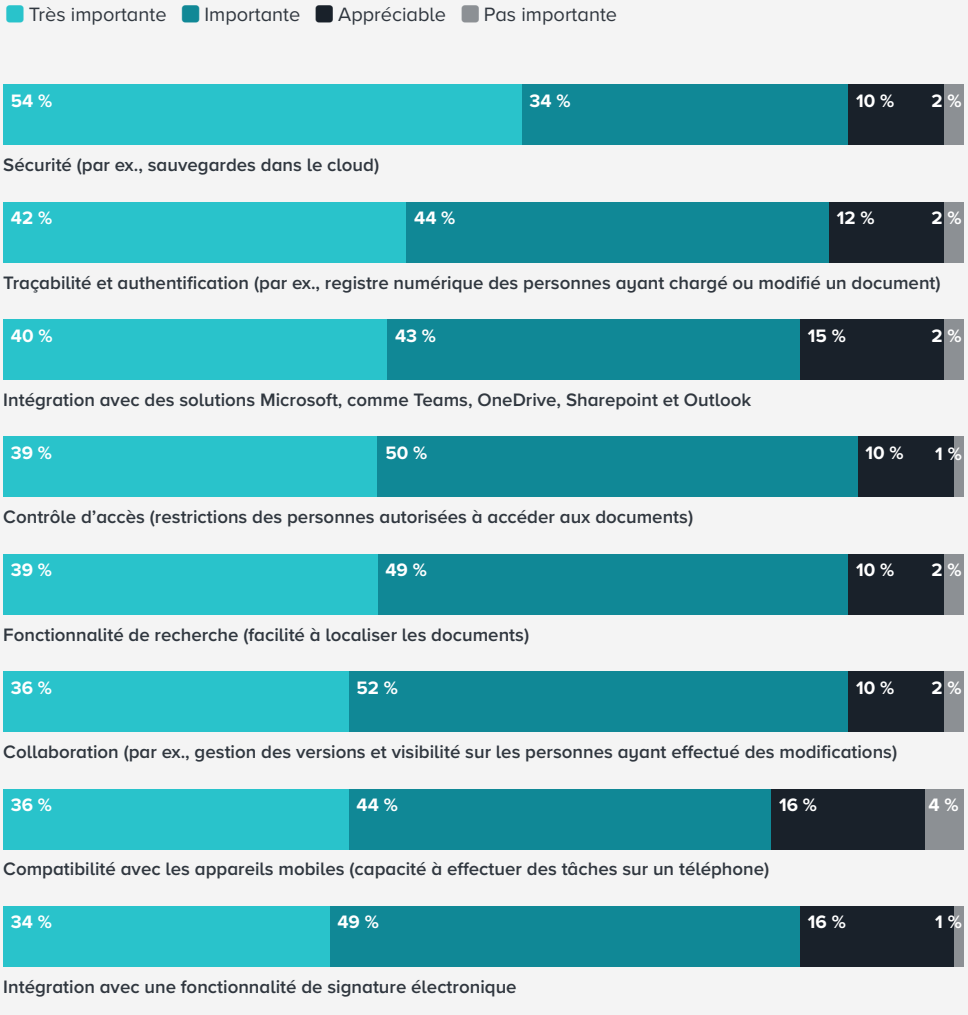


D'autres fonctionnalités, comme la « sandbox », les paramètres des ressources et les restrictions de partage, et Microsoft Purview Information Protection, sont toujours largement considérées comme « importantes », mais pas au point de remettre en question le choix d'une solution qui en serait dépourvue.

Plus de la moitié des responsables IT précisent également que le personnel attache une grande importance à la sécurité dans l'exercice de ses fonctions quotidiennes (*Figure 5*). Il s'agit d'ailleurs de la seule fonctionnalité qui est plus souvent qualifiée de « très importante » que d'« importante », et aussi l'une de celles auxquelles le qualificatif « appréciable » est le moins attribué.

FIGURE 5

Dans quelle mesure les fonctionnalités de gestion documentaire suivantes sont-elles importantes pour le personnel de votre entreprise dans ses tâches quotidiennes ?



Voilà qui montre, là encore, l'importance de concilier sécurité et simplicité d'utilisation. Certaines fonctionnalités, dont on s'attendrait pourtant à ce qu'elles soient considérées comme indissociables d'un système sécurisé (comme la traçabilité et l'authentification ou le contrôle d'accès), sont beaucoup plus rarement qualifiées de très importantes par celles et ceux qui les utilisent.

Ces chiffres semblent également indiquer que la sécurité n'est pas nécessairement perçue de la même manière par les utilisateurs et les utilisatrices d'une application que par leurs collègues du service IT. Ils font également état d'un autre problème pour les entreprises qui composent avec des niveaux de télétravail croissants.

Si les utilisateurs et les utilisatrices reconnaissent volontiers l'intérêt de la sécurité sur le plan théorique, cette conviction ne résiste guère, en pratique, à l'épreuve des délais qui leur sont imposés. La formation joue certes ici un rôle important, mais il est néanmoins préférable de disposer de systèmes « sécurisés par défaut » qui éviteront à ces utilisateurs et ces utilisatrices de s'écarter du droit chemin tout en leur facilitant la tâche.

Les problèmes éventuels

D'après une étude menée par IBM[1], le coût moyen mondial d'un piratage de données en 2022 s'élevait à 4,35 millions de dollars, en progression de 12,7 % par rapport à 2020. En 2022, ce coût moyen ressortait à 5,05 millions de dollars au Royaume-Uni, à 4,85 millions de dollars en Allemagne et à 4,34 millions de dollars en France. De son côté, la US National Cyber Security Alliance établit que 70 % de l'ensemble des cyberattaques ciblent de petites et moyennes entreprises, dont les pratiques de cybersécurité sont souvent moins draconiennes[2]. Les coûts induits englobent les aspects suivants :

- **Versement de rançons**
- **Baisse du cours de l'action (pour les sociétés cotées)**
- **Manque à gagner imputable aux pannes et dysfonctionnements des systèmes**
- **Mesures correctrices**
- **Frais de procédure et d'audit.** Harvard Business Review[3] indique : « Les frais d'audit facturés à des entreprises consécutivement à des fuites de données peuvent être supérieurs de 13,5 % environ à ceux appliqués à des entreprises non victimes de piratage ».
- **Renchérissement des primes d'assurance**

Mais les répercussions ne s'arrêtent pas là. Vous vous exposez également à d'autres désagréments :

- **Perte de propriété intellectuelle**
- **Majorations tarifaires.** 60 % des entreprises victimes d'un piratage de données n'ont d'autre choix que d'en répercuter le coût sur leur clientèle en augmentant leurs prix, d'après The Ponemon Institute[4].
- **Accès au financement en passe d'être plus difficile et plus onéreux.** HBR fait également observer que les cyber-risques peuvent entraîner une dégradation de la note de crédit.
- **Préjudice pour votre marque.** La clientèle existante (et potentielle) peut vous juger moins digne de confiance. Un rapport publié en 2022 par PwC[5] établit qu'au cours des trois années qui ont précédé, 27 % des entreprises à travers le monde ont subi une perte de clientèle et 23 % ont vu leur réputation ou leur image de marque entachée à cause d'un cyberpiratage ou d'un incident préjudiciable à la confidentialité des données. L'atteinte à l'image de marque entraînera également une hausse des coûts RP suite aux actions menées pour rétablir votre réputation.
- **Amendes infligées par les autorités règlementaires.** Si le piratage aboutit à l'exposition des données personnelles de la clientèle, vous risquez d'enfreindre les obligations légales. Conformément au RGPD[6], les autorités nationales en charge de la protection des données sont en droit d'infliger une amende à concurrence de 20 millions d'euros ou de 4 % du chiffre d'affaires mondial de l'entreprise, le montant le plus élevé étant retenu, en cas d'infraction. D'autres sanctions moindres peuvent être prononcées : avertissements et rappels à l'ordre, interdictions temporaires ou permanentes de traitement des données, injonction de mise en conformité, y compris sous astreinte, restriction ou effacement des données et suspension des transferts de données vers des pays tiers.

1 https://www.ibm.com/fr-fr/reports/data-breach
2 https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-the-consequences-of-a-data-breach-threaten-small-businesses
3 https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach
4 https://www.halock.com/summarizing-the-ponemon-cost-of-a-data-breach-report-2022/
5 https://www.pwc.fr/fr/espace-presse/communiques-de-presse/2022/octobre/une-entreprise-sur-quatre-violation-donnees-coutant-plus-d-un-million-de-dollars.html
6 https://gdpr.eu/fines/

Nos recommandations aux responsables IT de PME

Songez à des méthodes de travail souples et sécurisées.

À quoi bon donner à votre personnel les moyens de travailler n'importe où si, ce faisant, vous vous exposez à des piratages de données et à des cyberattaques ? Sans compter que la sécurité de vos documents est compromise. D'un autre côté, il ne sert à rien de mettre en place des systèmes de sécurité tellement hermétiques que le personnel aura du mal à utiliser les plateformes autorisées. En réalité, c'est même pire car s'il ne parvient pas à emprunter les canaux officiels, il trouvera les moyens de les contourner et il n'y aura alors plus aucune sécurité.

Songez aux solutions intégrées.

La gestion du télétravail à grande échelle est déjà suffisamment complexe pour que vous n'ayez pas en plus à vous soucier d'utiliser plusieurs outils (pour la gestion documentaire, le partage de fichiers et les signatures électroniques) sur différents canaux. Plus vous facilitez la tâche du personnel, plus il sera productif, et plus vous le serez vous aussi.

Songez à la sécurité par défaut.

Ne comptez pas sur votre personnel pour réfléchir à la sécurité : il a d'autres chats à fouetter. Aiguillez-le pour qu'il agisse sans commettre d'impair.

Songez à Adobe.

Renforcez au maximum la sécurité de votre pile technologique et de vos données en travaillant avec les solutions documentaires digitales intégrées d'une société dont toutes les activités sont ancrées et orientées sécurité.

Songez à Adobe

Fiabilité et identité dans Acrobat Sign

Acrobat Sign : la fiabilité pour mot d'ordre

Avec Acrobat Sign, vous pouvez utiliser une signature numérique en toute confiance, car elle repose sur une signature électronique et un certificat numérique. La signature numérique est jugée plus sécurisée et plus fiable qu'une simple signature électronique dans de nombreux pays du monde, y compris aux États-Unis et dans l'Union européenne. Elle utilise la cryptographie pour lier le certificat numérique au document signé afin de prouver que chaque signataire est bien la personne qu'elle ou il prétend être. De plus, un horodatage et un sceau infalsifiable vous aident à avoir confiance dans l'authenticité de votre document.

Centre de données dans l'Union européenne/la zone EMEA

Centres de données régionaux : performances et sécurité au plus près de votre entreprise

Certains de nos centres de données Document Cloud sont situés dans la zone EMEA/l'Union européenne. Ils rapprochent ainsi vos données de votre entreprise, ce qui permet de bénéficier de gains de performances, d'une meilleure collaboration et d'un accès simplifié. En unifiant l'espace de stockage Document Cloud et Creative Cloud, vous pouvez exploiter tout le potentiel et toutes les fonctionnalités des services Document Cloud, dont la création, la modification et le partage de fichiers PDF directement depuis les applications Microsoft 365. Par ailleurs, vous contrôlez mieux la situation, ce qui accélère l'adoption au sein de l'entreprise et optimise l'efficacité du stockage.

Attestation C5

C5 : votre sécurité est notre priorité

Adobe Document Cloud est conforme à la norme C5 (Cloud Computing Compliance Criteria Catalogue), un système d'attestation créé en Allemagne par l'Office fédéral de la sécurité des technologies de l'information (BSI) et soutenu par le gouvernement allemand. L'attestation C5 s'appuie sur des normes de sécurité IT reconnues sur le plan international afin d'offrir un framework de sécurité homogène pour la certification des fournisseurs de services cloud. L'obtention de la certification C5 s'inscrit dans notre engagement à optimiser la sécurité du cloud en garantissant la transparence de la protection des données et en vous donnant l'assurance que vos données seront gérées conformément aux normes de sécurité IT.

Méthodologie

Cet article technique rédigé par London Research pour le compte d'Adobe s'appuie sur une enquête réalisée auprès de 200 décisionnaires IT, responsables des applications de gestion documentaire dans de petites et moyennes entreprises implantées au Royaume-Uni, en France et en Allemagne. L'enquête a été réalisée sur le terrain en février 2023. Les PME désignent des entreprises réalisant un chiffre d'affaires annuel inférieur à 100 M£.

Qui sommes-nous ?

LONDON RESEARCH
Research Powered Content

Fondé par l'ex-directeur d'études d'Econsultancy, Linus Gregoriadis, London Research se consacre essentiellement à la production de contenus basés sur des études à destination d'audiences B2B. Nous sommes basés à Londres, mais notre approche et notre optique se veulent internationales. Nous travaillons essentiellement, mais non exclusivement, avec des agences et des fournisseurs de technologies qui s'efforcent de construire un scénario convaincant à partir d'études solides et de points de données éclairants.

Sous la houlette de Communitize Ltd à laquelle nous sommes rattachés, nous collaborons étroitement avec nos sociétés sœurs Digital Doughnut (communauté d'envergure mondiale rassemblant plus de 1,5 million de responsables marketing) et Demand Exchange (plateforme de génération de contacts), à la fois pour syndiquer nos études et générer des leads de grande qualité.

En savoir plus

Adobe Acrobat

Les entreprises continuent de faire appel aux documents, et leurs équipes veulent pouvoir les manipuler facilement, où qu'elles soient, en utilisant une application fiable et bien intégrée. Conçu par l'inventeur du format PDF, Adobe Acrobat est l'outil PDF et de signature électronique idéal pour les entreprises hybrides actuelles. Avec une solution de renom comme Adobe Acrobat, votre entreprise a toutes les cartes en main pour gérer efficacement ses workflows.

En savoir plus


LONDON
RESEARCH
Research
Powered
Content