

Assurer la sécurité documentaire

Allier IA, flexibilité du travail et confiance
dans un monde connecté



Holly Muscolino
Group Vice President,
Workplace Solutions, IDC



Grace Trinidad, PhD, MPH, MS
Research Director,
Trust Measurement and Metrics, IDC



Dans cet InfoBrief

 CLIQUEZ CI-DESSOUS POUR ACCÉDER AUX DIFFÉRENTES SECTIONS DE CE DOCUMENT.

Introduction	3	Surmonter les difficultés : Extraction de données et risques liés à la propriété intellectuelle.....	11
La flexibilité du travail soulève de nouvelles questions en matière de sécurité.....	4	Surmonter les difficultés : Intégrité des documents.....	12
L'IA générative donne une nouvelle dimension aux inquiétudes en matière de sécurité.....	5	Autre difficulté à prendre en compte : le changement de culture.....	13
Les documents sont le moteur de l'activité	6	Recommandations essentielles.....	14
Difficultés liées à la sécurité documentaire	7	Annexe : glossaire	15
Surmonter les difficultés : Les documents comme vecteur d'attaque	8	À propos des analystes d'IDC.....	16
Surmonter les difficultés : Accès ou partage non autorisé	10	Message du sponsor.....	17

Introduction

À l'ère des plateformes technologiques intégrées, de l'IA générative, des équipes dispersées et du travail flexible, **les entreprises repensent et modifient leur approche de la sécurité et de la gouvernance. Cette réflexion doit prendre en compte la sécurité documentaire.**

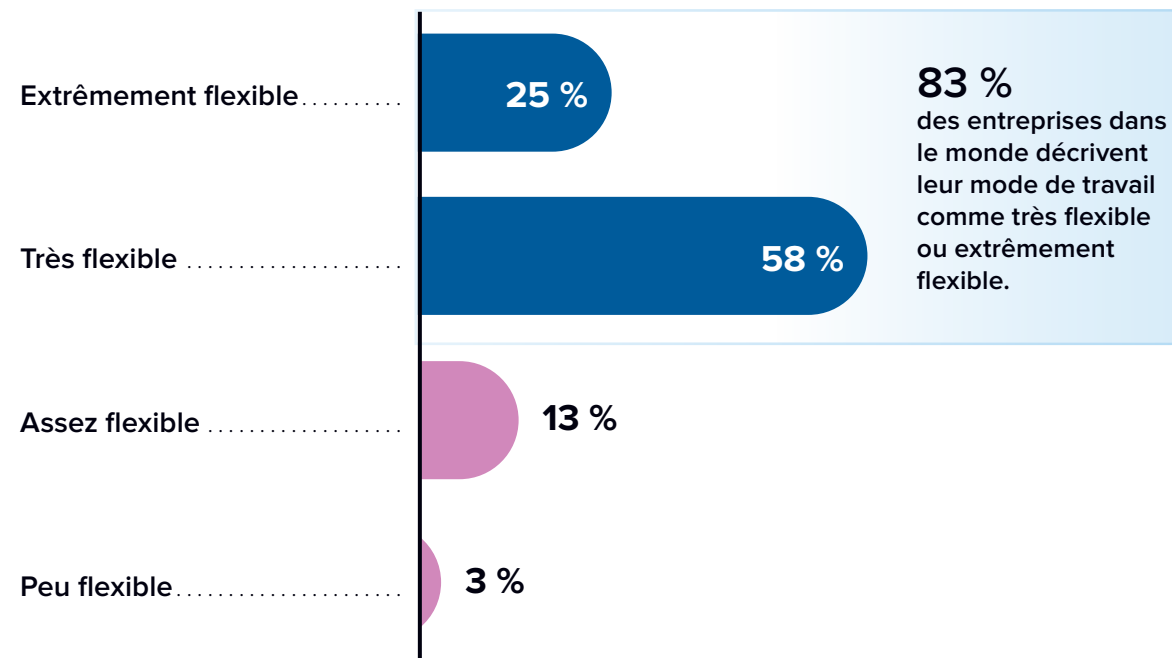
Cet InfoBrief IDC couvre un aspect souvent négligé de la stratégie en matière de sécurité : la sécurité documentaire. Les analystes IDC ont interrogé trois décideurs senior sur leur approche de la sécurité et de la conformité au sein de leur entreprise. Ce document comprend également une synthèse des recherches menées par IDC sur la sécurité organisationnelle liée aux modes de travail flexible et à l'essor de l'IA générative.



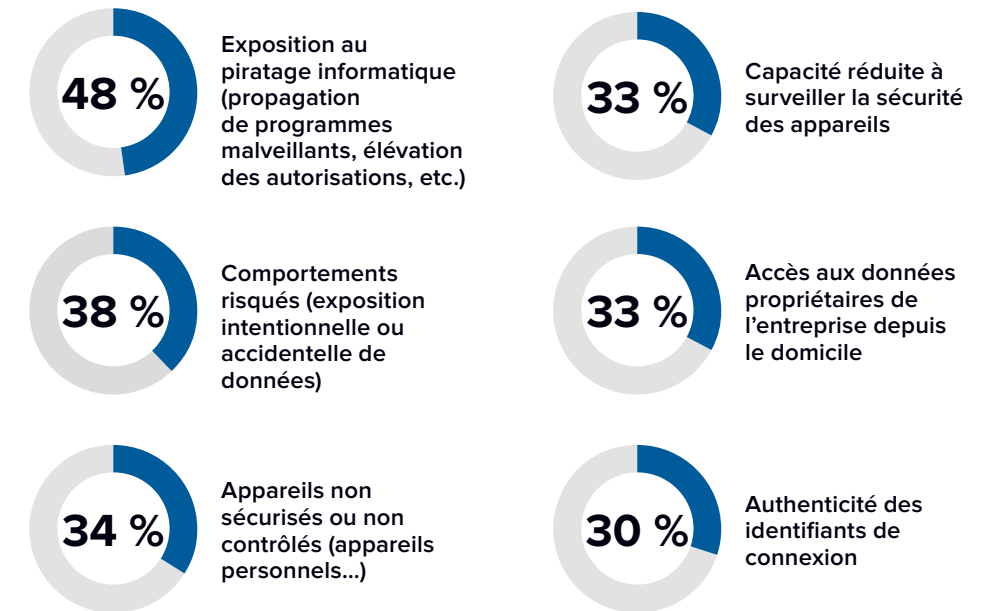
La flexibilité du travail soulève de nouvelles questions en matière de sécurité

Les équipes dirigeantes estiment que les modes de travail flexible augmentent les risques de piratage des systèmes et qu'il est difficile de se protéger des menaces de sécurité.

Comment décririez-vous le mode de travail de votre entreprise ?



Quelles sont vos principales inquiétudes en matière de sécurité liées aux modes de travail flexible ?



Remarque : les sommes peuvent ne pas être égales à 100 % en raison des arrondis. N = 1 269 ; source : *Worldwide Future of Work Survey*, IDC, juin 2024

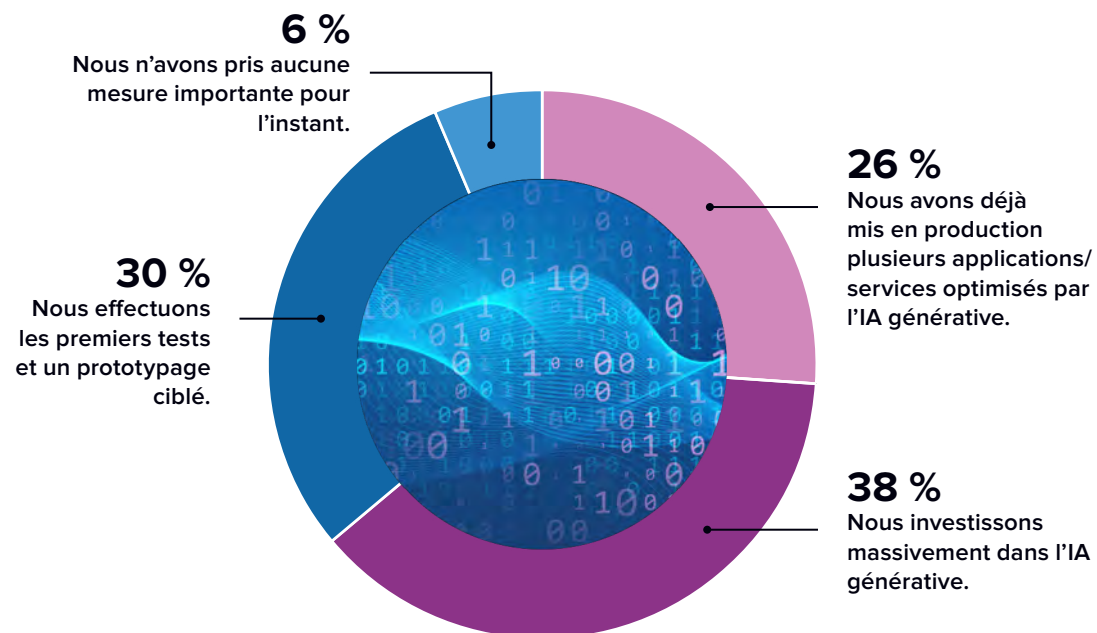


Les modes de travail flexible augmentent les préoccupations des entreprises en matière de sécurité, ou en créent de nouvelles.

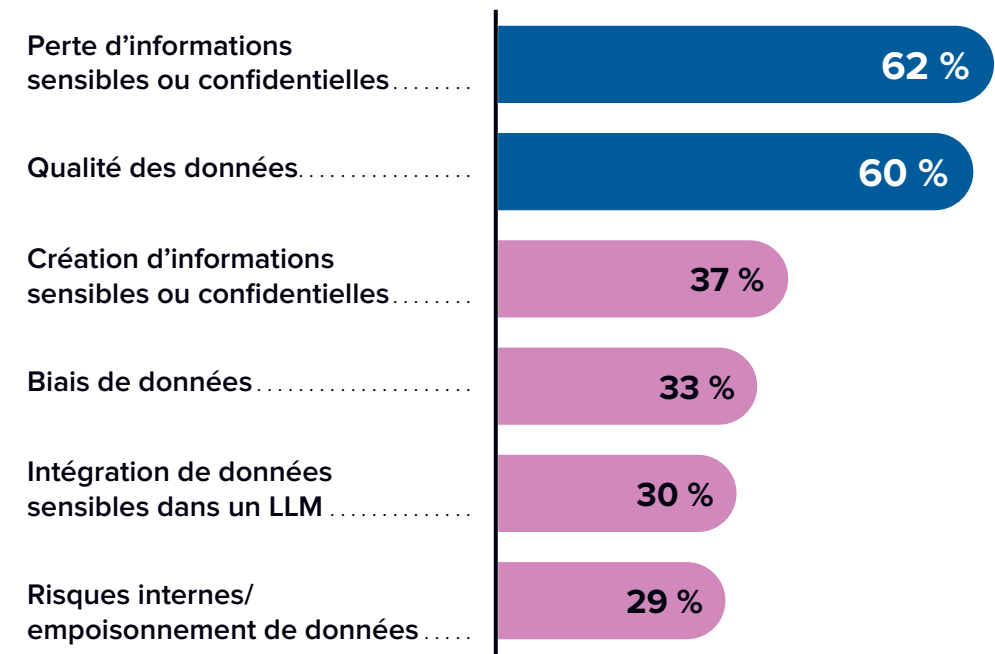
L'IA générative donne une nouvelle dimension aux inquiétudes en matière de sécurité

63 % des entreprises investissent massivement dans l'IA générative ou ont déjà déployé cette technologie, ce qui suscite de **nouvelles inquiétudes liées à la sécurité et à la conformité**.

Où votre entreprise en est-elle dans l'évaluation ou l'utilisation de l'IA générative ?



Quelles sont vos principales inquiétudes en matière de sécurité des données lorsqu'il s'agit d'interagir en privé avec des modèles d'IA générative ?



Remarque : les sommes peuvent ne pas être égales à 100 % en raison des arrondis. N = 891 ; source : *Future Enterprise Resiliency & Spending Survey Wave 7*, IDC, juillet 2024

Remarque : LLM = grand modèle de langage/ Large Language Model. N = 619 ; source : *Data Privacy Survey*, IDC, mars 2024

Les documents sont le moteur de l'activité

Entre 80 % et 90 % des données d'entreprises ne sont pas structurées et la plupart des processus métier dépendent de certains types de documents. Pourtant, la sécurité documentaire est un aspect souvent négligé dans la stratégie de sécurité globale des entreprises.



Ventes

- ▶ Contrats et accords
- ▶ Offres et devis



Juridique

- ▶ Gestion des contrats
- ▶ Accords de confidentialité



Finance

- ▶ Validation des budgets
- ▶ Autorisation de déplacement/frais
- ▶ Validation des factures



Télétravail

- ▶ Demandes
- ▶ Modifications des politiques
- ▶ Contrats et accords



Gestion des produits

- ▶ Autorisations de modifications
- ▶ Validation des conditions préalables
- ▶ Validation des roadmaps



IT

- ▶ Contrats fournisseur
- ▶ Gestion des assets
- ▶ Demandes de modifications



Marketing

- ▶ Onboarding de la clientèle
- ▶ Libre-service
- ▶ Contrats marketing
- ▶ Formulaires de décharge de responsabilité



RH

- ▶ Packages et offres
- ▶ Onboarding du personnel
- ▶ Affiliations
- ▶ Libre-service

Difficultés liées à la sécurité documentaire

Au sein de l'entreprise, la sécurité documentaire est un défi majeur que l'essor des modes de travail flexible a accentué.

Les documents sont un vecteur d'attaque

Tous les types de fichier sont exploitables (.doc, .xls, .ppt, .jpg, .png, etc.), mais les PDF sont la cible de prédilection des pirates car ils sont très répandus. Entre 2019 et 2020, Palo Alto Networks a constaté une hausse de **1 160 % du nombre de PDF malveillants**.

(Source : unit42.paloaltonetworks.com/phishing-trends-with-pdf-files)

Accès ou partage non autorisé

Les partages de documents et de PDF étant fréquents, **des contrôles d'accès trop rigoureux peuvent conduire à un accès non autorisé à des documents importants**. Le contrôle A.9.2.1 de la norme ISO 27001 limite l'accès des utilisateurs et utilisatrices aux informations et applications.

Risques liés à l'extraction de données, protection de la propriété intellectuelle

Les pirates informatiques et les équipes internes **peuvent exposer l'entreprise à un risque d'extraction de données non autorisée et préjudiciable**. Tout type de document est susceptible de contenir des métadonnées corrompues, du texte sélectionnable, des objets ou des liens intégrés et des données de formulaire masqués.

Conformité

Les règles et frameworks de sécurité actuels mettent **l'accent sur la pseudonymisation et le chiffrement des données pour protéger les informations personnelles**. L'article 32(1) du RGPD indique de : « [mettre en œuvre] les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : la pseudonymisation et le chiffrement des données à caractère personnel. »

« ... Identifier les données et être capable d'agir en conséquence est un enjeu majeur en interne... Lors de chaque transfert de données d'un système à un autre, nous essayons de déterminer précisément leur nature... »

Directeur, Application Development
d'une grande compagnie d'assurances

SURMONTER LES DIFFICULTÉS : Les documents comme vecteur d'attaque

Les types de documents les plus souvent utilisés, comme les PDF, sont devenus un vecteur d'attaque prisé car ils peuvent être modifiés facilement, leur utilisation est répandue sur l'ensemble des plateformes et du contenu peut y être incorporé facilement en utilisant des flux codés, du code JavaScript, des fichiers exécutables et d'autres méthodes.

En 2022, Sophos Labs a découvert qu'une macro VBA dissimulée dans un document Word, lui-même caché dans un fichier PDF, lançait une variante du ransomware Locky. Il suffisait qu'une personne de bonne foi suive les instructions du document et active la modification pour que la macro VBA télécharge et exécute le programme malveillant.



SURMONTER LES DIFFICULTÉS : Les documents sont un vecteur d'attaque (Suite)



Types de documents couramment utilisés

PDF

Documents MS Office (.docx, .pptx, .xlsx)

Fichiers compressés (.zip, .rar)

Fichiers image (.jpg, .png, .gif)

Fichiers exécutables (.exe, .msi)



Vecteurs d'attaque courants

Macros ou scripts malveillants

Flux codés, images, fichiers exécutables

Vulnérabilités des lecteurs de PDF, applications Microsoft

Phishing via du contenu trompeur



Options de contrôle de la sécurité

Formation et sensibilisation

Sandbox pour les pièces jointes

Restrictions sur les types de fichiers

E-mails cryptés

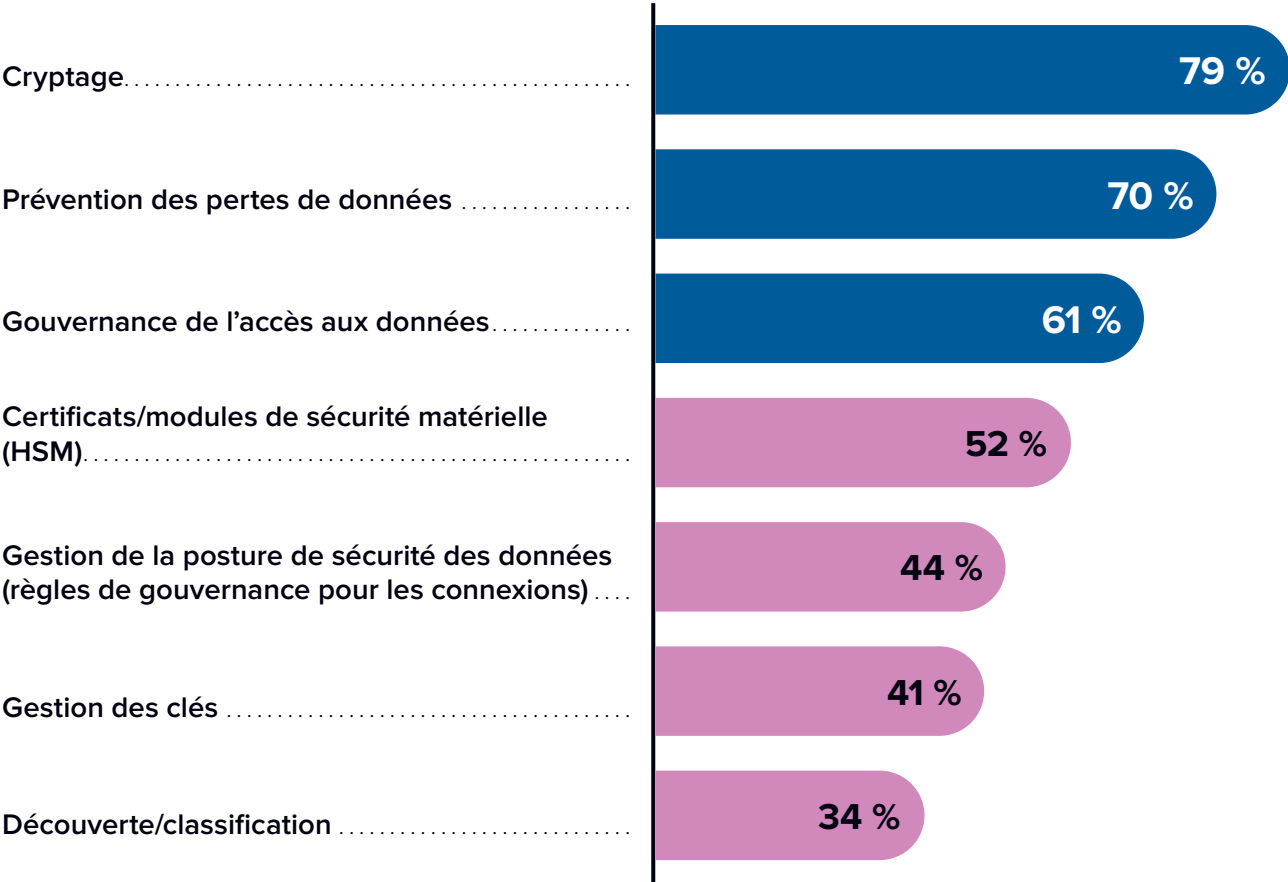
Solutions contre les programmes malveillants/antivirus sur les appareils

SURMONTER LES DIFFICULTÉS : Accès ou partage non autorisé

Technologies de sécurité

- ▶ Authentification et emplacements privilégiés
- ▶ Contrôle des accès
- ▶ Sécurité des applications (sandbox, sécurité JavaScript)
- ▶ Certifications de conformité
- ▶ Gestion des droits digitaux
- ▶ Signatures numériques
- ▶ Cryptage
- ▶ Étiquettes de confidentialité
- ▶ Biffure
- ▶ Partage de liens sécurisé, listes de liens autorisés
- ▶ Stockage sécurisé
- ▶ Tests de sécurité tiers

Quelles technologies de sécurité des données utilisez-vous pour la confidentialité/conformité à l'échelle mondiale ?



Remarque : HSM = Hardware security module (module de sécurité matérielle). N = 227 ; source : North America eSignature Market Survey, IDC, novembre 2021

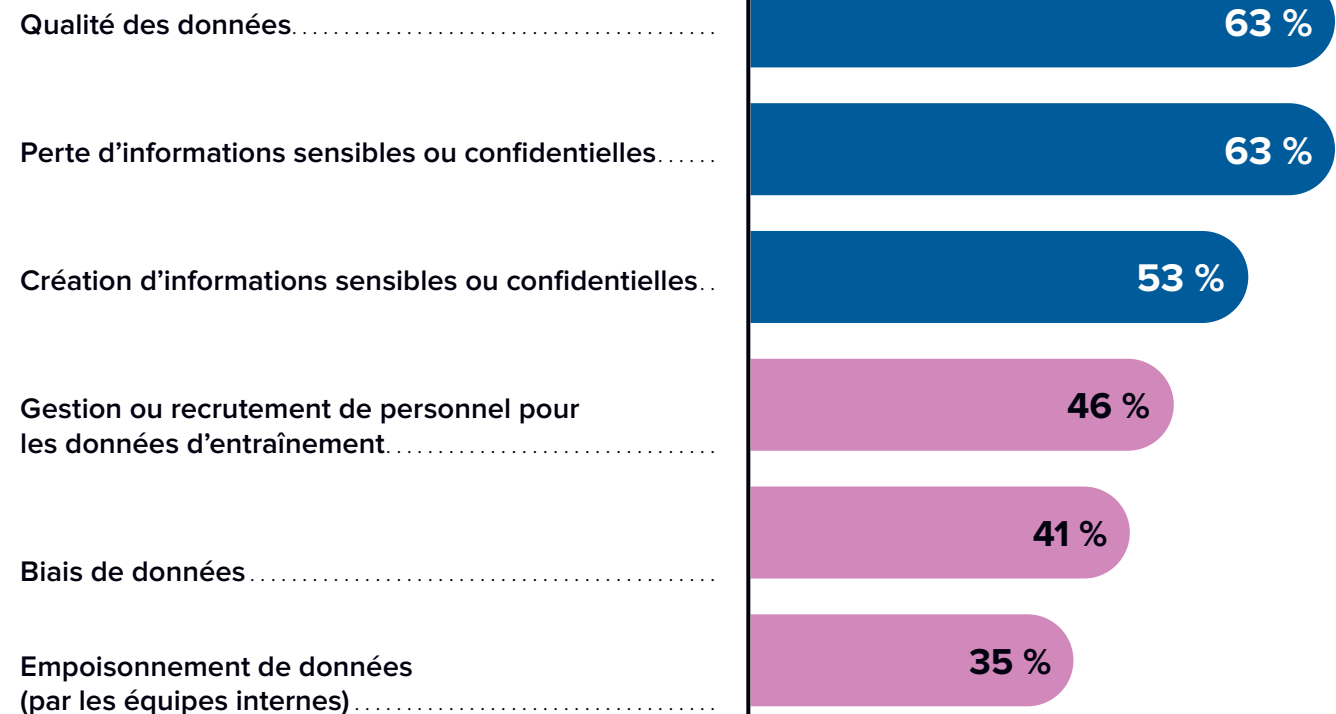
SURMONTER LES DIFFICULTÉS : Extraction de données et risques liés à la propriété intellectuelle

L'IA générative augmente les risques d'accès non autorisé à des données sensibles.

« Nous privilégions une utilisation responsable de l'IA générative. Pour accéder à ces données non structurées ... nous avons investi [près] d'un milliard de dollars en 10 ans pour tenter d'organiser nos données dans des data lakes Hadoop ... Avec l'arrivée de l'IA générative, ces data lakes ont été abandonnés. Ils n'étaient plus d'aucune utilité. »

Directeur, Application Development
d'une grande compagnie d'assurances

Quelles sont vos principales inquiétudes en matière de sécurité des données liées à l'utilisation des modèles d'IA générative ?

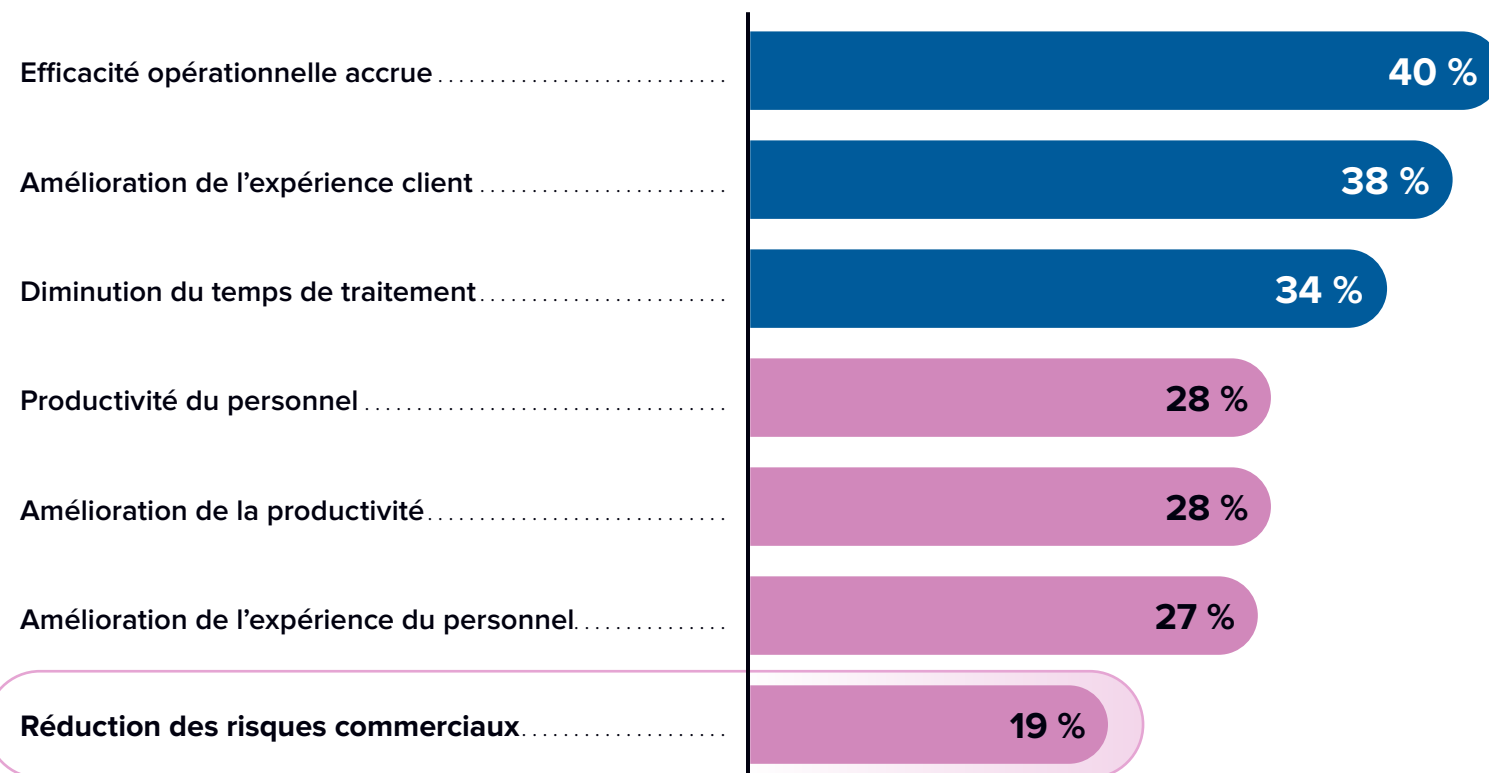


N = 610 ; source : Data Privacy Survey, IDC, mars 2024

SURMONTER LES DIFFICULTÉS : Intégrité des documents

Sécuriser les workflows à l'aide de signatures électroniques et numériques s'avère efficace.

Quels avantages votre entreprise a-t-elle tirés ou s'attend-elle à tirer du déploiement de technologies ou de services de digital workplaces intelligents ?



« Actuellement, nous avons deux personnes pour gérer 32 000 signatures électroniques par an. Ce système nous permet d'avoir une personne principalement responsable de leur gestion et une autre qui l'assiste occasionnellement. C'est extrêmement efficace. »

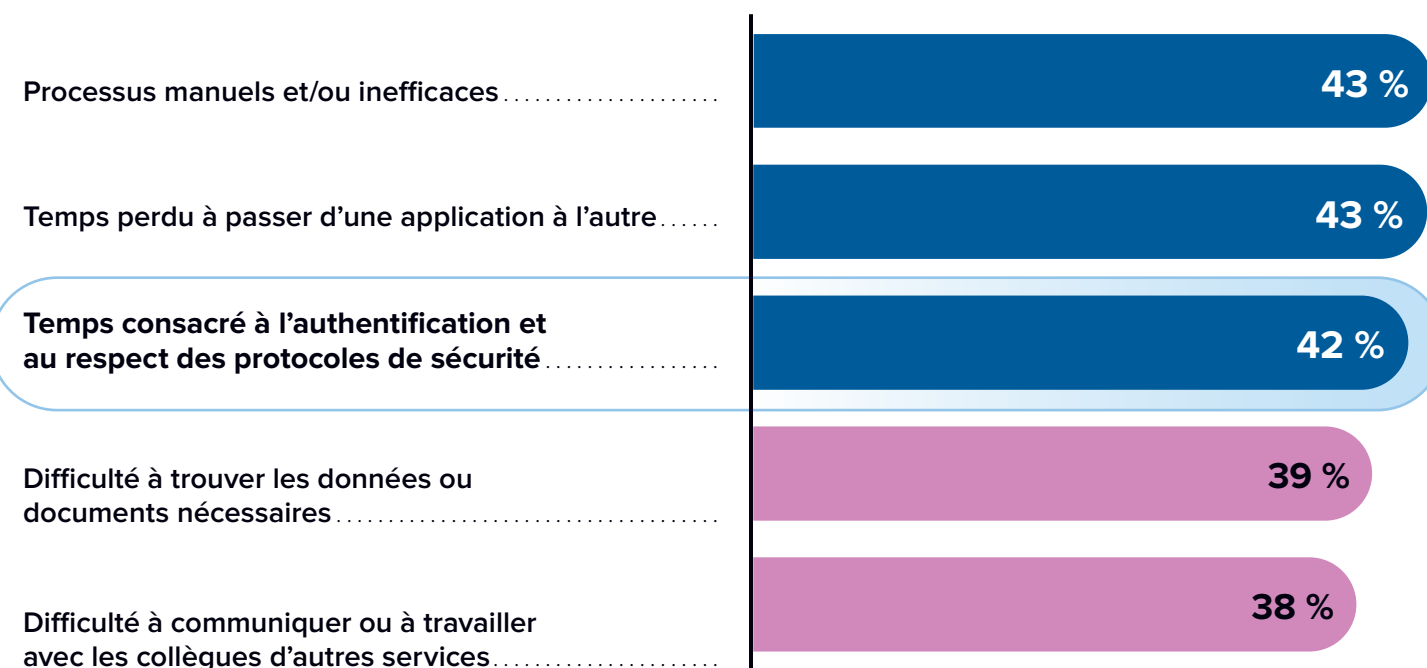
Director, Application Development
d'une grande compagnie d'assurances

N = 227 ; source : North America eSignature Market Survey, IDC, novembre 2021

Autre difficulté à prendre en compte : le changement de culture

Le temps passé à respecter les protocoles de sécurité est l'une des cinq principales difficultés empêchant les équipes de travailler aussi efficacement que possible.

Quels sont les cinq obstacles principaux à la productivité de vos équipes ?



« ... Je pense qu'il est essentiel ... d'avoir une approche de la sécurité axée sur les personnes. Il est primordial que notre équipe de sécurité représente réellement les personnes que nous servons. »

CISO/RSI d'un grand éditeur d'applications

N = 609 ; source : Intelligent Digital Workspace Market Survey, IDC, mai 2022

Recommandations essentielles

Avec plusieurs centaines de milliards de documents et PDF en circulation et de nouveaux fichiers créés chaque jour, **les décisionnaires doivent s'assurer que les workflows documentaires sécurisés font partie de la stratégie de sécurité globale de leur entreprise.**

- ✓ **Déployez des applications axées sur les documents**, sécurisées par défaut, avec des fonctionnalités de sandbox pour les pièces jointes, de restrictions sur les types de fichiers et de chiffrement des données.
- ✓ **Instaurez des règles et des procédures** pour limiter les risques d'accès ou de partage non autorisé, et des systèmes d'authentification et de gestion des identités et des accès adaptés.
- ✓ **Appréhendez les nouvelles menaces de sécurité et les risques** que présente l'IA, et adaptez votre stratégie de sécurité pour les atténuer.
- ✓ **Ne négligez pas le facteur humain.** Cultivez un état d'esprit axé sur la sécurité dans toute l'entreprise, prenez en compte les workflows du personnel sur site et à distance, établissez des règles en conséquence et assurez-vous qu'elles peuvent être respectées facilement.
- ✓ Enfin, **travaillez en partenariat avec des fournisseurs de technologies documentaires** qui peuvent vous aider à suivre les recommandations énoncées plus haut et qui ont conscience d'être l'un des maillons d'une supply chain opérationnelle.

Annexe : glossaire

Travail flexible : un mode de travail dynamique qui permet aux équipes de travailler sur site, sur le terrain ou à distance, en fonction de la politique de l'entreprise et des besoins de l'activité (également appelé **travail hybride**).

- ▶ **Non flexible** : il n'y a pas de stratégie officielle pour prendre en charge un mode de travail flexible.
- ▶ **Peu flexible** : des responsables autorisent sur demande et de manière ponctuelle un mode de travail flexible, mais aucune stratégie officielle n'a été mise en place.
- ▶ **Assez flexible** : l'équipe de direction a fourni des directives provisoires permettant un mode de travail flexible/hybride.
- ▶ **Très flexible** : nous avons mis en place dans de multiples services des règles permettant de travailler sur site et à distance en fonction des besoins de l'activité.
- ▶ **Extrêmement flexible** : nous avons mis en place une stratégie de travail flexible qui permet d'alterner entre travail sur site et à distance sans difficultés techniques ni problèmes de politiques.

À propos des analystes d'IDC



Holly Muscolino
Group Vice President,
Workplace Solutions, IDC

Holly Muscolino est Group Vice President, Workplace Solutions, chez IDC. Elle est responsable des études sur l'innovation et la transformation des solutions axées sur le contenu, comme le traitement documentaire intelligent, la signature électronique, l'imagerie et l'impression, et d'autres services liés aux workflows de contenu. Ses recherches portent également sur la transformation du travail, les compétences digitales et le rôle de la technologie dans l'avenir du travail.

[En savoir plus sur Holly Muscolino](#)



Grace Trinidad, PhD, MPH, MS
Research Director,
Future of Trust, IDC

Grace Trinidad est Research Director au sein du service d'étude Security and Trust d'IDC. Elle est responsable du programme de recherche Future of Trust. À ce titre, elle fournit des orientations stratégiques et un soutien à la recherche sur les approches en matière de risque, de sécurité, de conformité, de confidentialité, d'éthique et de responsabilité sociale. Grace Trinidad a publié des travaux reconnus sur la confidentialité et la confiance, plus précisément sur l'attitude du public à l'égard de l'utilisation à des fins commerciales de données médicales personnelles. Ses recherches portent également sur l'éthique de l'intelligence artificielle et du partage de données, la confiance à l'égard des prestataires et établissements de santé, l'accès aux bases de données génomiques et leur utilisation, et l'équité en matière de données.

[En savoir plus sur Grace Trinidad](#)

Message du sponsor



Déployez des expériences de qualité en toute confiance.

Adobe Acrobat permet aux entreprises de proposer des expériences documentaires fiables, qui transforment leur activité et assurent leur croissance.

- ▶ Travaillez en toute sécurité où que vous soyez, grâce à une sécurité et une conformité adaptées aux exigences de l'entreprise.
- ▶ Tirez parti de fonctionnalités d'IA pour créer des documents de qualité, avec des insights vérifiables pour accélérer le travail.

Téléchargez Adobe Acrobat dès aujourd'hui

IDC Custom Solutions

Cette publication a été produite par IDC Custom Solutions. L'opinion, l'analyse et les résultats de recherche fournis sont issus d'études et d'analyses plus détaillées ayant été menées et publiées de manière indépendante par IDC (sauf mention spéciale de partenariat d'un fournisseur spécifique). IDC Custom Solutions produit du contenu IDC dans un grand nombre de formats, afin d'en assurer sa potentielle diffusion par différentes entreprises. Ce support IDC peut faire l'objet d'un usage externe sous licence et l'utilisation ou la publication d'une étude IDC ne signifie en aucun cas qu'IDC cautionne les produits ou stratégies des sponsors ou titulaires de licence.



IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, États-Unis
Tél. : +1 508 872 8200

[idc.com](https://www.idc.com)

[in @idc](https://www.linkedin.com/company/idc)

[X @idc](https://twitter.com/idc)

International Data Corporation (IDC) est un acteur majeur de la recherche, du conseil et de l'évènementiel sur les marchés des technologies de l'information, des télécommunications et des technologies grand public. Avec plus de 1 300 analystes dans plus de 110 pays à travers le monde, IDC offre une expertise internationale, régionale et locale sur les opportunités et tendances technologiques et industrielles. Les analyses et insights d'IDC aident les spécialistes IT, les décideurs et la communauté des investisseurs à prendre des décisions éclairées en matière de technologie et à atteindre leurs objectifs clés.

©2025 IDC. La reproduction de ce document sans autorisation est interdite. Tous droits réservés. [CCPA](#)