

# MarketScape IDC : Evaluation mondiale 2022-2023 des fournisseurs de systèmes d'impression papier proposant des solutions et des services de sécurité

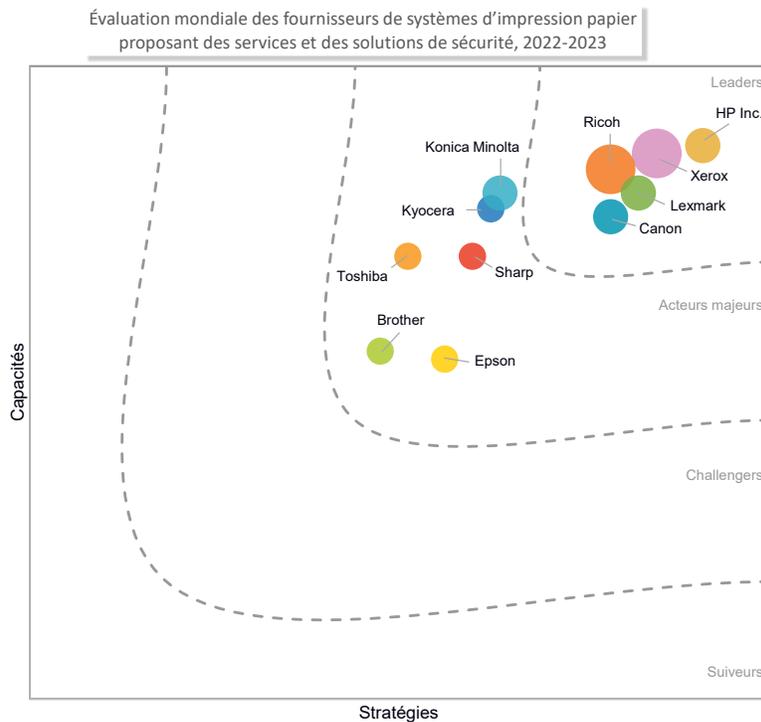
Robert Palmer

LEXMARK EST CITÉ DANS CET EXTRAIT DU MARKETSCAPE IDC

## REPRÉSENTATION GRAPHIQUE DU MARKETSCAPE IDC

FIGURE 1

### MarketScape IDC : Evaluation mondiale des fournisseurs de systèmes d'impression papier proposant des services et des solutions de sécurité



Source : IDC, 2023

Veillez vous reporter à l'Annexe pour en savoir plus sur la méthodologie, la définition du marché et les critères de notation utilisés par IDC.

## DANS CET EXTRAIT

---

Cet extrait est directement tiré du MarketScape IDC : Worldwide Security Solutions and Services Hardcopy 2022-2023 Vendor Assessment (doc. N° US48851622). Les chapitres suivants figurent en partie ou en totalité dans cet extrait : Le point de vue d'IDC ; Critères d'inclusion des fournisseurs dans le MarketScape IDC ; Annexe et En savoir plus. La Figure 1 a également été reprise.

## LE POINT DE VUE D'IDC

---

L'étude réalisée par IDC s'appuie sur le modèle MarketScape d'IDC utilisé pour analyser le marché des services et des solutions de sécurité proposés par une sélection de fournisseurs de systèmes d'impression. Elle examine les critères quantitatifs et qualitatifs qui conditionnent le succès de ces fournisseurs. Ce MarketScape IDC porte sur divers fournisseurs de systèmes d'impression et repose sur un cadre permettant d'évaluer différentes fonctionnalités et solutions de sécurité autonomes, proposées dans des contrats de services managés d'impression et de gestion des documents (MPDS), ou dans des services professionnels managés n'entrant pas dans la catégorie des MPDS. De nombreux fabricants de systèmes d'impression proposent des solutions et des services de sécurité afin d'enrichir leurs offres actuelles de services managés de gestion des impressions et des documents, tout en développant d'autres offres distinctes, ou connexes. En s'appuyant sur le MarketScape d'IDC, les entreprises peuvent identifier les fournisseurs offrant des solutions de qualité et s'appuyant sur des stratégies commerciales intégrées permettant de pérenniser leurs activités et de rester durablement compétitifs. Les capacités et les stratégies considérées comme pertinentes dans le cadre de cette étude sont les suivantes :

- Le fournisseur doit disposer d'un portefeuille de solutions disponibles, proposer des fonctionnalités de sécurité intégrées à ses périphériques, des services managés, des services professionnels et autres capacités permettant de sécuriser l'infrastructure d'impression et de gestion des documents.
- Il doit avoir les compétences essentielles en matière d'évaluation des niveaux de menace, de détection et de réduction des risques.
- Il doit disposer d'une feuille de route répondant aux problèmes spécifiquement rencontrés par les entreprises pour sécuriser leur infrastructure d'impression et de gestion des documents.
- Il doit proposer des ressources et des stratégies permettant à ses clients de respecter leurs obligations de conformité et de s'aligner avec les principaux standards de leurs secteurs respectifs.
- Il doit disposer de ressources et de stratégies pour aider ses clients à déterminer la meilleure façon d'aborder la sécurisation de leur environnement d'impression dans le cadre d'une politique de sécurité de type zero trust.
- Il doit avoir une approche holistique en proposant des solutions adaptées à des secteurs d'activités spécifiques ainsi que des solutions répondant à des besoins transverses, via des canaux de distribution directs et indirects.
- Il doit chercher à atteindre l'excellence opérationnelle et en matière de prestations de services, en proposant notamment des services cohérents à l'échelle locale, régionale et mondiale.
- Il doit disposer de ressources et de stratégies pour surmonter des défis spécifiques en matière de sécurité dans les environnements de travail hybride, y compris en matière de migration vers les infrastructures d'impression dans le cloud.

- Il doit en permanence étendre ses activités pour couvrir de nouvelles zones géographiques, de nouveaux secteurs d'activité et de nouvelles applications métiers.
- Il doit proposer des modèles de services, de tarification et de facturation flexibles, ainsi que des solutions adaptées aux infrastructures sur site et dans le cloud public comme privé.

## CRITERES D'INCLUSION DES FOURNISSEURS DANS LE MARKETSCOPE IDC

---

Cette étude consiste en une analyse de 11 grands fabricants d'équipements d'impression papier, disposant d'un large portefeuille de matériels dédiés aux environnements d'impression pour des équipes/des départements distribués dans le monde. Le fournisseur doit disposer d'un portefeuille de solutions et de services de sécurité autonomes et y consacrer une partie importante de son budget de R&D. Les entreprises spécialisées dans l'externalisation de l'IT ou des processus métiers, ainsi que les éditeurs de logiciels proposant des services d'impression, de sécurité et de gestion documentaire dans le cadre de leurs services IT, ou qui sous-traitent ces services auprès de fabricants d'équipements d'impression, ont été exclus de l'analyse. Ont également été exclus de cette étude les distributeurs indirects des fabricants d'équipements d'impression papier.

## CONSEILS POUR LES ACHETEURS DE SOLUTIONS TECHNOLOGIQUES

---

La sécurité reste l'une des préoccupations majeures des entreprises de toutes tailles. Pourtant, les initiatives visant à renforcer la sécurité des systèmes d'impression accusent depuis toujours un retard par rapport à la sécurité IT dans son ensemble. De nombreux CISO et responsables IT ont supposé que les systèmes mis en place pour protéger le réseau s'étendraient aux périphériques connectés. Mais la sécurité autour du réseau devient de plus en plus fragile. Chaque périphérique qui y est connecté constitue désormais un risque de sécurité, y compris les imprimantes et les périphériques multifonctions.

Une faille de sécurité sur l'infrastructure d'impression et de gestion des documents a les mêmes conséquences que toute autre faille de sécurité : coûts importants dus aux interruptions de services nécessaires pour identifier et réparer, amendes pour défaut de conformité lié à la gouvernance de l'entreprise ou au respect de la réglementation, pertes de clients et dommages réputationnels. La sécurité de l'infrastructure IT est égale à celle son maillon le plus faible. Et pour de nombreuses entreprises, l'infrastructure d'impressions et de gestion des documents est un des éléments les plus vulnérables.

En parallèle, la pandémie de COVID-19 a modifié l'organisation du travail, ce qui a soulevé de nouveaux problèmes de sécurité. La généralisation du travail hybride accélère la transition vers un modèle de sécurité zero trust, afin de prendre en charge les utilisateurs à distance, les applications cloud et les actifs externes. Il est devenu dangereux de supposer que tout ce qui se trouve derrière le pare-feu de l'entreprise est protégé. Encore faudrait-il que cela soit possible. Au contraire, chaque requête doit être traitée comme si elle provenait d'un réseau ouvert. Par conséquent, il convient d'adopter une approche globale de la sécurité de l'infrastructure d'impression.

Pour cette raison, les organisations devraient considérer les recommandations suivantes :

- **Sécurité de l'impression dans un environnement hybride.** Peu d'entreprises ont fourni à leurs salariés travaillant à distance les lignes directrices en matière d'achat et d'utilisation des imprimantes. Certaines leur ont conseillé d'utiliser leur imprimante personnelle, tandis que

d'autres ont autorisé leurs collaborateurs à acheter une nouvelle imprimante puis les ont remboursés. Ce manque d'homogénéité induit des risques de sécurité importants que les responsables IT et de la sécurité doivent traiter en priorité.

- **Concilier praticité, productivité et sécurité.** Les organisations sont dans la délicate position où elles doivent garantir à leurs salariés une expérience pratique et cohérente en matière d'impression, tout en s'assurant que les imprimantes et les périphériques multifonctions (MFP) utilisés sont conformes à leurs politiques de sécurité et de conformité. A l'occasion d'une récente étude réalisée par IDC, 43 % des entreprises indiquent que les failles de sécurité, ainsi que la capacité à s'assurer que les périphériques d'impression sont conformes à leurs politiques de gouvernance et de sécurité, constituent un défi majeur.
- **Prendre en compte la sécurité de l'impression dans la stratégie globale de sécurité IT.** Il s'agit d'élaborer un plan à long terme, avec des indicateurs permettant de surveiller en continu la sécurité des systèmes d'impression. Les fournisseurs proposent une large gamme de services de protection des périphériques et des données. Nombre de ces services sont conçus pour être intégrés aux systèmes métiers et à ceux de gestion des documents déjà utilisés par l'entreprise afin de fournir une protection supplémentaire et de répondre aux exigences de gouvernance et de conformité réglementaire.
- **Etendre le périmètre des outils de sécurisation d'impression sur site pour englober les lieux distants.** Les entreprises peinent à surveiller et à gérer les périphériques à distance. Les fonctionnalités classiques des logiciels d'impression, telles que l'impression sur la base de règles, l'impression sécurisée, le suivi des tâches et la comptabilité, restent essentielles pour avoir une meilleure visibilité sur le recours à l'impression. C'est particulièrement vrai dans le contexte du travail hybride où les périphériques ne sont souvent pas visibles et où les pratiques ne sont pas faciles à suivre.
- **Considérer vos fournisseurs actuels de systèmes d'impression.** Lors de l'analyse des besoins en matière de sécurité des impressions et des documents, il convient de tenir également compte des fournisseurs actuels. Il est probable qu'ils disposent d'un ensemble de solutions et de services adaptés, s'appuyant sur une feuille de route d'intégration de technologies permettant de répondre à l'évolution des besoins de l'entreprise.
- **Identifier les solutions répondant à vos problématiques sectorielles.** Les besoins en matière de sécurité ainsi que les exigences de conformité réglementaire varient considérablement d'un secteur d'activité à l'autre. Il convient donc de rechercher un fournisseur compétent dans la gestion des processus d'impression et documentaires, la gestion de contenu et la sécurisation des services d'impression, en fonction de vos activités spécifiques.
- **Zero trust.** Les entreprises ont tout intérêt à réfléchir à des solutions permettant d'intégrer la gestion des impressions à leur politique zero trust. Des outils et des technologies spécifiques peuvent être nécessaires pour garantir des workflows d'impression sécurisés, tels que le développement d'applications sécurisées, des solutions cloud de pull printing, des certificats pour les périphériques, des fonctionnalités matérielles multi-niveau, du chiffrement et de l'authentification multi-facteur. Les impressions et les outils de gestion des impressions dans le cloud peuvent être pertinents pour les organisations cherchant à simplifier et à rendre cohérente l'expérience d'impression des salariés en télétravail.

## PROFIL RESUME DU FOURNISSEUR

---

Cette section présente brièvement les principales observations d'IDC ayant permis de positionner le fournisseur dans le MarketScape IDC. Bien que chaque fournisseur soit évalué selon les critères

décrits dans l'Annexe, les informations présentées dans cette section permettent d'avoir un résumé des atouts et des challenges rencontrés par chaque fournisseur.

## Lexmark

Lexmark se positionne dans la catégorie des leaders dans le MarketScape IDC 2022-2023 portant sur le marché mondial des services et des solutions de sécurité pour systèmes d'impression. Le siège de Lexmark est situé à Lexington, dans le Kentucky, Etats-Unis.

Quelques informations concernant Lexmark :

- **Nombre de salariés** : 7 780
- **Présence géographique** : bureaux en Amérique du Nord, en Asie/Pacifique, dans la région EMEA et en Amérique Latine.
- **Principaux secteurs d'activités ciblés** : santé, finance, éducation, secteur gouvernemental, juridique, retail et industrie
- **Tailles des organisations ciblées** : PME, grandes entreprises, très grandes entreprises
- **Services/solutions évalués** : solutions et services de sécurité pour systèmes d'impression
- **Modèles de commercialisation évalués** : fonctionnalités intégrées aux appareils, solutions autonomes, contrats de services managés de gestion des impressions et des documents (MPDS), services professionnels managés n'entrant pas dans la catégorie des MPDS.
- **Particularités** : Lexmark a une longue expérience sur le marché de l'impression de bureau, via une approche sectorielle, poussant le fournisseur à évoluer vers un modèle davantage centré sur les services et les clients (cette approche a permis à Lexmark de cibler certains secteurs d'activités en proposant une large gamme de solutions et de services qui leur sont adaptés. Simultanément, Lexmark a su tirer parti de son expérience et de son expertise acquises grâce à cette approche pour proposer une gamme complète de solutions d'impression répondant à des besoins communs).
- **Fait intéressant** : Lexmark compte parmi ses clients : 7 des 10 plus grandes banques du monde, 9 des 10 plus grands retailers du monde, 10 des plus grandes chaînes de pharmacies de détail aux États-Unis, 8 des 10 plus industriels mondiaux, et 7 des 10 plus grandes agences fédérales américaines.

## Forces

- **Services cloud sécurisés** : Lexmark a développé l'un des plus vastes portefeuilles de services cloud dans le but d'aider les entreprises à moderniser leur infrastructure d'impression et à migrer vers un modèle as-a-service. Les services cloud de Lexmark sont regroupés dans trois grandes familles : Cloud Print Management, Cloud Fleet Management, et Apps and Connectors. Chacune de ces familles contient des modules proposant des options de connectivité cloud, de services de configuration et de gestion des actifs, de gestion des impressions et de traitements analytiques. Les informations recueillies par tous ces modules donnent une meilleure visibilité sur les pratiques et les workflows d'impression propres à chaque entreprise, permettant d'augmenter le niveau de sécurité et de protection en général, grâce au contrôle des informations et des processus.
- **Sécurisé by design** : Lexmark estime avoir une longueur d'avance dans le domaine de la sécurité des impressions grâce à d'importants investissements en protection des données et des périphériques réalisés depuis 10 ans. La stratégie de sécurité de Lexmark repose sur ce que l'entreprise appelle « Secure by Design », un terme général décrivant son approche systématique pour protéger ses périphériques et les données. Les périphériques Lexmark

sont dotés d'un ensemble de fonctions renforçant leur sécurité physique et leur protection. En complément de son portefeuille de solutions et de services, Lexmark fournit des services de protection complète des périphériques et des firmwares, de gestion de parc, de sécurisation des documents et des données, de formation à la sécurité, de gouvernance, ainsi que des services d'assistance en matière de respect des normes sectorielles et de certifications de sécurité.

- **Politique zero trust** : L'approche de sécurité de Lexmark inclut les infrastructures zero trust, lesquelles ont un rôle essentiel pour les clients faisant face aux nouveaux défis de sécurité découlant des modèles de travail hybride et de l'évolution des environnements de travail. Pour répondre à ce besoin, Lexmark propose des outils de gestion des périphériques et de la conformité, de protection des processus d'exécution et des firmwares, ainsi que des services d'analyse de sécurité et de traitements analytiques. Grâce à ces outils et ces services, Lexmark est en mesure de garantir que les environnements d'impression s'inscrivent dans un cadre global de sécurité zero trust reposant sur les principes suivants : segmentation et compartimentation des données, sécurité des périphériques, ne jamais faire confiance, vérification systématique et accès accordés selon le moindre privilège.
- **Services d'impression managés (MPS) et Lexmark Cloud Bridge** : Lexmark propose une gamme complète de services avancés d'impression, y compris pour les entreprises ayant des besoins spécifiques en fonction de leur taille et de leur secteur d'activité. Dans le cadre de ses programmes MPS, Lexmark fournit des services sécurisés, notamment pour la gestion des actifs, la gestion des consommables, les pannes et les réparations, l'intégration du service d'assistance, des services prédictifs, l'évaluation de la sécurité et la gestion des configurations. La technologie Lexmark Cloud Bridge joue un rôle clé dans la politique générale de Lexmark en matière de MPS. Elle permet en effet à tous les environnements réseaux hybrides de bénéficier des fonctionnalités et des services d'impression les plus avancés. Avec Lexmark Cloud Bridge, les entreprises de toutes tailles peuvent profiter des avantages des MPS de Lexmark en tirant parti du cloud et de l'Internet des objets pour simplifier et optimiser les environnements d'impression.

### *Défis*

- **Go to market** : La stratégie de go to market de Lexmark pourrait bénéficier d'une politique marketing plus ambitieuse afin de renforcer la notoriété de la marque et de positionner l'entreprise comme leader d'opinion sur les sujets de sécurité qu'il couvre, en particulier dans les domaines où elle se distingue comme le cloud, l'IoT et le travail hybride.
- **Renforcement des canaux de distribution** : Lexmark doit continuer à aider ses partenaires distributeurs en leur donnant accès à la large gamme d'outils, de solutions et de services de sécurité que l'entreprise a développés en travaillant directement avec ses clients. Cet aspect est particulièrement important dans la mesure où Lexmark cherche à développer ses activités d'impression as-a-service auprès de PME.

### *Dans quels cas choisir Lexmark ?*

Les entreprises devraient évaluer Lexmark lorsqu'elles souhaitent travailler avec un fournisseur disposant d'une connaissance et d'une expertise approfondie de leur secteur d'activité. Elles devraient également shortlister Lexmark lorsqu'elles souhaitent renforcer la sécurité et répondre aux défis du travail hybride, migrer leur infrastructure d'impression vers le cloud, développer une posture de sécurité forte et évolutive avec le temps, et bénéficier de services cohérents au niveau mondial.

### Comment lire la représentation graphique du MarketScape IDC ?

Pour les besoins de cette analyse, IDC a réparti les facteurs de réussite potentielle des fournisseurs en deux catégories : « capacités » et « stratégies ».

L'axe des ordonnées reflète les capacités et l'étendue des services actuellement proposés par le fournisseur, ainsi que l'adéquation entre sa proposition et les besoins des clients. Il s'agit des « capacités » du fournisseur et de ses produits à l'instant présent et dans le contexte actuel. Au sein de cette catégorie, les analystes d'IDC étudient comment les capacités conçues/offertes par un fournisseur lui permettent de mettre en œuvre sa stratégie.

L'axe des abscisses (l'axe « stratégies ») mesure l'adéquation de la stratégie future du fournisseur avec les exigences des clients d'ici trois à cinq ans. Cette catégorie examine les décisions de haut-niveau et les hypothèses sur lesquelles se fondent les offres, les segments de clients ciblés, ainsi que les programmes commerciaux et les plans de go-to-market pour les trois à cinq prochaines années.

Dans le MarketScape IDC, la taille du marqueur associé à chaque fournisseur est proportionnelle à sa part de marché, sur le segment de marché spécifiquement étudié.

### Méthodologie utilisée pour le MarketScape IDC

Les critères de sélection, les pondérations et les notes attribuées aux fournisseurs dans le cadre de ce MarketScape expriment une appréciation d'IDC fondée sur une analyse approfondie du marché et de certains fournisseurs en particulier. Les analystes d'IDC adaptent les critères d'évaluation utilisés en fonction des échanges, des enquêtes et des entretiens structurés conduits auprès d'entreprises leaders du marché, de divers participants et d'utilisateurs finaux. Les pondérations de marché sont basées sur des entretiens avec des utilisateurs, des enquêtes réalisées auprès d'acheteurs et des informations de marché fournies par les experts d'IDC. Les analystes d'IDC déterminent les notes individuelles attribuées à chaque fournisseur, ainsi que le classement sur le MarketScape, en fonction des enquêtes et des entretiens approfondis conduits auprès des fournisseurs, des informations publiques disponibles et des expériences des utilisateurs finaux. Les données recueillies permettent de procéder à une évaluation précise et cohérente des caractéristiques, des pratiques et des capacités de chaque fournisseur.

### Définition du marché

Pour les besoins de ce MarketScape 2022-2023, IDC définit les services de sécurité des impressions et des documents comme « des solutions et des services répondant aux préoccupations en matière de sécurité liées à l'infrastructure d'impression et de gestion des documents, qu'il s'agisse de solutions offrant des capacités et des fonctionnalités de sécurité pour les périphériques, de solutions logicielles, ou de services professionnels et managés permettant d'évaluer, de détecter et d'éliminer les risques liés aux menaces de sécurité ».

Ce MarketScape IDC s'appuie sur des mesures permettant d'évaluer la sécurité des périphériques ainsi que la protection des données/contenus. Les capacités évaluées sont notamment les suivantes :

- Gestion des identités et des accès
- Politiques de chiffrement et meilleures pratiques
- Protection des appareils contre les malwares

- Mise à jour des BIOS, des systèmes d'exploitation et des firmwares, et gestion des mots de passe
- Disques durs et dispositifs de stockage amovibles
- Antivirus, antimalware/spyware
- Gestion des événements de sécurité
- Surveillance et gestion permanente des systèmes de détection des intrusions et des pare-feu
- Supervision des correctifs et des mises à jour
- Évaluation et audit de sécurité
- Sécurité, confidentialité et intégrité des données (au niveau du matériel et des logiciels)
- Installation, configuration et utilisation des équipements
- Impression mobile, à distance et avec des appareils personnels (BYOD)

Les solutions de sécurité proposées par les fournisseurs de systèmes d'impression peuvent être composées de logiciels, de matériel et de services professionnels ou managés.

Les services de sécurité peuvent inclure des services de conseil ou de mise en œuvre (services professionnels et managés), y compris pour l'audit et l'évaluation de la sécurité des impressions et des documents ; la gestion des événements et des politiques de sécurité ; la surveillance en continu et la gestion des systèmes de détection des intrusions et des pare-feu ; la supervision des correctifs et des mises à jour ; la sécurité, la confidentialité et l'intégrité des données (au repos ou en mouvement) ; l'installation, la configuration et l'utilisation d'équipements ; et la sécurité des systèmes utilisés pour les impressions mobiles, à distance et avec des appareils personnels (BYOD). L'intégration avec les systèmes historiques des entreprises et la prise en charge des futures politiques de conformité réglementaire sont également prises en considération.

## EN SAVOIR PLUS

---

### Études en rapport avec le présent document

- *IDC FutureScape: Worldwide Imaging, Printing, and Document Solutions 2023 Predictions* (IDC n° US49751022, octobre 2022)
- *Market Analysis Perspective: Worldwide Next-Gen Document Services, 2022* (IDC n° US49326522, août 2022)
- *Worldwide and U.S. Managed Print and Document Services and Basic Print Services Forecast, 2022- 2026* (IDC n° US47975222, juillet 2022)
- *Worldwide and U.S. Managed Print and Document Services and Basic Print Services Market Shares, 2021: Hybrid Work Drives Cloud Adoption* (IDC n° US48532922, juillet 2022)
- *Enabling a New Print Services Model for the Hybrid Workforce, Part 3: Security and Zero Trust* (IDC n° US49104022, mai 2022)

### En résumé

Cette étude réalisée par IDC analyse le marché des services et des solutions de sécurité des impressions et des documents, proposés par les plus grands fournisseurs de systèmes d'impression. Elle identifie les forces de ces différents acteurs ainsi que les défis auxquels ils sont confrontés. Pour cela, elle examine les critères quantitatifs et qualitatifs qui conditionnent le succès de ces fournisseurs sur ce segment de marché. Cette étude IDC repose sur un cadre d'évaluation des outils de sécurité

fournis sous forme de fonctionnalités ou de solutions autonomes, dans le cadre d'un contrat MPDS, ou sous forme de services professionnels managés n'entrant pas dans la catégorie des MPDS.

« Les entreprises ont besoin d'aide pour mieux comprendre comment les modèles de travail hybride affectent la sécurité des impressions et des documents », estime Robert Palmer, research vice president Imaging, Printing, and Document Solutions group chez IDC. L'écosystème de l'impression souffre de nombreuses vulnérabilités en matière de sécurité qui ne font que s'aggraver lorsque des périphériques distants y sont intégrés. Par conséquent, les entreprises doivent se pencher sur les questions de la sécurité des périphériques, de la protection des données et des politiques zéro trust.

## À propos d'IDC

IDC est un acteur majeur de la recherche, du conseil et de l'événementiel sur les marchés des technologies de l'information, des télécommunications et des technologies grand public. IDC aide les professionnels évoluant sur les marchés IT et les investisseurs à prendre des décisions stratégiques basées sur des données factuelles. Plus de 1 100 analystes d'IDC proposent leur expertise globale, régionale et locale sur les opportunités et les tendances technologiques dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC propose des analyses stratégiques pour aider ses clients à atteindre leurs objectifs. IDC est une filiale d'IDG, leader mondial dans les domaines des médias, de la recherche et des événements liés à la technologie.

## Siège social mondial :

140 Kendrick Street  
Building B  
Needham, MA 02494, États-Unis  
États-Unis  
+1.508.872.8200  
Twitter : @IDC  
blogs.idc.com  
www.idc.com

---

Copyright et marques de commerce

Ce document d'étude d'IDC a été publié dans le cadre d'un service de veille continue d'IDC proposant des études écrites, des interactions avec des analystes, des télébriefings et des conférences. Consultez le site [www.idc.com](http://www.idc.com) pour en savoir plus sur les services d'abonnement et de conseil d'IDC. Pour consulter la liste des bureaux d'IDC dans le monde, rendez-vous à l'adresse [www.idc.com/offices](http://www.idc.com/offices). Vous pouvez contacter la hotline d'IDC au 800.343.4952, poste 7988, depuis les États-Unis (ou au +1.508.988.7988 depuis les autres pays) ou en écrivant à l'adresse [sales@idc.com](mailto:sales@idc.com) pour obtenir des informations sur les modalités tarifaires entre ce document et un service d'IDC, ou pour savoir comment obtenir des copies supplémentaires ou des informations sur les droits Internet. IDC et IDC MarketScape sont des marques de commerce d'International Data Group, Inc.

Copyright 2023 IDC. Toute reproduction sans autorisation écrite est strictement interdite. Tous droits réservés.

