IDC MarketScape

IDC MarketScape : Évaluation mondiale des solutions et services de sécurité liés à l'impression proposés par les fournisseurs de systèmes (2019-2020)

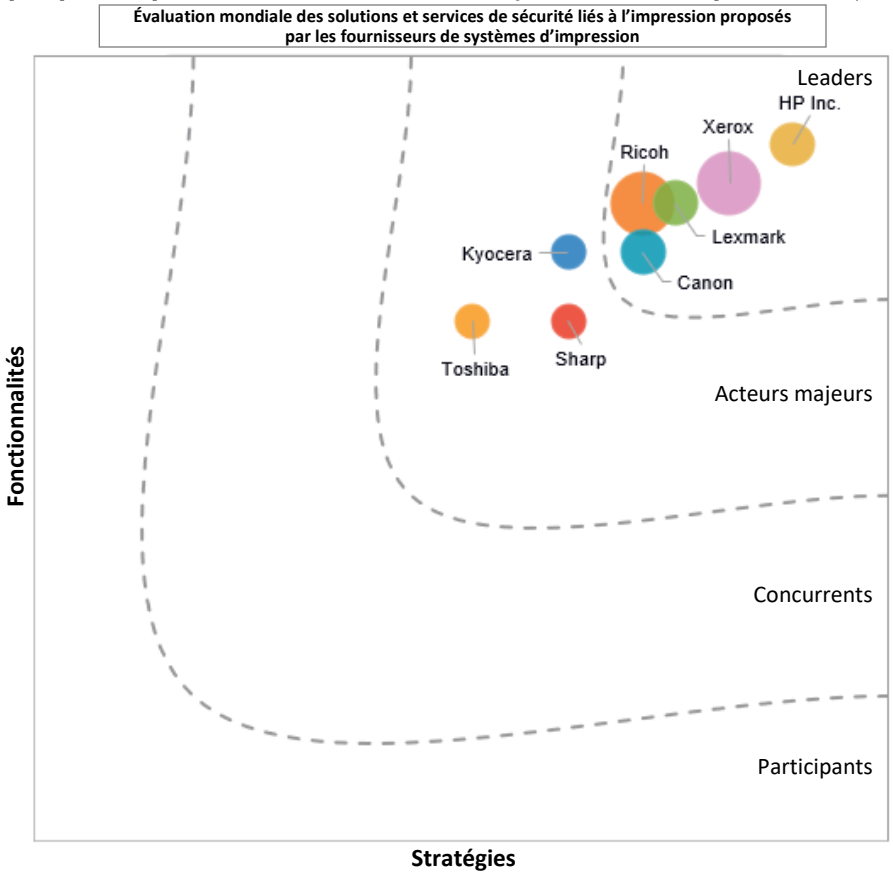
Robert Palmer Allison Correia

CET EXTRAIT DE L'ÉTUDE IDC MARKETSCAPE CONCERNE LEXMARK.

GRAPHIQUE IDC MARKETSCAPE

GRAPHIQUE 1

Évaluation mondiale des solutions et services de sécurité liés à l'impression proposés par les fournisseurs de systèmes d'impression (2019-2020)



Source : IDC 2019

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

Décembre 2019, IDC N° US44811119e

DANS CET EXTRAIT

Cet extrait est directement tiré de l'étude IDC MarketScape : Worldwide Security Solutions and Services Hardcopy 2019–2020 Vendor Assessment (doc. N° US44811119). Les sections mentionnées ci-après figurent en partie ou en totalité dans cet extrait : Le point de vue d'IDC ; Critères d'inclusion des fournisseurs dans l'IDC MarketScape ; Annexe et En savoir plus. Le graphique 1 a également été repris.

LE POINT DE VUE D'IDC

Cette étude d'IDC se base sur le modèle IDC MarketScape pour analyser le marché des services et solutions de sécurisation des impressions et documents proposés par une sélection de fournisseurs de systèmes d'impression sur papier. Elle examine les critères quantitatifs et qualitatifs qui conditionnent le succès de ces fournisseurs sur ce segment de marché. Cette étude IDC MarketScape porte sur divers fournisseurs de systèmes d'impression sur papier et se base sur un mécanisme d'évaluation approfondi des moyens de sécurisation fournis à travers des fonctionnalités et des solutions autonomes, au travers d'un contrat d'infogérance (MPDS) pour les services d'impression et documentaires ou d'autres types de contrats d'infogérance. De nombreux fournisseurs de systèmes d'impression sur papier proposent des solutions et des services de sécurisation des impressions et des documents dans le cadre de leurs services d'infogérance, tout en développant parallèlement des solutions indépendantes (ou complémentaires) de ces services. À l'aide de cette étude IDC MarketScape, les entreprises pourront identifier les fournisseurs offrant des solutions et des services de qualité et s'appuyant sur des stratégies commerciales bien intégrées qui leur permettront de pérenniser leurs activités et de rester compétitifs dans la durée. L'étude a permis de faire ressortir les caractéristiques et facteurs stratégiques conditionnant le succès de ces fournisseurs :

- Un important portefeuille actuel de solutions, avec des fonctionnalités de sécurité intégrées aux appareils, des services professionnels d'infogérance ainsi que d'autres capacités permettant de répondre aux préoccupations de sécurité liées à l'infrastructure d'impression et documentaire.
- Des compétences de base permettant d'évaluer le niveau des menaces et de détecter et d'éliminer les risques.
- Une capacité à proposer des solutions spécifiques aux entreprises pour sécuriser leur infrastructure d'impression et documentaire.
- Des compétences pour permettre au client une mise en conformité en matière de sécurité tout en respectant les principales normes sectorielles dans ce domaine.
- Une adaptabilité à des secteurs d'activités généraux et spécialisés via des circuits de distribution directs et indirects.
- Des services uniformes sur le plan local, régional et mondial s'inscrivant dans une démarche d'excellence en matière opérationnelle.
- L'extension continue de ses activités à de nouveaux secteurs géographiques, de nouveaux secteurs d'activité et de nouvelles applications métiers.
- Des modèles de service, de tarification et de facturation flexibles, ainsi que des solutions adaptées aux infrastructures sur site et cloud (public et privé).

CRITERES D'INTEGRATION DES FOURNISSEURS A L'IDC MARKETSCAPE

Ce document analyse huit grands fabricants d'équipements d'impression sur papier qui disposent d'un large portefeuille permettant de répondre aux besoins spécifiques de différents départements/groupes de travail. Les fournisseurs doivent proposer un large panel de solutions/services de sécurité indépendants du matériel et y allouer une partie importante de leur budget de R&D. En raison de ces impératifs, certains fournisseurs de solutions d'impression et d'imagerie ont été exclus de l'étude malgré un poids de chiffre d'affaires conséquent sur le marché. Le périmètre va également exclure les sociétés spécialisées dans l'externalisation de services informatiques ou de processus métiers, ainsi que les éditeurs de logiciels proposant des services d'impression, de sécurité et documentaires ou sous-traitant ces services auprès de fabricants de systèmes d'impression. Il en est de même pour les partenaires de distribution indirecte des fabricants de systèmes d'impression sur papier.

CONSEILS POUR LES ACHETEURS DE SOLUTIONS TECHNOLOGIQUES

Si la sécurité reste l'une des préoccupations majeures des entreprises, toutes tailles comprises, l'étude d'IDC montre que la plupart d'entre elles n'accordent pas la même importance si nous parlons de sécurité informatique ou de sécurité des impressions/documents. Ainsi, nombreux sont les responsables de la sécurité des systèmes d'information et responsables informatiques ayant 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, et chaque périphérique connecté constitue désormais un risque de sécurité en bout de chaîne, y compris les imprimantes et les périphériques multifonction.

Les conséquences d'une faille de sécurité affectant les matériels d'impression sont similaires à toute autre faille critique : des coûts importants résultant des interruptions de services nécessaires pour identifier et réparer ces failles, des amendes pour défaut de conformité à la gouvernance d'entreprise ou à la réglementation, des pertes de clients et un préjudice pour la réputation de l'entreprise.

Aujourd'hui, le niveau de risque de l'infrastructure informatique est égal à celui de son élément le plus à risque, qui est dans de nombreux cas l'infrastructure autour du matériel d'impression. Cela étant, les périphériques de bureau multifonction peuvent être considérés au travers de deux prismes : d'un côté, ces appareils constituent une menace en tant que dispositif connecté non contrôlé. Mais ils peuvent être exploités comme des dispositifs positionnés en première ligne pour sécuriser les accès au réseau, gérer la sécurité des contenus et protéger l'accès aux informations. Beaucoup d'entreprises se sont heurtées à des difficultés lorsqu'elles ont voulu définir une stratégie de sécurisation des impressions.

Pour cette raison, nous suggérons aux entreprises de prendre en considération les recommandations suivantes :

- **Analysez le niveau de complexité que la sécurité des impressions et des documents est susceptible d'impliquer au cours des trois prochaines années.** Les fonctionnalités de protection des terminaux conçues pour les périphériques d'impression sont de plus en plus courantes. Cependant, les entreprises qui souhaitent mettre en place une stratégie complète de sécurisation de leur infrastructure d'impression devraient plutôt se tourner vers des solutions et des services permettant d'étendre les mesures de protection bien au-delà des périphériques.

- **Cherchez à bien appréhender votre environnement actuel.** Examinez votre infrastructure d'impression actuelle afin d'identifier les risques de sécurité auxquels elle est exposée ainsi que ses vulnérabilités. Pour cela, il peut être nécessaire de faire appel à des services d'audit et d'évaluation dans le cadre général de votre stratégie de sécurité informatique.
- **Inscrivez la sécurité des impressions à l'agenda de votre stratégie globale de sécurité informatique.** Élaborez un plan à long terme avec des indicateurs permettant de mesurer la gestion et la surveillance continues des programmes de sécurité des impressions et des documents. Les fournisseurs proposent une large gamme de services de protection des périphériques et des données dont beaucoup s'intègrent aux systèmes de gestion de contenu d'entreprise (ECM) en place afin de fournir une protection supplémentaire et satisfaire aux exigences de gouvernance.
- **Adressez-vous à votre fournisseur de systèmes d'impression.** Lorsque vous analyserez vos besoins de sécurisation des impressions et des documents, échangez avec votre fournisseur actuel sur le sujet. Il est fort probable qu'il dispose d'un ensemble de solutions et de services adaptés à vos besoins ainsi que d'une feuille de route claire prévoyant l'intégration de ces technologies.
- **Identifiez les besoins en sécurité spécifiques à votre secteur d'activité.** Les besoins en matière de sécurité ainsi que les exigences de conformité réglementaire varient considérablement en fonction du secteur d'activité. Recherchez un fournisseur qui non seulement sera compétent dans la gestion des processus d'impression et documentaires, la gestion des contenus et la sécurisation des services d'impression, mais répondra également aux besoins propres à vos activités.
- **Identifiez vos besoins de services selon vos contraintes organisationnelles.** Vous pouvez, par exemple, avoir besoin de prendre en charge des services cloud ou une plateforme en tant que service et ainsi harmoniser vos solutions et services.

PROFIL DU FOURNISSEUR

Cette section présente brièvement les principales constatations d'IDC ayant permis de déterminer la position du fournisseur dans l'IDC MarketScape. Outre l'évaluation de chaque fournisseur selon les critères énoncés dans l'Annexe de ce document, cette section résume les forces du fournisseur ainsi que les défis auxquels il doit faire face.

Lexmark

Lexmark occupe une position de leader dans l'étude mondiale d'IDC MarketScape 2019-2020 sur les solutions et services de sécurisation des impressions et des documents.

Lexmark est une société basée aux États-Unis. Son siège social se situe à Lexington, dans le Kentucky. En développant son concept « Full Spectrum Security » (la sécurité à tous les niveaux), Lexmark a opté pour une approche globale et systématique de la protection de l'infrastructure d'impression et documentaire qui inclut la sécurité matérielle, l'intégration de la sécurité dans les processus de développement, la gestion des risques liés à la chaîne d'approvisionnement et la gouvernance d'entreprise. La sécurité à tous les niveaux implique en premier lieu l'emploi de technologies et de solutions permettant de protéger les périphériques, les données, le réseau, les utilisateurs, les outils, les services et les applications, en respectant un processus de développement intégrant la sécurité dès la conception, ce que Lexmark appelle « Secure by design ». Lexmark affirme que la sécurité est intégrée par essence à ses produits et ses solutions dès leur conception initiale, puis au cours des phases de développement, de fabrication et de distribution. La politique de Lexmark

consiste à préconiser, valider et implémenter le niveau de protection nécessaire pour satisfaire aux exigences à court et long terme de ses clients en matière de sécurité.

Les moyens utilisés par Lexmark pour protéger les périphériques contre les vecteurs d'attaque potentiels sont variés et comprennent des fonctionnalités d'authentification basée sur les rôles, accessibles depuis un tableau de contrôle et l'intégration des systèmes. L'entreprise a également prévu de nombreuses fonctionnalités de protection des données stockées sur ses périphériques : écrasement et chiffrement des données, effacement lors de la mise hors service des périphériques, autres politiques/services de gestion associés à la fin de vie des produits.

Lexmark dispose également d'un large éventail de solutions de sécurité composé de ses propres produits et d'outils d'intégration de diverses applications tierces. Lexmark Print Management (LPM) est la principale solution sur site de l'entreprise. Elle permet de contrôler les accès sécurisés aux équipements des utilisateurs de l'entreprise. LPM est une plateforme unifiée permettant d'imprimer de façon sécurisée en mode « pull » depuis des appareils mobiles, ainsi que des ordinateurs de bureau ou portables. LPM repose sur trois composantes principales (la libération des tâches d'impression, la comptabilisation des documents et l'impression mobile) qui jouent un rôle clé dans le dispositif de sécurisation de la gestion des impressions proposé par Lexmark.

L'approche retenue par Lexmark pour sécuriser les impressions et les documents s'appuie également sur des technologies cloud. Dans ce domaine, Lexmark a notamment lancé sa plateforme en tant que service appelée Cloud Print Infrastructure (CPI) en début d'année. Proposée sous la forme d'une solution en tant que service adossée à un abonnement, la plateforme CPI permet aux entreprises d'externaliser en totalité la prise en charge de leurs besoins en matière d'impression, en évitant ainsi d'acheter et de gérer diverses composantes individuelles d'une infrastructure d'impression. Grâce à ses équipements prêts pour l'Internet des objets (IoT), Lexmark offre la possibilité à ses clients de supprimer leurs serveurs d'impression installés sur site et d'opter pour une solution d'impression totalement externalisée basée sur un modèle de facturation à l'usage. Outre ces avantages, la plateforme CPI de Lexmark contribue à uniformiser le parc de périphériques d'impression tout en éliminant les risques auxquels sont exposés les serveurs lorsqu'il existe des firmwares, des systèmes d'exploitation et des correctifs de sécurité qui ne sont pas à jour.

À l'appui de ses produits et solutions, Lexmark propose différents services liés à la sécurité. L'objectif de ces services consiste notamment à aider les entreprises à évaluer et comprendre les menaces, à établir des comparaisons avec les meilleures pratiques et à orienter leurs décisions afin de limiter les risques. Lexmark continue à travailler sur l'intégration de ses services de sécurité à ses programmes d'infogérance tout en étoffant son équipe d'experts de la sécurité pour développer ses activités d'implémentation sur mesure. Parallèlement, l'entreprise poursuit sa politique de partenariat avec les plus grands fournisseurs d'outils et de services de sécurité afin de renforcer son offre et proposer un ensemble cohérent de fonctionnalités de sécurité pour toute sa gamme de produits.

Forces

Lexmark s'appuie sur un large ensemble d'outils, de services, de données, d'appareils et de technologies réseau afin de couvrir tout l'environnement de l'entreprise. Cette approche globale s'inscrit dans une logique de sécurité systémique englobant les appareils, le parc d'impression et l'infrastructure réseau. La stratégie de Lexmark consiste avant tout à bien appréhender tous les aspects de la sécurité propres aux environnements de ses clients afin d'élaborer un programme de sécurité en phase avec les objectifs organisationnels, les contraintes humaines, les composantes réseau, les vulnérabilités et l'architecture réseau de chacun d'entre eux. Pour Lexmark, il est important

de disposer de solutions propriétaires, mais le renforcement de son expertise et de ses partenariats l'aidera également à affirmer sa position sur le marché.

L'entreprise persiste dans son approche spécialisée du marché, et sa capacité à concevoir et tirer parti de solutions dédiées à des secteurs spécifiques contribue à la différencier de ses concurrentes. La majorité des solutions de sécurité de Lexmark peuvent être installées sur site ou sont accessibles à distance via le cloud. Dans ce deuxième cas de figure, plusieurs formules sont possibles : achat de licence, abonnement ou formules de facturation de type SaaS. Lexmark continue à enrichir son catalogue cloud afin de proposer des solutions et des services de sécurisation des impressions/documents permettant aux entreprises de toute taille d'évoluer facilement vers une stratégie plaçant le cloud en priorité (stratégie dite « cloud-first »). Les services professionnels de Lexmark reposent sur un vaste réseau mondial de consultants, d'ingénieurs système intervenant sur site et d'experts. Tous sont spécialisés, formés et certifiés dans le domaine de la sécurité. L'expertise sectorielle et technologique de Lexmark, ainsi que l'uniformité de ses services dans le monde permettent à Lexmark d'occuper une position pertinente sur le marché en pleine évolution des solutions de sécurisation des impressions et des documents.

Défis

IDC estime que Lexmark doit poursuivre ses efforts visant à développer des partenariats et des alliances pour renforcer et étendre sa gamme de produits. En outre, le plan de commercialisation de ses produits pourrait être amélioré à l'aide de programmes marketing de sensibilisation à ses stratégies et solutions de sécurité mettant l'accent sur sa politique d'investissements réguliers dans le cloud, les capacités de ses équipements en matière d'IoT et son infrastructure d'impression en tant que service.

Pourquoi faire appel à Lexmark ?

Les entreprises devraient se pencher sur les offres de Lexmark si elles recherchent un fournisseur qui connaît parfaitement le secteur, propose des solutions uniformes à l'échelle mondiale et est en mesure de concevoir un programme / une politique de sécurité répondant à des objectifs organisationnels, des contraintes humaines, des composantes réseau, des vulnérabilités et des architectures réseau spécifiques. Lexmark fait partie des rares fournisseurs susceptibles de satisfaire les entreprises qui souhaitent mettre en œuvre une stratégie de sécurité s'inscrivant dans le cadre d'un projet informatique plus large, tout en bénéficiant d'un maximum d'options de modèles de tarification et de prestations de services.

ANNEXE

Conseils pour la lecture du graphique IDC MarketScape

Pour son analyse, IDC a classé les facteurs clefs de succès en deux catégories : capacités d'un côté, stratégies de l'autre.

Le positionnement sur l'axe des ordonnées (capabilities) reflète les capacités et le panel de services actuels du fournisseur, ainsi que son alignement par rapport aux attentes des clients. Cette catégorie se concentre sur les capacités et produits de l'entreprise à l'heure actuelle. Ainsi, les experts d'IDC analysent les outils de chaque fournisseur et si ceux-ci lui permettent de mettre en œuvre la stratégie choisie sur le marché.

Le positionnement sur l'axe des abscisses (strategies) indique la qualité de l'alignement du fournisseur avec les attentes des clients à l'horizon trois à cinq ans. Pour cela, les experts ont analysé les grandes décisions et orientations en matière d'offres, de segments de clientèle et de plans de commercialisation sur les trois à cinq prochaines années.

La taille du marqueur individuel de chaque fournisseur dans le graphique représente sa part de marché sur le segment évalué, ici les services d'infogérance pour les impressions et les documents (MPDS).

Méthodologie utilisée pour l'étude IDC MarketScape

La sélection des critères, les pondérations et scores des fournisseurs illustrent les résultats de l'analyse avancée réalisée par IDC sur les marchés et fournisseurs présélectionnés. Ces résultats proviennent d'échanges, sondages et interviews réalisés avec les leaders de marché, les participants et les utilisateurs finaux. Les pondérations sont basées sur les interviews utilisateurs, les sondages acheteurs et l'apport des experts IDC sur chaque marché. Les analystes se sont appuyés sur les sondages et interviews avec les fournisseurs, les informations disponibles au grand public et les expériences des utilisateurs finaux afin de fournir une évaluation précise et cohérente des caractéristiques, comportements et capacités de chaque fournisseur et positionner chacun d'eux sur le graphique.

Définition du marché

Pour les besoins de cette étude mondiale IDC MarketScape 2019 sur les services de sécurité des impressions, IDC définit les services de sécurité des impressions et des documents comme des « solutions et services répondant aux enjeux de sécurité liés à l'infrastructure d'impression intégrant les fonctionnalités associées aux périphériques, ainsi que les solutions logicielles ou les services professionnels et d'infogérance permettant l'évaluation des menaces et la détection et l'élimination des risques ».

Cette étude IDC MarketScape tient compte de mesures permettant d'évaluer la sécurité des terminaux ainsi que la protection des données/contenus. Les caractéristiques étudiées sont notamment les suivantes :

- Authentification et accès autorisé des utilisateurs
- Gestion des appareils
- Protection des appareils contre les malwares
- Mise à jour des BIOS, des systèmes d'exploitation et des firmwares, et gestion des mots de passe
- Protection des disques durs ou des dispositifs de stockage amovibles
- Antivirus et antimalware/spyware
- Gestion des événements de sécurité (Security Event)
- Surveillance et gestion permanente des systèmes de détection des intrusions et des pare-feu
- Gestion 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

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

Les services de sécurité peuvent inclure des services de conseil ou de mise en œuvre (services professionnels ou d'infogérance), y compris des audits et des évaluations de la sécurité des impressions et des documents ; la gestion des événements et des politiques de sécurité ; la surveillance permanente 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 des équipements ; et la sécurité des systèmes utilisés pour les impressions mobiles, à distance et avec des appareils personnels. Les possibilités d'intégration avec les systèmes utilisés pour gérer les métiers et la possibilité de prendre en charge les futures politiques de conformité réglementaire sont également prises en considération.

EN SAVOIR PLUS

Documents de recherches associés

- *IDC FutureScape : Worldwide Imaging, Printing, and Document Solutions and 3D Printing 2020 Predictions* (IDC N° US45586119, octobre 2019)
- *Market Analysis Perspective: Worldwide and U.S. Next-Gen Document Services, 2019* (IDC N° US44634019, septembre 2019)
- *Worldwide and U.S. Managed Print and Document Services and Basic Print Services Market Shares, 2018: Why the Channel Matters* (IDC N° US43832819, juillet 2019)
- *Worldwide and U.S. Managed Print and Document Services and Basic Print Services Forecast, 2019-2023* (IDC N° US45237919, juillet 2019)

Synopsis

Cette étude d'IDC analyse le marché des services et solutions de sécurisation des impressions et des documents proposés par les plus grands fournisseurs de systèmes d'impression, tout en identifiant leurs forces et les défis auxquels ils sont confrontés. Elle examine les critères quantitatifs et qualitatifs qui conditionnent le succès de ces fournisseurs sur ce segment de marché. Cette étude IDC se base sur un mécanisme d'évaluation approfondi des moyens de sécurisation fournis à travers des fonctionnalités et des solutions autonomes, des contrats d'infogérance pour les services d'impression et documentaires ou d'autres types de contrats d'infogérance.

« Les questions de sécurité liées à l'infrastructure d'impression et documentaire restent un problème majeur pour la plupart des entreprises », explique Robert Palmer, vice-président de la recherche du groupe Imaging, Printing, and Document Solutions. « Les fournisseurs de systèmes d'impression ont beaucoup progressé pour aider les entreprises à limiter leurs vulnérabilités en intégrant des systèmes de protection aux périphériques et en proposant des services étendus permettant de contrôler les accès, superviser les comportements des utilisateurs, protéger les informations critiques et assurer le respect permanent des politiques de sécurité de l'entreprise ».

À propos d'IDC

International Data Corporation (IDC) est le premier fournisseur mondial de renseignements sur les marchés, de services de conseil et de services événementiels pour les marchés des technologies de l'information, des télécommunications et des technologies dédiées au grand public. IDC aide les professionnels de l'informatique, les dirigeants d'entreprise et la communauté des investisseurs à prendre des décisions qui se fondent sur des faits pour les acquisitions technologiques et la stratégie de l'entreprise. Plus de 1 100 analystes d'IDC apportent leur expertise mondiale, régionale et locale sur les questions d'opportunités technologiques et sectorielles, ainsi que sur les tendances qui se dégagent dans plus de 110 pays à travers le monde. Depuis 50 ans, IDC fournit des informations approfondies stratégiques afin d'aider ses clients à atteindre leurs objectifs commerciaux clés. IDC est une filiale d'IDG, le leader mondial dans le domaine des médias, de la recherche et des événements liés à la technologie.

Siège social mondial :

5 Speen Street
Framingham, MA 01701
États-Unis
+1.508.872.8200
Twitter : @IDC
idc-community.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. Rendez vous sur le site 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. Vous pouvez contacter la hotline d'IDC en téléphonant au 800.343.4952, 7988 depuis l'étranger (ou +1.508.988.7988) ou en écrivant à l'adresse sales@idc.com pour obtenir des informations sur les modalités de déduction du prix de ce document sur le prix d'achat d'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 2019 IDC. Toute reproduction sans autorisation écrite est strictement interdite. Tous droits réservés.