Livre blanc, sponsorisé par DigiCert | Juin 2024

L'évolution de l'entreprise numérique façonne le paysage cryptographique moderne

Jennifer Glenn
Research Director,
Security and Trust Group, IDC

Table of Contents

CLIQUEZ SUR UN TITRE POUR ACCÉDER DIRECTEMENT À LA PAGE CORRESPONDANTE.

Résumé

La transformation numérique est la nouvelle réalité pour la plupart des entreprises. Dans l'enquête d'IDC *Future Enterprise Resiliency and Spending Survey* de janvier 2024, **47 % des personnes interrogées ont indiqué qu'elles étaient principalement des entreprises numériques voire des entreprises « digital-native », i.e. natives du numérique** . L'un des principaux avantages de la transformation numérique d'une entreprise est que les données peuvent être facilement partagées avec un plus grand nombre d'applications, de propriétés Web, d'appareils, de départements et d'utilisateurs. Cela permet aux organisations d'autoriser en toute confiance le travail à distance, de communiquer en toute sécurité tout au long de la chaîne logistique et de créer des services et des produits numériques qui font le bonheur des clients.

La réalité d'une entreprise numérique est qu'elle nécessite un environnement complexe qui combine de multiples infrastructures cloud et des données numériques, ainsi que du matériel et des données hérités pour que les entreprises fonctionnent de manière optimale. En outre, il y a tout simplement plus de tout : plus d'appareils qui communiquent entre eux, plus d'utilisateurs qui accèdent à distance aux ressources de l'entreprise et plus d'applications qui fonctionnent dans différents clouds ou sur site. Le volume et la valeur des données augmentent de façon exponentielle. Le maintien de la sécurité et de l'intégrité de cet environnement complexe, et la protection de tous ces actifs, sont essentiels à la réussite de l'entreprise.

Un bon chiffrement est essentiel pour une sécurité efficace ; la crypto-agilité est essentielle pour un chiffrement efficace

Il existe de nombreuses façons de sécuriser les données au sein de l'entreprise et de son écosystème. Le chiffrement, sous ses différentes formes, est une capacité de sécurité courante permettant de protéger l'intégrité des connexions et des données dans chacun de ces environnements. Par exemple, le chiffrement empêche les utilisateurs non autorisés de consulter les données contenues dans les appareils. Il protège les données des sites Web publics contre toute compromission. Il protège également les données lorsqu'elles sont transférées d'un appareil à l'autre pour des mises à jour logicielles ou des communications entre l'agent logiciel et ses hôtes.

Les organisations peuvent utiliser plusieurs algorithmes de chiffrement pour masquer les données, en particulier lorsqu'elles sont considérées comme confidentielles ou sensibles. Le chiffrement est une composante courante et nécessaire de la sécurité. Dans l'enquête d'IDC *Data Security and Privacy Survey* de mars 2024, près de 80 % des personnes interrogées ont déclaré utiliser le chiffrement comme moyen de protection de la confidentialité (voir **figure 1** page suivante). Le processus de chiffrement et de déchiffrement des informations entre les appareils et/ou les utilisateurs nécessite des technologies supplémentaires pour confirmer la légitimité et l'autorisation.

Ces technologies incluent :

Clés cryptographiques :
La génération et la gestion des clés cryptographiques, qui permettent le chiffrement et le déchiffrement des données par l'entité concernée (utilisateur, appareil, application, etc.).

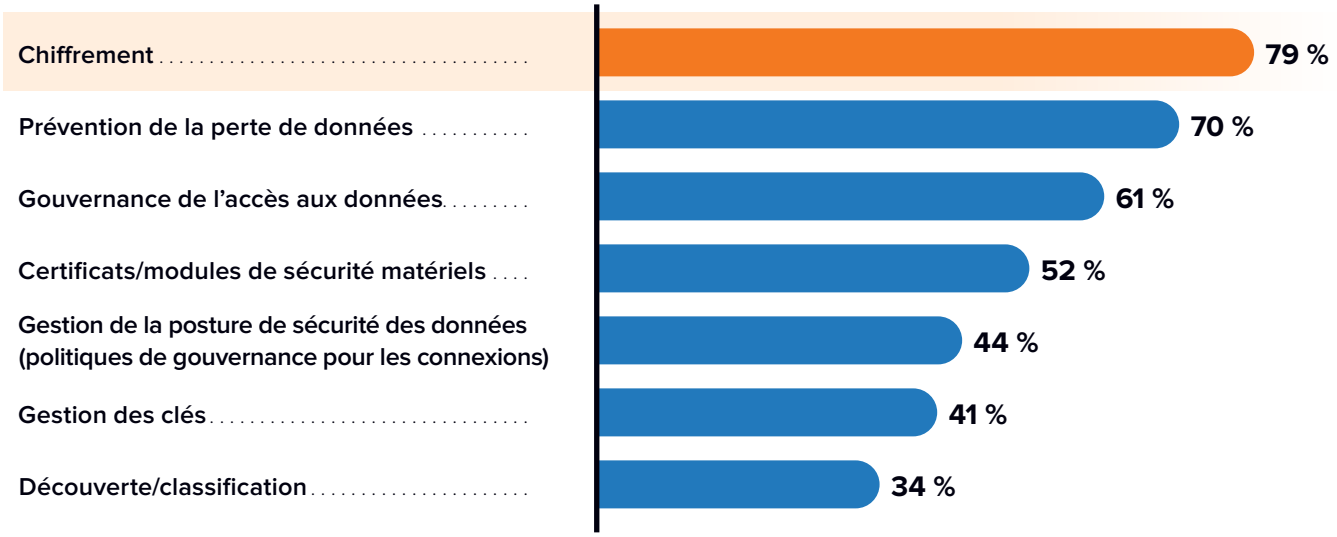
Certificats numériques :
L'association d'une identité à la clé cryptographique pour certifier que la machine, l'application ou l'utilisateur est valide et légitime. (Les certificats sont émis par une autorité de certification [CA] qui utilise des normes industrielles pour valider l'identité d'un utilisateur ou d'une machine. Ces validations sont limitées dans le temps et peuvent expirer ou être révoquées si une clé cryptographique est compromise ou si les normes changent. Une infrastructure à clé publique (PKI) fournit le cadre nécessaire à l'émission de certificats numériques).

GRAPHIQUE 1

Technologies de sécurité des données fréquemment utilisées pour le respect de la confidentialité

Quelles sont les technologies de sécurité des données utilisées pour démontrer le respect de la confidentialité/la conformité ?

(pourcentage des personnes interrogées)



Remarque : les réponses multiples étaient autorisées. n = 619 ; Source : Enquête d'IDC *Data Security and Privacy Survey* de mars 2024

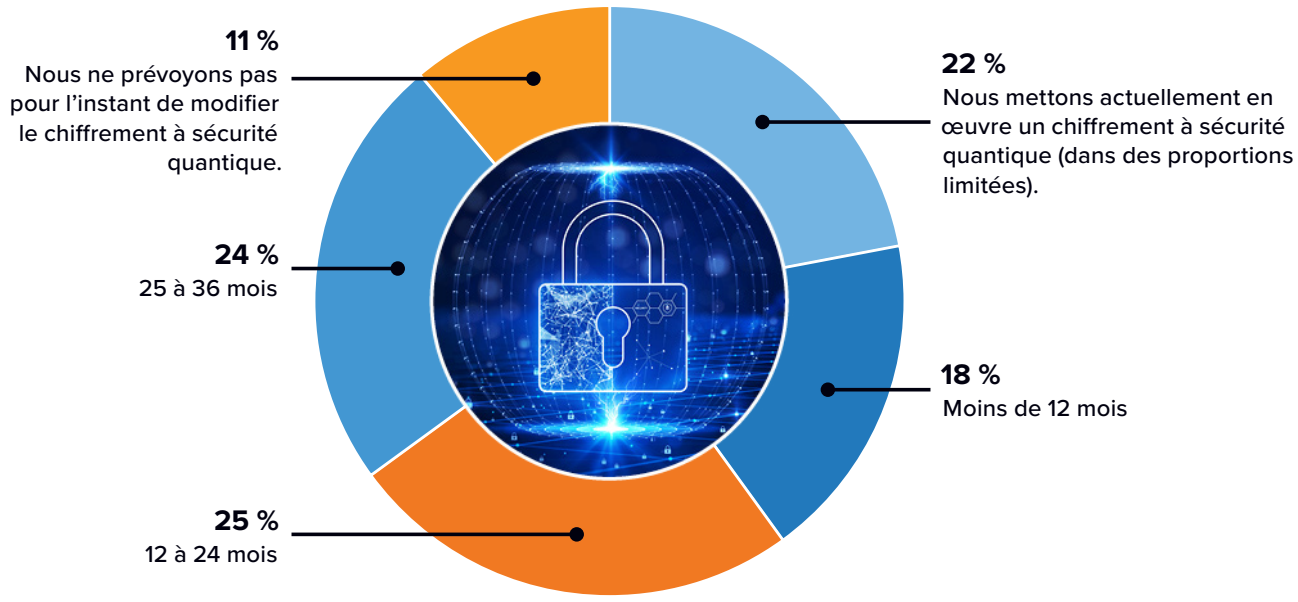
L'ensemble de ce processus joue un rôle important dans l'élaboration de la confiance numérique. Mais, comme l'infrastructure qu'elle protège, elle doit évoluer et se moderniser pour assurer la sécurité des données et des systèmes. Des pirates peuvent tirer parti de processus informatiques plus puissants pour casser les algorithmes de chiffrement. Les normes réglementaires changent. La cryptographie évoluera et progressera. Plus que d'une simple modernisation, les entreprises numériques d'aujourd'hui ont besoin de crypto-agilité.

La crypto-agilité permet aux entreprises d'adapter ou de changer rapidement l'algorithme, les paramètres ou la méthode de chiffrement sans devoir procéder à une refonte majeure de l'infrastructure. Cela sera important car les organisations se préparent à faire face aux vulnérabilités découlant de l'informatique quantique, qui promet une puissance de traitement plus rapide capable de casser les algorithmes de chiffrement existants en quelques secondes. De nombreuses organisations mettent déjà activement en œuvre un chiffrement à sécurité quantique pour assurer la sécurité de ces connexions et de ces données. Dans la même enquête d'IDC *Data Security and Privacy Survey,* 22 % des personnes interrogées ont indiqué qu'elles mettaient actuellement en œuvre un chiffrement à sécurité quantique dans des proportions limitées. Par ailleurs, 18 % des personnes interrogées prévoient de mettre en œuvre un chiffrement à sécurité quantique dans moins d'un an (voir **figure 2**).

GRAPHIQUE 2

La mise en œuvre d'un chiffrement à sécurité quantique est déjà en cours

Quand prévoyez-vous de mettre en œuvre un chiffrement à sécurité quantique au sein de votre organisation ?
(pourcentage des personnes interrogées)



n = 415 ; Source : Enquête d'IDC *Data Security and Privacy Survey* de mars 2024

Outre la préparation à l'informatique quantique, l'adoption de processus intégrant la crypto-agilité peut faciliter la résolution de certains des autres défis qui résultent de la multiplicité des infrastructures cloud et existantes, notamment :

Augmentation du volume de certificats :
Avec la croissance des infrastructures hybrides et multicloud, le nombre de connexions au sein de l'écosystème d'une organisation a augmenté. Ces certificats peuvent avoir des propriétaires différents dans plusieurs départements. Les dates d'expiration varient pour chaque certificat en fonction de son utilisation. En outre, les propriétés Web réduisent le cycle de vie de leurs validations de certificats au nom de la sécurité. Dans le même temps, le souhait de faire preuve de confiance dans ces connexions est également devenu une priorité pour la plupart des entreprises. Au total, cela a ajouté des milliers de certificats et d'attributs à gérer, ce qui rend difficile la connaissance de l'état de chacun d'entre eux.

Dispersion des certificats :
Le passage à des infrastructures multicloud et hybrides crée plus de points de connexion provenant d'un plus grand nombre d'endroits. Les certificats peuvent être exigés par les équipes chargées des produits ainsi que par les groupes chargés des opérations informatiques à des fins différentes. Souvent, ces équipes ne travaillent pas ensemble et peuvent utiliser des autorités de certification différentes. Sans une vue unifiée, la gestion de l'ensemble des processus de chiffrement de l'organisation est pratiquement impossible.

Manque de personnel qualifié/manque de spécialisation des ressources :
La cryptographie est un métier spécialisé qui relève le plus souvent du département informatique. Pour ceux qui ont accepté ce rôle intentionnellement, il peut être difficile de démontrer sa valeur opérationnelle (en dehors du fait qu'il empêche l'expiration des certificats), ce qui conduit à déléguer des tâches supplémentaires à l'employé. Il est également probable que de nombreuses personnes ont hérité du poste suite à des départs. Dans les deux cas, la capacité à gérer efficacement le processus de cryptographie est entravée.

Mise en place d'une infrastructure de confiance numérique moderne

La confiance numérique permet aux organisations de faire preuve de confiance et d'intégrité dans les connexions et les données qu'elles offrent aux clients. La mise en œuvre d'une infrastructure capable de crypto-agilité est un élément essentiel pour garantir la confiance numérique aujourd'hui et à l'avenir.

Pour que la confiance numérique devienne une réalité, il faudra adopter une approche en plusieurs étapes combinant technologie et processus incluant :

Cyber-hygiène :
La base de la crypto-agilité consiste simplement à savoir quels éléments cryptographiques sont en circulation. Il s'agit notamment d'un catalogue des certificats dans l'ensemble de l'entreprise, comprenant leur propriété, leur cycle de vie et leur pertinence. En outre, les organisations doivent comprendre les normes régissant la délivrance de ces certificats et les changements à venir. Comme indiqué précédemment, l'environnement commercial actuel peut rendre cette tâche difficile.

Définir la réussite :
Une fois que l'on sait ce qui doit être géré, l'étape suivante consiste à déterminer ce qu'est la réussite pour l'organisation et à mettre en place les éléments adéquats pour y parvenir. Il s'agit notamment des éléments suivants :

- **Fixation d'objectifs :**
  Déterminer les éléments essentiels au fonctionnement de l'entreprise. Pour beaucoup, il s'agit de la disponibilité du service, ce qui signifie qu'il n'y a pas de pannes dues à l'expiration de certificats. Pour ceux qui ont une présence importante dans le domaine de l'Internet des objets, la réussite consiste à s'assurer que les objets connectés sont mis à jour en toute sécurité. Parmi les autres domaines d'action, citons la sécurité et la validité des produits, ainsi que la sécurité des télétravailleurs.

- **Établir des priorités :**
  Identifier les systèmes/résultats les plus menacés. Compte tenu de l'étendue des actifs cryptographiques qui composent l'entreprise moderne, il est essentiel de définir des priorités. Il peut également s'agir de savoir quels systèmes peuvent être mis à jour rapidement par rapport à ceux qui nécessiteront une refonte importante.

- **Investissement dans les ressources :**
  Planifier et budgétiser les produits, les partenaires et le personnel nécessaires pour effectuer le travail. Le personnel qualifié et le budget sont toujours une préoccupation. Il peut être utile de hiérarchiser les tâches essentielles.

Visibilité et gestion centralisées :
La découverte et la planification de ces actifs sont essentielles, mais la création d'un processus continu pour tout gérer est un élément clé de la crypto-agilité. Rassembler les actifs de l'ensemble de l'organisation dans une vue unique permet de voir ce qui peut manquer, ainsi que l'état, le propriétaire et les besoins de chaque actif.

Rapports et justifications :
Un élément important de tout processus d'entreprise est sa capacité à démontrer sa réussite. Il en va de même pour la crypto-agilité. Le personnel impliqué doit être prêt à partager des données importantes liées à la planification de la réussite, notamment le nombre de pannes évitées et les mesures prises pour réduire les risques au sein des télétravailleurs.

Ajustement :
L'ajustement est un domaine négligé pour la mise en œuvre de la crypto-agilité. L'objectif du processus de crypto-agilité est d'être flexible pour l'entreprise, mais le processus lui-même peut nécessiter quelques ajustements. Sur la base des résultats, où l'organisation doit-elle apporter des changements ? Y a-t-il des redondances ? Existe-t-il des domaines dans lesquels il est possible d'accroître l'efficacité et la sécurité ou de démontrer plus clairement cette sécurité ?

Avantages de la modernisation de l'infrastructure à clé publique/ Crypto-agilité

La crypto-agilité prépare les organisations à l'informatique à sécurité quantique tout en les aidant à atteindre plusieurs autres objectifs, tels que l'automatisation. Comme nous l'avons souligné précédemment, il peut y avoir des centaines de milliers de certificats numériques dans une entreprise, avec des propriétaires, des utilisations, des normes et des cycles de vie différents. La mise en place de processus de crypto-agilité facilite l'automatisation de la découverte, de l'approvisionnement et de la gestion de ces actifs.

L'automatisation des processus manuels présente de nombreux avantages pour l'entreprise, notamment :

Réduction des coûts :
Grâce à une meilleure visibilité, les organisations ont une meilleure idée des certificats et des actifs cryptographiques dont elles disposent. Il s'agit de la première étape de l'élimination des actifs devenus inutiles. En outre, l'automatisation peut aider les organisations à accroître leurs performances avec moins de personnel.

Gain de temps :
Cela permet de gagner directement du temps, notamment en réduisant de plusieurs semaines la durée de l'ensemble du processus. Elle permet également de gagner indirectement du temps en réduisant les interruptions de service qui obligent les équipes à interrompre leurs activités pour régler le problème d'expiration du certificat.

Amélioration de la conformité avec les audits internes et externes :
Les anciennes méthodes de gestion des certificats utilisant des processus manuels et des scripts rendent les organisations vulnérables aux pannes et aux vulnérabilités de sécurité causées par des certificats expirés non découverts. Comme le décrit le document NIST SP 1800-16, l'automatisation de la gestion des cycles de vie des certificats, de la découverte au renouvellement ou à la révocation, est essentielle pour minimiser les risques et maintenir la conformité.

Flexibilité du lieu de travail :
L'automatisation des opérations de confiance numérique telles que la gestion des certificats permet une authentification évolutive, ce qui est essentiel pour la flexibilité du lieu de travail. Grâce à l'authentification avancée sans mot de passe, les entreprises peuvent permettre à leurs employés de travailler de la façon et depuis le lieu qui leur convient sans avoir à se soucier de l'intégrité et de la sécurité de leurs connexions.

Envisager DigiCert pour la modernisation de la confiance numérique

DigiCert, dont le siège se trouve à Lehi, dans l'Utah, est un fournisseur mondial de solutions de confiance numérique. Sa gamme de solutions est conçue pour permettre aux entreprises de construire un avenir à l'abri des menaces quantiques.

DigiCert Trust Lifecycle Manager (TLM) est conçu pour répondre aux besoins à chaque étape de la modernisation du processus cryptographique, à savoir :

Découverte :
La crypto-agilité commence par la connaissance et le contrôle de tous vos actifs. TLM offre une large visibilité sur le paysage cryptographique d'une organisation, que les certificats aient été émis par une autorité de certification publique ou privée. Cela signifie qu'il faut découvrir, cataloguer et fournir des actifs cryptographiques tels que des certificats publics et privés dans l'ensemble de l'organisation. Grâce à ces informations, les organisations sont en mesure d'identifier plus facilement les vulnérabilités, les pratiques inefficaces et les certificats frauduleux.

Gestion :
Un environnement cryptographique agile est proactif dans l'identification des problèmes de sécurité ou d'exploitation. DigiCert TLM comprend des fonctionnalités permettant de gérer le cycle de vie des certificats à partir d'un tableau de bord unique et de réunir les infrastructures à clé publique privées et publiques. Les capacités de gestion comprennent également des critères essentiels de chronologie et d'autorisation, tels que la connaissance de la date d'expiration des certificats et la connaissance de ceux qui doivent être remplacés en raison de l'évolution des normes.

Automatisation :
L'augmentation du nombre d'actifs cryptographiques dans l'entreprise numérique rend l'automatisation nécessaire pour les initiatives de crypto-agilité. DigiCert TLM comprend des modèles et des configurations pour automatiser les flux de travail et les autorisations d'accès aux certificats. En supprimant la charge qui pèse sur les équipes chargées des actifs cryptographiques, ces dernières sont mieux positionnées pour évoluer et faire preuve d'agilité.

DigiCert Trust Lifecycle Manager est un élément central de la plateforme DigiCert ONE pour la confiance numérique. Outre les logiciels, DigiCert propose des services PKI conçus pour fournir aux organisations un environnement complet pour la mise en place, la gestion et la migration des autorités de certification. Cet environnement comprend des modules de sécurité matériels, des politiques prédéfinies, des capacités de révocation et plusieurs types de certificats.

Outre les logiciels, DigiCert propose des services PKI conçus pour fournir aux organisations un environnement complet pour la mise en place, la gestion et la migration des autorités de certification.

Défis et opportunités

La crypto-agilité (et la cryptographie en général) est un concept très technique pour la plupart des organisations. Si les équipes informatiques et de sécurité considèrent que la gestion des certificats est importante, en particulier lorsqu'il s'agit de pannes et de propriété, elles investissent souvent du temps et des ressources dans d'autres initiatives de sécurité qui ont une plus grande visibilité exécutive, telles que le maintien des données sensibles hors des modèles d'IA générative et la lutte contre les rançongiciels.

En ce qui concerne l'informatique quantique et la cryptographie à sécurité quantique, les équipes chargées de la sécurité et de l'informatique auront probablement du mal à justifier les dépenses liées à ces technologies, même en cas d'attaques qui exfiltrent des données dans l'intention de les décrypter ultérieurement. Il faudra encore plusieurs années pour que l'informatique quantique soit mise en œuvre à grande échelle et, bien que des efforts soient déployés pour anticiper les menaces, il est peu probable que l'on passe à grande échelle à des déploiements à sécurité quantique avant qu'une attaque ou une compromission notable ne se produise. Cette lenteur d'adoption pourrait constituer un défi pour les fournisseurs tels que DigiCert, car les organisations cherchent à investir dans d'autres domaines.

Néanmoins, la crypto-agilité ne se limite pas à l'informatique à sécurité quantique. Il s'agit de pouvoir déplacer et ajuster les protections rapidement et facilement. Lorsque l'on évoque les risques liés aux projets à long terme, la crypto-agilité, ou la nécessité de garantir la confiance numérique, est une préoccupation légitime. Pour les équipes qui ont du mal à justifier les dépenses liées au chiffrement résistant à l'informatique quantique, se concentrer sur des approches et des fournisseurs qui offrent des capacités plus approfondies, telles quela crypto-agilité, peut être une opportunité de se préparer à un monde post-quantique tout en répondant à d'autres besoins de l'entreprise.

Conclusion

Le commerce numérique a augmenté de façon exponentielle le nombre de connexions et de données protégées par des algorithmes cryptographiques.

L'augmentation du volume s'accompagne d'une augmentation du risque, non seulement de compromission, mais aussi d'oubli de mises à jour essentielles dans des périodes de surcharge. Ce problème ne fera que s'aggraver au fil du temps, à mesure que les volumes de données continueront d'augmenter et que l'informatique post-quantique portera ses fruits. La modernisation des processus cryptographiques dans un souci d'agilité et d'évolutivité est un élément important pour les entreprises stratégiques. Elle procure un dispositif de sécurité solide et la capacité de s'adapter à l'évolution des normes qui protègent l'infrastructure cryptographique dans un monde post-quantique.

À propos de l’analyste IDC

Jennifer Glenn
Research Director, Security and Trust Group, IDC

Jennifer Glenn est directrice de recherche pour l’IDC Security and Trust Group et est responsable de la pratique de la sécurité de l’information et des données. Jennifer couvre un large éventail de technologies, notamment la sécurité de la messagerie, la gestion des données sensibles, le chiffrement, la tokenisation, la gestion des droits, la gestion des clés et les certificats. Dans le cadre de cette étude, Jennifer démontre le rôle essentiel de la sécurité des données dans les principales stratégies d’entreprise, telles que la consolidation de la confiance des clients et la transformation numérique.

En savoir plus sur Jennifer Glenn

Message du sponsor

digicert®

DigiCert est l'un des principaux fournisseurs mondiaux de confiance numérique, permettant aux particuliers et aux entreprises de s'engager en ligne avec la certitude que leur empreinte dans le monde numérique est sécurisée.

DigiCert ONE, la plateforme de confiance numérique, offre aux organisations une visibilité et un contrôle centralisés sur un large éventail de besoins de confiance publics et privés, sécurisant les sites Web, l'accès et la communication d'entreprise, les logiciels, l'identité, le contenu et les appareils. DigiCert associe son logiciel primé à son leadership industriel en matière de normes, d'assistance et d'opérations. Il est un fournisseur de confiance numérique de premier choix pour les entreprises de premier plan du monde entier.

Pour plus d'informations, visitez le site www.digicert.com

suivez @digicert

IDC Custom Solutions

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

idc.com @idc @idc

International Data Corporation (IDC) est un acteur majeur en matière de veille commerciale, de conseil et d'événementiel sur les marchés des technologies de l'information, des télécommunications et des technologies grand public. Avec l'aide de plus de 1 300 analystes répartis dans le monde, IDC propose une expertise mondiale, régionale et locale sur les opportunités et les tendances technologiques et sectorielles dans plus de 110 pays. Les analyses d'IDC aident les professionnels de l'informatique, les cadres dirigeants et la communauté des investisseurs à prendre des décisions technologiques factuelles et à atteindre leurs principaux objectifs commerciaux.