EXECUTIVE BRIEF

Protection des données unifiée pour les environnements

Sponsorisé par : Symantec

Carla Arend Andrew Buss

Mars 2014

CONTENU DE LA NOTE DE SYNTHÈSE

Cette note de synthèse IDC fait le point sur l'évolution et les défis de la protection des données pour les environnements virtuels. Elle montre en outre comment une solution de protection des données moderne peut permettre aux professionnels de la virtualisation et aux spécialistes du stockage d'assurer le succès de leurs opérations de sauvegarde et surtout de restauration. Les avantages et difficultés de la protection des données en environnements virtuels sont également abordés, ainsi que les meilleures pratiques qui émergent aujourd'hui pour garantir une protection unifiée performante.

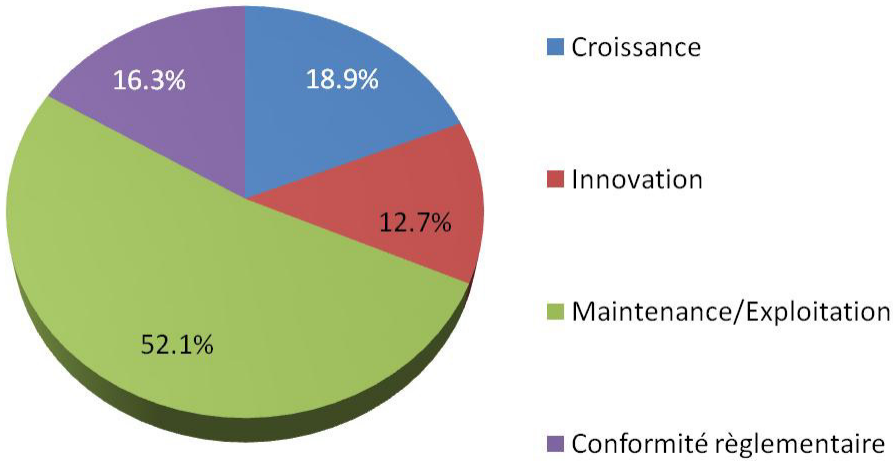
LES NOUVEAUX BESOINS DE L'ENTREPRISE EXIGENT UNE INFRASTRUCTURE IT PLUS AGILE

Le fonctionnement des entreprises a connu une profonde mutation au cours de ces dernières années, la technologie jouant un rôle de plus en plus important dans tous les aspects de leurs activités : développement des produits, gestion de la chaîne d'approvisionnement, fabrication, vente et gestion des stocks, circuits de distribution, gestion de la clientèle. Les cycles d'activité s'accélèrent et l'informatique est fortement sollicitée pour répondre à l'urgence des évolutions technologiques nécessaires.

Ces améliorations requises sur les plans de l'agilité et de la flexibilité ont fortement renforcé les exigences associées à la fonction DSI. Pour relever un tel défi, avec des budgets restant pour l'essentiel inchangés, le DSI doit transformer la façon dont l'informatique est structurée et gérée afin de réduire le coût -traditionnellement élevé- des opérations courantes et d'augmenter les budgets alloués aux investissements, au développement et à l'innovation.

FIGURE 1

Allocation des budgets informatiques en Europe



n = 1 651

Source : Enquête IDC sur les marchés verticaux en Europe, 2013

De réels progrès ont été accomplis dans ce domaine, comme le montre la figure 1, avec une diminution considérable des coûts d'exploitation, en termes réels, au cours de ces dernières années. Ceux-ci pouvaient représenter jusqu'aux trois quarts du budget informatique total il y a quelques années ; mais les améliorations apportées aux outils et processus ont contribué à faire baisser cette proportion jusqu'à la moitié environ.

Dans une récente enquête menée par IDC auprès des DSI, un certain nombre de thèmes ont émergé comme revêtant une importance critique pour permettre à l'infrastructure informatique de répondre au mieux aux exigences de l'entreprise : simplification, innovation, accélération et sécurité. Si l'on prend en compte les investissements requis pour garantir la conformité de l'entreprise, ainsi que sa flexibilité en fonction des objectifs de croissance, on constate que seulement 12,7 % du budget informatique est consacré à des objectifs d'innovation.

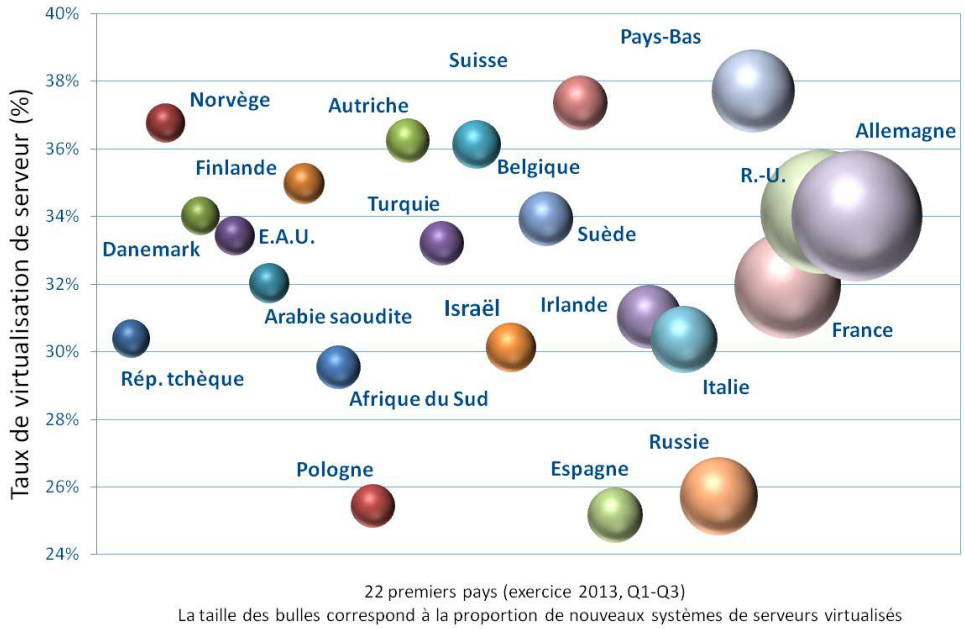
Pour répondre à l'ensemble de ces défis sur les volets métier et IT, et pour augmenter la portion du budget allouée à l'innovation, l'infrastructure informatique doit impérativement gagner en stabilité et en prévisibilité. Elle doit être conçue selon les mêmes modalités que celles d'un service de distribution publique, garantissant un fonctionnement permanent tout en pouvant s'adapter à l'évolution des besoins. La clé du succès d'un tel projet réside dans l'intégration et la gestion des différentes parties de l'infrastructure (serveurs, stockage et réseau, en particulier), de manière à ce qu'elles fonctionnent comme un ensemble homogène. Il est également important que les applications ne soient plus liées à tel ou tel système physique individuel, et puissent au contraire être déployées précisément là où elles seront le plus utiles.

LA VIRTUALISATION : NOUVELLE PIERRE ANGULAIRE DE L'INFRASTRUCTURE INFORMATIQUE

Parmi les nombreuses technologies déployées par les services informatiques pour gagner en agilité et en efficacité, c'est sans doute la virtualisation qui a eu le plus grand impact. Après des débuts relativement lents au début des années 2000, l'intégration des pratiques de virtualisation est aujourd'hui quasiment systématique dans les moyennes et grandes entreprises et tend à se généraliser sur le segment PME. La figure 2 illustre le taux de virtualisation de nouveaux serveurs dans la zone EMEA.

FIGURE 2

Adoption de la virtualisation dans la zone EMEA



22 premiers pays (exercice 2013, Q1-Q3)
La taille des bulles correspond à la proportion de nouveaux systèmes de serveurs virtualisés

Source : IDC 2013

Cette adoption accélérée des pratiques de virtualisation offre de nombreux avantages, en renforçant l'efficacité du hardware utilisé et en accélérant considérablement le déploiement des applications. Elle peut toutefois également engendrer un certain nombre d'effets secondaires qui, s'ils sont négligés, risquent de nuire à la capacité du service informatique à fournir des services performants. La performance de l'architecture risque par exemple d'être imprévisible si différentes machines virtuelles dépendent des mêmes ressources physiques (processeur et mémoire notamment) et si le contrôle des services n'est pas mis en œuvre de façon efficace. Du fait de la grande facilité de création et de déploiement des machines virtuelles (VM), celles-ci risquent de proliférer rapidement, de ponctionner les ressources de calcul et de mémoire au détriment des systèmes de production et des capacités de stockage, si les bibliothèques VM ne sont pas gérées de manière efficace.

Un autre domaine dans lequel les environnements virtuels se développent plus rapidement que l'infrastructure informatique est celui de la protection des données. Traditionnellement, les équipes responsables du stockage assuraient la gestion des efforts de sauvegarde et de restauration pour

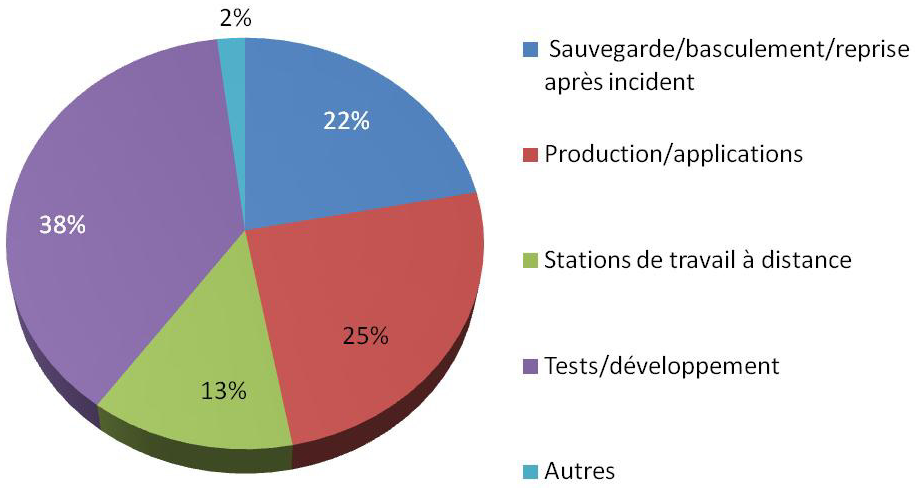
les systèmes physiques. Cette approche fonctionnait bien au temps des systèmes et des applications dédiées ; à l'ère des machines virtuelles, des applications distribuées et du cloud privé, en revanche, le système de sauvegarde doit être renforcé et garantir une protection centrée sur l'information, en plus de l'approche « centrée client » traditionnellement suivie pour les systèmes physiques. Dans la mesure où les infrastructures virtuelles, les applications distribuées et le cloud privé sont des environnements agiles et dynamiques, qui ne dépendent pas d'un hôte physique ou d'une machine virtuelle spécifiques, l'approche suivie en matière de sauvegarde et de restauration doit intégrer de nouvelles méthodologies plus adaptées. Il est généralement contre-productif d'essayer de gérer ces environnements en ayant recours à l'ancienne approche centrée client.

Au début de l'ère de la virtualisation, lorsque les charges de travail portaient essentiellement sur les activités de test et de développement, cela n'était pas aussi problématique. La situation a radicalement changé. Si les tâches de test et de développement constituent toujours la première source d'utilisation de la virtualisation, elles sont en revanche minoritaires pour ce qui est des scénarios de déploiement, ainsi que le montre la figure 3. Les applications de bureau à distance et de production rivalisent désormais avec les tâches de test et de développement. La virtualisation est également fortement mobilisée pour améliorer la fiabilité, la disponibilité et la facilité de maintenance (RAS) de l'infrastructure informatique.

La conséquence d'une telle dépendance vis-à-vis de la virtualisation est que la sécurité des infrastructures virtuelles est désormais aussi importante que la protection des environnements physiques.

FIGURE 3

Utilisation de la virtualisation dans la zone EMEA



n = 2 203 entreprises ayant recours à la virtualisation de serveurs

Source : Enquête auprès des utilisateurs, IDC 2013

DÉFIS POSÉS PAR LES ENVIRONNEMENTS MIXTES EN MATIÈRE DE PROTECTION DES DONNÉES

Cette forte montée en puissance de la virtualisation a fini par renforcer considérablement les responsabilités des administrateurs d'infrastructures virtuelles en matière de protection des données et des infrastructures critiques de l'entreprise. Le rythme rapide des évolutions technologiques a fait que, dans de nombreux cas, les produits traditionnels fondés avant tout sur la protection physique des données ne permettaient de garantir la flexibilité et l'agilité nécessaires pour protéger les nouvelles infrastructures virtuelles.

Des produits ponctuels spécialisés dans la protection des machines virtuelles étaient souvent achetés spécifiquement pour répondre précisément à ce besoin. Ces produits ont été développés pour accompagner les améliorations rendues possibles par la virtualisation, telles la possibilité de restaurer rapidement des machines virtuelles directement à partir d'une sauvegarde réalisée sur un hôte cible sans nécessiter aucun autre traitement complémentaire, ou encore la possibilité de procéder à leur sauvegarde plus efficacement en traitant uniquement les changements identifiés entre une image de machine virtuelle maître et les clones auxquels ont été appliquées certaines mesures de customisation.

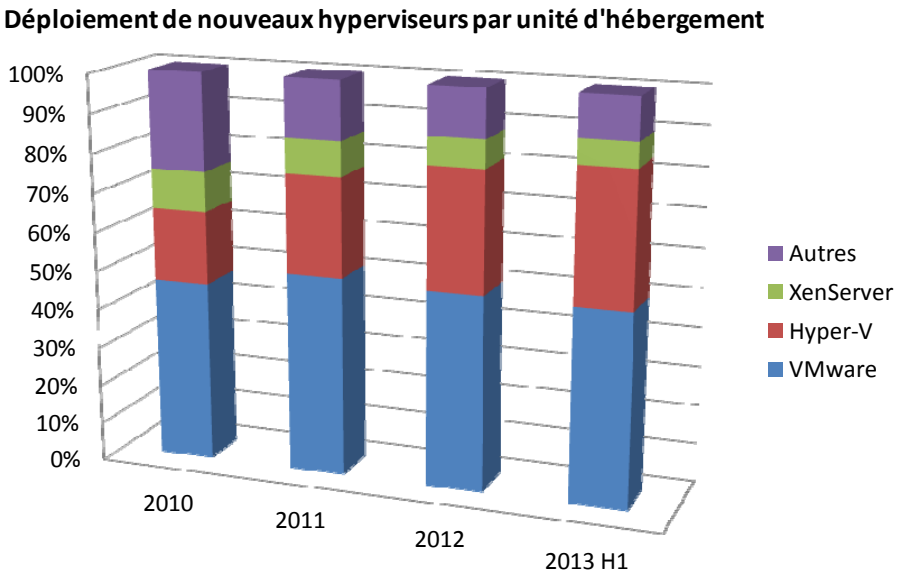
Une telle évolution a toutefois fini par faire émerger deux environnements de protection des données parallèles et souvent fragmentés, l'un pour l'infrastructure physique et l'autre pour l'infrastructure virtuelle, avec des parties communes et une intégration très limitées.

Cette approche permet certes de résoudre le problème immédiat lié à la nécessité de garantir une protection des données adéquate pour les environnements physiques et virtuels. Celle-ci génère en revanche des problèmes à plus long terme sur les plans de la gestion et de la cohérence des tâches visant à garantir la continuité de l'activité et la conformité, augmente les frais de fonctionnement, et aggrave les risques d'erreur et défaillance du fait des interventions manuelles nécessaires sur les systèmes.

Une autre question qui se pose à propos de la protection des données dans les infrastructures virtuelles est celle de la maintenance des hyperviseurs. Pendant de nombreuses années, VMware a été le choix par défaut pour la plupart des installations. Plus récemment, Microsoft a fini par émerger comme un concurrent sérieux, tandis que XenServer, KVM et Oracle entre autres, sont utilisés dans de nombreuses entreprises (cf. figure 4).

FIGURE 4

Utilisation des plateformes d'hyperviseur dans la zone EMEA



Source : IDC 2013

Bon nombre de solutions de protection des données pour infrastructures virtuelles ont focalisé leur offre sur des fournisseurs d'hyperviseurs spécifiques, ou ont adopté une approche du plus petit dénominateur commun pour la prise en charge des différentes fonctionnalités et capacités, tendant alors à limiter leur intérêt réel.

Lorsqu'une solution de protection des données est exclusivement focalisée sur l'environnement virtuel ou sur un fournisseur d'hyperviseur particulier, cela engendre nécessairement certains problèmes de migration et de compatibilité. Si le sens « physique-virtuel » est important pour les tâches de migration et de restauration, les sens « virtuel-virtuel » et « virtuel-physique » le sont tout autant. Toutes ces formes d'utilisation doivent être prises en compte pour garantir un environnement de protection de données homogène sur l'ensemble de l'infrastructure physique et virtuelle.

Si le travail d'intégration requis pour déplacer les environnements virtuels entre ces différents domaines est trop important, cela finira par créer des îlots d'infrastructure séparés les uns des autres, nécessitant chacun des compétences et des ressources spécifiques. Or cela est précisément à l'opposé des objectifs à long terme du DSI et de son entreprise, à savoir la simplification, la standardisation et l'agilité. Une nouvelle approche est par conséquent nécessaire.

UNE PROTECTION DES DONNÉES UNIFIÉE POUR LES ENVIRONNEMENTS PHYSIQUES ET VIRTUELS

Pour assurer la protection de leurs données, de nombreuses entreprises ont décidé de déployer des solutions « *best-of-breed* » pour leurs infrastructures virtuelles, tout en conservant leurs solutions existantes pour leurs actifs physiques. Si elles sont pratiques et relativement simples et rapides à mettre en œuvre, ces solutions font en revanche émerger un certain nombre de problématiques plus générales ayant trait à l'intégration, à la gestion et à la cohérence.

Idéalement, une entreprise a besoin d'une solution fondée sur un produit unique, offrant une large palette de fonctionnalités, permettant de mettre en œuvre la protection des données de manière cohérente sur les environnements physiques et virtuels, et prenant en charge les différentes technologies d'hyperviseur proposées par les grands fournisseurs.

Une telle solution peut sembler encore utopique mais l'on constate pourtant que les suites intégrées sont en train de devenir riches en fonctionnalités et sont désormais capables de produire d'excellents résultats dans le domaine de la protection des données. De telles solutions, dites « *best-of-need* », permettront à terme de proposer une partie importante des capacités des offres « *best-of-breed* », tout en apportant des avantages supplémentaires en termes d'intégration et de gestion sur l'ensemble des scénarios physiques et virtuels.

MEILLEURES PRATIQUES EN MATIÈRE DE PROTECTION DES DONNÉES DANS LES ENVIRONNEMENTS VIRTUELS

Avec le recours de plus en plus généralisé aux clouds privés et au modèle SDDC (*Software-Defined Data Center*), les services informatiques tendent à focaliser leur action sur l'élimination des « îlots » au sein de l'infrastructure qui nécessitent des opérations, compétences et traitements spécifiques. Lorsque la virtualisation n'était encore qu'une niche technologique, elle nécessitait des outils spécialisés pour les opérations de sauvegarde et de restauration. La virtualisation s'étant désormais imposée comme la méthode de déploiement privilégiée dans la plupart des configurations, les processus adjacents tels que la sauvegarde et la restauration doivent pouvoir être gérés à l'identique pour l'ensemble de l'infrastructure, à la fois physique et virtuelle : il n'est plus envisageable de composer un « patchwork » de solutions ponctuelles fonctionnant indépendamment les unes des autres.

La protection et la récupération des données doivent être intégrées en toute transparence au sein des couches supérieures d'automatisation et d'orchestration mises en place pour accompagner des pratiques de virtualisation désormais fermement ancrées. À terme, la maturité et l'intégration de la fonction de protection des données doivent être telles que cette dernière finira par devenir l'un des nombreux attributs du niveau de service défini pour une application.

Si l'on est réaliste, on doit toutefois considérer que cela nécessitera inévitablement une plateforme de protection des données intégrée. Le recours à une multiplicité de produits ponctuels, déployés individuellement, compliquera fortement cette tâche si des efforts importants ne sont pas consentis pour intégrer les différents éléments.

L'un des moyens d'accélérer la mise en œuvre d'une structure unifiée pour la protection des données sera d'envisager le déploiement d'une appliance contenant l'ensemble du hardware et du software nécessaires, directement intégrés au sein d'une unité autonome. La solution pourra ainsi être opérationnelle et entièrement prise en charge dans des délais très courts, avec l'ensemble du hardware et du software nécessaires, et sans les coûts associés à la sélection et à l'achat de serveurs, d'équipements de stockage et de licences de logiciels distincts.

La migration des charges de travail dans le sens physique-virtuel, puis dans le sens retour, ainsi qu'entre les différents environnements d'hyperviseur, est une fonctionnalité critique qui doit impérativement être prise en charge par la solution de protection des données. Cela permettra aux responsables informatiques de transférer, en toute transparence, les charges de travail entre les différents environnements, ainsi que vers des plateformes de traitement externes, le cas échéant.

AVANTAGES DE LA PROTECTION DES DONNÉES UNIFIÉE POUR L'INFRASTRUCTURE INFORMATIQUE

La possibilité de définir une politique de gestion de la protection des données unique pour les différents environnements physiques et virtuels simplifie grandement le processus de sauvegarde et de restauration. La cohérence permet également de garantir plus facilement, et de documenter plus efficacement la mise en conformité. Une approche intégrée permettra en outre d'éviter la fragmentation entre des îlots incompatibles en matière de protection des données, d'améliorer l'efficacité opérationnelle, et de réduire les frais de fonctionnement, ce dernier point étant un objectif clé pour tout DSI cherchant à investir dans de nouvelles opportunités de développement.

La prise en charge des implémentations d'hyperviseur les plus courantes permettra de déployer et d'exécuter les VM et les charges de travail sur la plateforme la plus appropriée compte tenu des niveaux de service à respecter. Les frais de licences et d'assistance technique des différents hyperviseurs varient considérablement. La possibilité de pouvoir choisir la plateforme la plus appropriée (notamment en fonction de critères tels que la prise en charge des éditeurs de logiciels indépendants, les performances, la réduction des coûts ou la facilité de gestion) pourra aider à optimiser les coûts de fonctionnement associés aux charges de travail en exécutant celles-ci là où elles seront les plus efficaces, au lieu d'être restreintes à un environnement d'hyperviseur spécifique.

La bibliothèque de protection de données peut agir comme une couche de stockage supplémentaire. Les machines virtuelles stockées dans la bibliothèque peuvent être mises en rotation directement, sans avoir à être restaurées sur un support de stockage intermédiaire. Les fichiers et données peuvent ainsi être récupérés rapidement à partir des machines virtuelles en les mettant en rotation, tandis qu'il sera possible de restaurer intégralement des applications et services, jusqu'à un état de fonctionnement complet, directement à partir de la sauvegarde réalisée sur l'hôte cible, assurant ainsi des interruptions de services minimales.

Cette capacité de la solution de protection de données à agir comme une couche de stockage supplémentaire présente un autre avantage : si le fournisseur de la solution propose un ensemble plus large de fonctionnalités de stockage, celles-ci pourront utiliser le stockage de protection de façon à optimiser l'intégralité de la pile de stockage et à libérer un espace précieux pour les données volatiles conservées sur les structures de stockage haute performance, tout en permettant de déployer les technologies courantes, telles que la déduplication, la compression, le chiffrement et la réplication, pour optimiser les capacités de protection des données.

POINTS CLÉS À RETENIR

La virtualisation est désormais une technologie incontournable pour les services informatiques automatisés de nouvelle génération, fondés sur des clouds privés et hybrides/publics, et l'on peut anticiper sa généralisation dans la plupart des entreprises au cours des prochaines années, à mesure que les infrastructures informatiques évolueront vers le modèle SDDC (*Software Defined Data Centre*).

Le choix d'un fournisseur capable de proposer un portefeuille complet d'outils de protection des données, fonctionnant indifféremment dans les environnements physiques et virtuels et prenant en charge les implémentations d'hyperviseur les plus courantes, sera un critère de choix majeur pour toute entreprise souhaitant pouvoir fournir des services de bout en bout agiles et performants, tout en éliminant les îlots de service devant être gérés séparément.

On pourra par ailleurs considérer comme un atout supplémentaire le fait que ce portefeuille soit complété par un ensemble plus large de fonctionnalités de gestion du stockage, permettant de mobiliser la protection des données pour optimiser le stockage et la gestion des images et données des infrastructures virtuelles.

IDC recommande de considérer uniquement les solutions de protection des données qui permettent de protéger à la fois les infrastructures physiques et virtuelles, et qui prennent en charge les cinq solutions d'hyperviseur les plus courantes

A propos d'IDC

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. IDC aide les professionnels évoluant sur les marchés IT et les investisseurs à prendre des décisions stratégiques basées sur des données factuelles. Plus de 1000 analystes proposent leur expertise globale, régionale et locale sur les opportunités et les tendances technologies dans plus de 110 pays à travers le monde. Depuis plus de 48 ans, IDC propose des analyses stratégiques pour aider ses clients à atteindre leurs objectifs clés. IDC est une filiale de la société IDG, leader mondial du marché de l'information dédiée aux technologies de l'information.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com