

rapport de
recherche
personnalisé

MIT SMR CUSTOM STUDIO

Rapport d'enquête : Pourquoi les entreprises font davantage confiance au cloud

Septembre 2017

POUR LE
COMPTE DE :

Google Cloud

Table des matières

Point de vue du commanditaire	2
Résumé	3
Méthodologie	4
Introduction	5
Figure 1 : Agilité, sécurité et rapidité : principaux avantages du cloud	
Adoption stratégique	6
Figure 2 : Le stockage des données comme : principale charge de travail déployée dans le cloud - Croissance la plus forte prévue pour le ML et l'IA	
Figure 3 : Les données de type IdO seront les plus déployées dans le cloud d'ici à deux ans	
Évaluation de la sécurité du cloud	8
Figure 4 : La protection des données : principale exigence envers le cloud en matière de sécurité	
Sceptiques	10
Figure 5 : Parmi les sceptiques, les problèmes de sécurité constituent encore une barrière au déploiement dans le cloud	
Figure 6 : Les cadres supérieurs des grandes entreprises sont les plus sceptiques à l'égard du cloud	
Utilisation future du cloud	11
Figure 7 : Les données de type ML/IA parfaitement adaptées au cloud	
Conclusion	12

Avis de droit d'auteur et de non-responsabilité

Google Inc. n'émet aucune garantie relative à l'exactitude ou à l'exhaustivité de ce rapport. Google Inc. ne saurait être tenu pour responsable à l'égard de l'utilisateur ou d'une quelconque autre personne en cas d'inexactitude, d'erreur ou d'omission, quel qu'en soit le motif, ni de tout autre préjudice en découlant. En tout état de cause, ni Google Inc., ni d'autres entreprises ou concédants de licence tiers ne sauraient être tenus pour responsables de tous dommages indirects, particuliers ou consécutifs, y compris, mais de façon non limitative, d'une perte de temps, d'argent, de fonds commercial ou d'un manque à gagner, causé ou non par responsabilité contractuelle, délictuelle ou sans faute, que de tels dommages soient prévus ou non dans le cadre d'une utilisation quelconque de ce document. Ce document ou toute partie de celui-ci ne peut pas être reproduit, transmis, inséré dans un système d'extraction ni diffusé sans l'autorisation écrite de Google Inc.

© Copyright 2017 Google Inc. Tous droits réservés.

Les noms des entreprises et produits réels mentionnés dans le présent document peuvent être des marques déposées de leurs propriétaires respectifs.



Rob Sadowski
Confiance et sécurité, Google cloud



De plus en plus d'entreprises font confiance au cloud. Voici pourquoi.

MIEUX VOUS ÊTES INFORMÉ, plus vous êtes susceptible de confier vos données les plus importantes à un fournisseur cloud.

C'est ce qu'indique un récent sondage mondial effectué auprès de plus de 500 décideurs informatiques pour Google cloud en association avec MIT SMR Custom Studio. Les répondants qui avaient l'expérience la plus directe avec la technologie du cloud avaient davantage confiance en sa sécurité.

Il n'est pas étonnant que de nombreuses entreprises considèrent aujourd'hui le cloud computing comme une composante essentielle de leur stratégie informatique. Mais, en plus des moteurs traditionnels d'adoption du cloud, tels que la vitesse et l'agilité qu'il offre, la sécurité joue un rôle de plus en plus important dans la décision de passer au cloud. Et ce sont les responsables informatiques ayant une expérience directe du cloud qui mènent la charge.

Mais il reste bien entendu des sceptiques. Et la sécurité de votre pile informatique dépendra toujours des partenaires et des modèles de mise en œuvre que vous choisirez. Avec Google Cloud, nous avons pleinement investi dans la sécurité, qu'il s'agisse de matériel spécialisé ou du bon déroulement de nos opérations quotidiennes. Il est gratifiant de voir les responsables informatiques reconnaître que, dans de nombreux cas, le passage au cloud peut en réalité permettre de renforcer la sécurité.

Lisez la suite pour en savoir plus sur les principales charges de travail que les entreprises font passer dans le cloud, ainsi que sur les mesures qu'elles prennent pour gérer la sécurité sur les plates-formes cloud.

Et si vous êtes prêt à parler à un partenaire cloud, contactez-nous à l'adresse suivante :

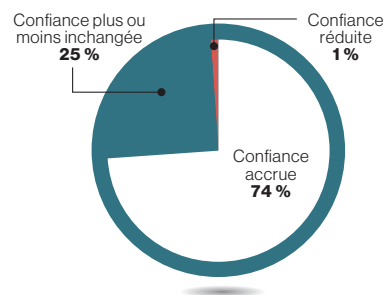
<https://cloud.google.com/contact>. ■

Résumé

- Une « confiance accrue dans la sécurité du cloud » et un « besoin constant d'agilité et de rapidité » sont les principaux moteurs d'adoption du cloud. Parmi les critères de passage au cloud, on retrouve également la nécessité d'être plus flexible, tant sur le plan commercial que technique, et l'attrait d'une meilleure intégration avec de nouveaux outils et plates-formes.
- L'analyse des données, le stockage des données et la collaboration sont les principales charges de travail actuellement mises en œuvre dans le cloud ou qui devraient être déployées au cours des deux prochaines années.
- Le Machine learning et l'intelligence artificielle sont les charges de travail à la croissance la plus rapide, avec un déploiement dans le cloud qui devrait quasiment doubler d'ici à 2019.
- L'utilisation du cloud est passée de 24 % à 44 % des charges de travail au cours des deux dernières années, et devrait atteindre 65 % au cours des deux prochaines années.

Trois répondants sur quatre ont plus confiance dans le cloud

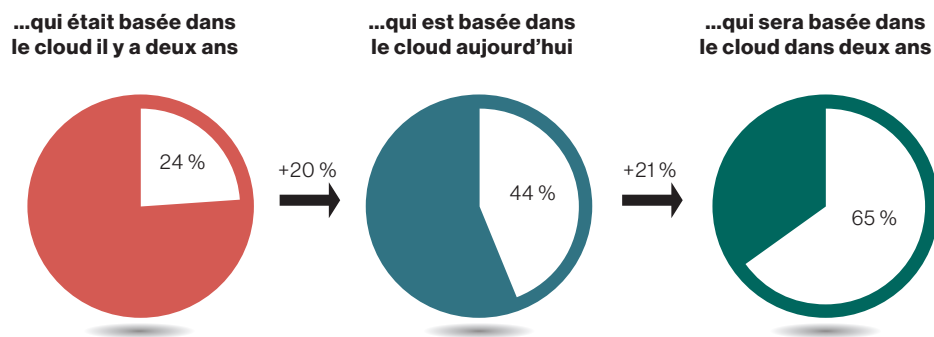
Il a été demandé aux répondants : Au cours des deux dernières années, de quelle manière votre confiance en la sécurité des applications et de l'infrastructure du cloud a-t-elle évolué ?



N = 509
Base : enquête auprès de 509 dirigeants et responsables informatiques d'entreprises de taille moyenne et de grandes entreprises à travers le monde
Source : MIT SMR Custom Studio/Google, juin 2017 Cloud Security Survey

Croissance constante de l'utilisation du cloud

Il a été demandé aux répondants : Veuillez estimer la proportion de vos applications, données et/ou infrastructures...

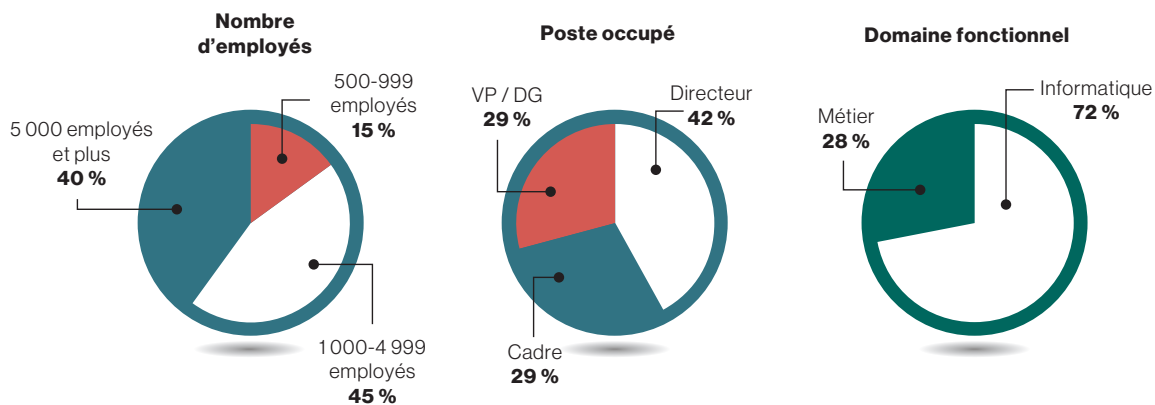


N = 509
Base : enquête auprès de 509 dirigeants et responsables informatiques d'entreprises de taille moyenne et de grandes entreprises à travers le monde
Source : MIT SMR Custom Studio/Google, juin 2017 Cloud Security Survey

Méthodologie

- Portant spécifiquement sur la façon dont les entreprises adoptent et gèrent la sécurité du cloud, l'enquête en ligne de 25 questions (hors questions démographiques) a été distribuée sous forme d'invitation par e-mail, et effectuée entre le 8 juin et le 22 juin 2017.
- Nous avons reçu 509 réponses complètes à l'enquête. 38 % provenaient d'Amérique du Nord (États-Unis et Canada) ; 18 % d'Amérique latine (Mexique, Brésil) ; 24 % d'Europe (Royaume-Uni, France, Allemagne), du Moyen-Orient et d'Afrique (EMEA) ; et 20 % du Japon et de la région Asie-Pacifique (Australie / Nouvelle-Zélande, Inde, Japon – JAPAC).
- L'enquête ciblait les DSI et les cadres supérieurs (y compris les directeurs, les vice-présidents, les directeurs généraux et les membres des équipes de direction) qui influencent les décisions et initiatives informatiques de leur entreprise, ou qui y participent. Pour les entreprises situées en Amérique du Nord, en Amérique latine ainsi que dans les régions EMEA et JAPAC, 72 % des répondants à l'enquête travaillaient dans l'informatique et 28 % représentaient le secteur d'activité de leur entreprise.
- Seuls les répondants ayant une connaissance significative des technologies du cloud étaient qualifiés pour participer à l'enquête.
- L'enquête ciblait les entreprises de plus de 1 000 employés aux États-Unis et de plus de 500 employés dans les autres régions. Parmi les répondants à l'enquête, 40 % représentaient des entreprises de plus de 5 000 employés, 45 % représentaient des entreprises d'entre 1 000 et 4 999 employés et 15 % représentaient des entreprises de moins de 1 000 employés.

Profil des répondants



N = 509

Base : enquête auprès de 509 dirigeants et responsables informatiques d'entreprises de taille moyenne et de grandes entreprises à travers le monde

Source : MIT SMR Custom Studio/Google, juin 2017 Cloud Security Survey

La sécurité : moteur principal d'adoption du cloud par les entreprises

L'époque où l'on s'inquiétait de la sécurité du cloud est révolue. Non seulement l'adoption du cloud se généralise dans tous les secteurs, mais la confiance dans la sécurité du cloud augmente également, au point que cette sécurité accrue est l'une des principales raisons pour laquelle les entreprises passent au cloud.



Introduction

Selon une récente enquête menée à l'échelle mondiale auprès de plus de 500 répondants pour Google Cloud, en association avec MIT SMR Custom Studio, l'utilisation du cloud est passée de 24 % à 44 % des charges de travail au cours des deux dernières années, et devrait augmenter à 65 % des charges de travail d'ici à 2019.

Fini le temps où les entreprises se résignaient à passer au cloud uniquement parce qu'il s'agissait du moyen le moins coûteux d'adapter leurs ressources de calcul, de stockage et de réseau à leurs besoins. Le cloud est

aujourd'hui une nécessité stratégique et son agilité, ses capacités d'intégration et sa vitesse (ainsi que sa sécurité) sont les principaux moteurs de son adoption croissante (voir Figure 1 « Agilité, sécurité et rapidité : principaux avantages du cloud » page 6).

Cette approche plus stratégique s'étend à la façon dont les organisations gèrent le cloud. Les résultats de cette enquête montrent que ces entreprises adoptent une approche approfondie et systématique pour évaluer la sécurité des applications, des infrastructures et des

plates-formes accessibles sur Internet. Les résultats montrent également que l'expérience directe est souvent ce qui sépare les convaincus des sceptiques.

Autre indicateur de la maturité croissante en matière de gestion du cloud : les différents secteurs, régions et rôles s'accordent tous sur les capacités nécessaires pour atteindre les niveaux requis de sécurité dans le cloud.

Toutefois, pour certains, une inquiétude subsiste concernant l'intégration des applications métier dans le cloud ou la façon dont les régulateurs traitent les données qui leur sont confiées. Pour ceux qui hésitent toujours à adopter le cloud, la sécurité demeure la principale préoccupation.

Ce rapport examine la confiance croissante des entreprises dans la sécurité du cloud, la façon dont elles fondent leurs décisions d'hébergement sur la flexibilité et l'intégration offertes par le cloud, et leurs projets d'utilisation du cloud pour de futures charges de travail telles que l'intelligence artificielle (IA) et le Machine learning (ML). Il permet également de mieux comprendre les points de vue de ces organisations quant aux capacités de sécurité dont elles ont besoin de la part des fournisseurs, et les raisons pour lesquelles les sceptiques restent peu convaincus.

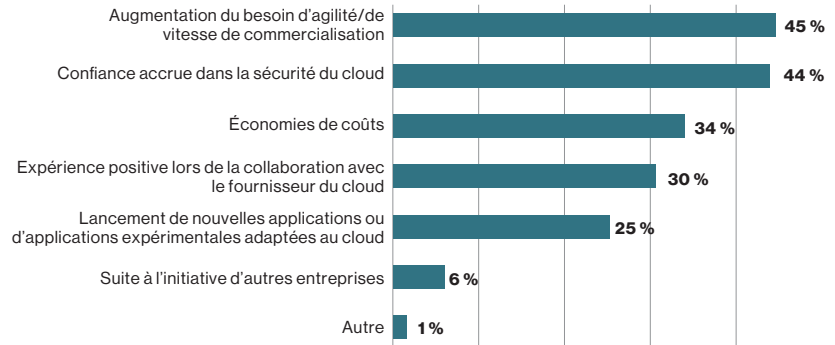
Adoption stratégique

À l'ère du numérique, les entreprises doivent rapidement déployer de nouvelles applications et de nouveaux services, partager des données avec de nouveaux périphériques et partenaires commerciaux et adopter de nouvelles technologies. Lorsqu'on leur demande pourquoi elles déploient actuellement, ou envisagent de déployer, des charges de travail spécifiques dans le cloud, les répondants à l'enquête citent systématiquement « une

Figure 1

Agilité, sécurité et rapidité : principaux avantages du cloud

Il a été demandé aux répondants : Parmi les éléments ci-dessous, quelles sont les raisons pour lesquelles votre utilisation générale du cloud a augmenté au cours des deux dernières années (deux réponses maximum) ?



N = 447

Base : enquête auprès de 509 dirigeants et responsables informatiques d'entreprises de taille moyenne et de grandes entreprises à travers le monde
Source : MIT SMR Custom Studio/Google, juin 2017 Cloud Security Survey

flexibilité accrue dans les processus métier et le choix des fournisseurs » et la « capacité à intégrer de nouveaux outils et plates-formes » comme les deux principales raisons du déploiement de la plupart de leurs charges de travail.

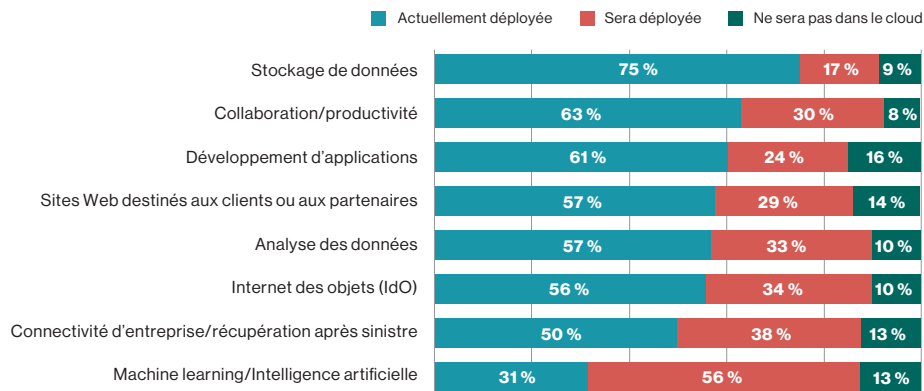
« Le cloud offre les outils de développement les plus modernes ainsi que des fonctionnalités de DevOps et de conteneurs plébiscitées par les développeurs pour concevoir et déployer des applications plus rapidement », explique Jim Reavis, cofondateur et directeur général de la Cloud Security Alliance, une organisation à but non lucratif qui promeut les bonnes pratiques en matière de sécurité du cloud. Le cloud permet également aux organisations de développer leurs ressources sans avoir à commander ni à installer de serveurs et à « tester rapidement une application ou piloter un nouveau processus métier et l'itérer », affirme-t-il. En effet, 31 % des répondants à l'enquête sur le cloud ont cité la « capacité d'intégration de nouveaux outils/plates-formes » comme principale raison pour laquelle ils choisissent de déployer des charges de travail dans le cloud.

Les retardataires qui passent tout juste au cloud déploient tout d'abord des méthodologies telles que le développement agile, l'intégration continue et la livraison

Figure 2

Le stockage des données comme : principale charge de travail déployée dans le cloud - Croissance la plus forte prévue pour le ML et l'IA

Il a été demandé aux répondants : Parmi ces charges de travail actuellement mises en œuvre par votre organisation, lesquelles ont été déployées dans le cloud ? Parmi les charges de travail que vous mettrez en œuvre au cours des deux prochaines années, lesquelles seront déployées dans le cloud ?



N = 506 ; les totaux peuvent dépasser 100 % en raison des arrondissements

Base : enquête auprès de 509 dirigeants et responsables informatiques d'entreprises de taille moyenne et de grandes entreprises à travers le monde
Source : MIT SMR Custom Studio/Google, juin 2017 Cloud Security Survey

continue d'applications en interne « dans le cadre de leur plan de préparation au cloud », explique Doug Cahill, analyste senior chez Enterprise Strategy Group, société de conseil. Selon lui, cette approche consiste souvent à lancer l'intégration et la livraison continues en interne afin de comprendre comment étendre leur utilisation lors de la migration vers le cloud.

Lorsqu'on leur a demandé pourquoi leur utilisation du cloud avait augmenté au cours des deux dernières années, les répondants ont cité « un besoin accru d'agilité/de vitesse de commercialisation » (45 %), une « confiance accrue dans la sécurité du cloud » (44 %) et des « économies de coûts » (34 %) comme les trois principaux facteurs.

Cela ne suffit pas pour stimuler la flexibilité et les processus métier d'une organisation « si vous utilisez le cloud simplement pour pouvoir mettre votre matériel au sous-sol » explique Stuart Madnick, professeur de technologie de l'information à la MIT Sloan School of Management. Il affirme que les bénéfices plus importants proviennent de la combinaison d'un passage au cloud avec une architecture de services Web plus modulaire qui facilite

le partage de données importantes à la fois au sein de l'organisation et avec les partenaires commerciaux.

Parmi les répondants, le stockage des données était la charge de travail la plus souvent mise en œuvre ou dont la mise en œuvre était envisagée dans le cloud, suivie de la collaboration/productivité, du développement d'applications et de l'Internet des objets (IdO). Les répondants ont également indiqué que près de 90 % de ces charges de travail seraient déployées

dans le cloud d'ici à 2019. L'IdO s'est révélé être une charge de travail fortement déployée dans le cloud (56 % actuellement déployés sur le cloud et 90 % déployés d'ici à 2019) - un résultat quelque peu surprenant étant donné que la croissance de ces objets connectés à Internet n'en est encore qu'à ses balbutiements (voir Figure 2 « Le stockage des données comme : principale charge de travail déployée dans le cloud - Croissance la plus forte prévue pour le ML et l'IA » ci-dessus).

Selon Roy Illsley, analyste principal de la société d'analystes Ovum, une grande partie des données IdO actuellement hébergées dans le cloud provient de plateformes établies depuis longtemps, telles que les systèmes de contrôle industriels. Mais alors que les entreprises déploient de plus en plus de données issues de nouveaux appareils IdO dans le cloud, il prédit que les fournisseurs développeront de nouveaux services qui stockeront ces données en périphérie physique du réseau afin qu'elles puissent être analysées suffisamment rapidement pour que les appareils réagissent en fonction de l'évolution des conditions en temps réel. Selon lui, ces données en

périphérie pourraient être stockées dans de petites infrastructures telles que des pôles téléphoniques ou encore dans des centres de données partagés situés dans des zones industrielles et servant plusieurs clients. Cela permettra, par exemple, de pouvoir analyser rapidement des données sur la performance d'un robot de fabrication, les pressions dans un puits de pétrole ou le trafic sur les routes locales afin d'anticiper et prévenir les problèmes.

Selon l'étude, les données clients et employés (59 %), ainsi que les données IdO (également 59 %), étaient les trois types de données les plus susceptibles d'être hébergés aujourd'hui dans le cloud, suivis de près par les données financières de l'entreprise, les documents relatifs au développement de produits et les données relatives aux ressources humaines (RH) de l'entreprise.

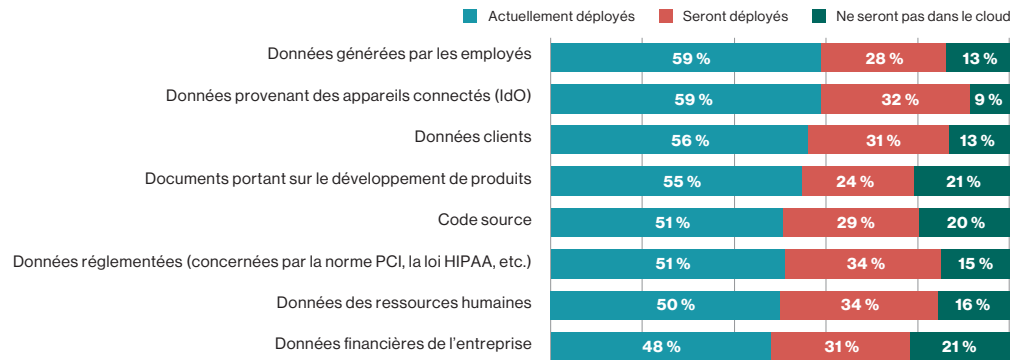
Autre signe de la confiance grandissante envers la sécurité offerte par le cloud : même les organisations aux données hautement réglementées ont cité « une sécurité accrue » comme l'une des raisons de leur migration vers le cloud. Au cours des deux prochaines années, on s'attend à une forte augmentation de l'hébergement dans le cloud de données régies par la réglementation médicale et la confidentialité financière, ainsi que des données financières des entreprises (voir la Figure 3 « Les données de type IdO seront les plus déployées dans le cloud d'ici à deux ans » ci-dessus).

Selon Rik Turner, analyste principal des solutions d'infrastructure chez Ovum, même l'industrie des services

Figure 3

Les données de type IdO seront les plus déployées dans le cloud d'ici à deux ans

Il a été demandé aux répondants : Parmi les types de données actuellement mises en œuvre par votre organisation, lesquels ont été déployés dans le cloud ? Parmi les types de données que votre organisation envisage de mettre en œuvre au cours des deux prochaines années, lesquels prévoyez-vous de déployer dans le cloud ?



N = 488
Base : enquête auprès de 509 dirigeants et responsables informatiques d'entreprises de taille moyenne et de grandes entreprises à travers le monde
Source : MIT SMR Custom Studio/Google, juin 2017 Cloud Security Survey

financiers, pour laquelle la sécurité est importante, « semble avoir été largement convaincue ». Il ajoute qu'Ovum a récemment sondé 75 grandes banques dans le monde. « Nous...avons été surpris par le nombre d'entreprises ayant déclaré qu'elles faisaient passer des charges de travail dans le cloud public de façon quasi générale. »

Évaluation de la sécurité du cloud

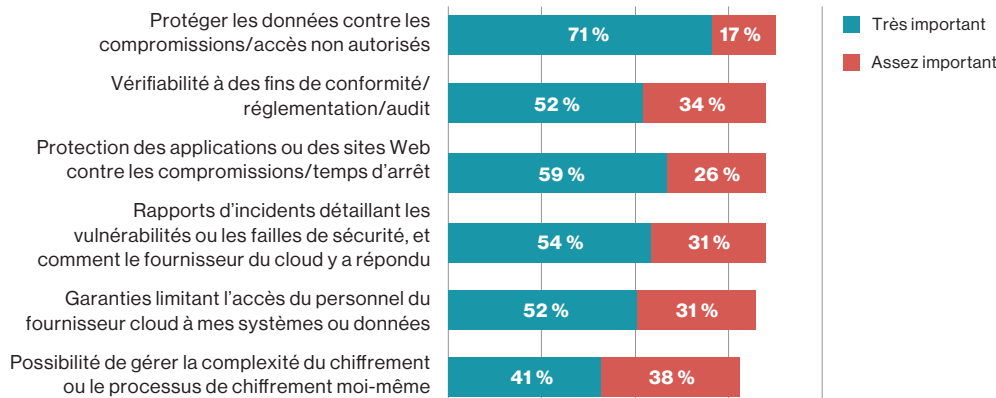
Pourquoi les entreprises sont-elles de plus en plus nombreuses à faire confiance au cloud ? Une expérience directe et des évaluations prudentes et systématiques mettant à profit plusieurs sources, telles que des audits détaillés et des comparatifs, sont quelques-unes des raisons. Le motif le plus fréquent de cette confiance (67 % de nos répondants) est « le constat direct de la qualité de la sécurité du cloud par rapport à un stockage en interne », suivi d'un « audit ou examen détaillé de la sécurité du stockage en interne par rapport à celle du cloud » (51 %).

Concernant les facteurs les plus importants dans leur évaluation de la sécurité du cloud, les répondants ont, dans l'ordre, cité :

Figure 4

La protection des données : principale exigence envers le cloud en matière de sécurité

Les répondants ont été interrogés sur l'importance des facteurs suivants en matière de sécurité du cloud. (Réponses multiples autorisées.)



N = 509

Base : enquête auprès de 509 dirigeants et responsables informatiques d'entreprises de taille moyenne et de grandes entreprises à travers le monde
Source : MIT SMR Custom Studio/Google, juin 2017 Cloud Security Survey

- Évaluations par leur propre équipe de sécurité
- Respect des normes de sécurité et de conformité
- Outils de sécurité proposés par le fournisseur du cloud
- Recommandations d'analystes et de consultants

Sans surprise, l'exigence la plus fréquemment mentionnée en matière de sécurité était la protection des données (71 %). Ont également été citées : la protection des applications et des sites Web contre les compromissions ou les temps d'arrêt ; la génération de rapports sur les incidents de sécurité et la façon dont le fournisseur de cloud y a répondu ; et le contrôle et les garanties contre l'accès du personnel du fournisseur de cloud aux données du client (voir Figure 4 « La protection des données : principale exigence envers le cloud en matière de sécurité » ci-dessus).

Selon Jim Reavis, de la Cloud Security Alliance, les fournisseurs de cloud peuvent faire encore davantage pour répondre aux besoins des utilisateurs en termes de rapports, en particulier concernant les données incluses dans les fichiers journaux. Les normes portant sur les types d'informations pouvant être partagées dans les rapports d'incident pourraient nécessiter la modification des

contrats des fournisseurs de services, qui interdisent actuellement à un fournisseur de dire à un client que les informations d'un autre client ont été compromises.

Cependant, bien que « les audits et les rapports soient très importants, ce n'est pas ce qui fait la différence », explique Michael Fuller, directeur associé chez The Hackett Group. « Ce que nous entendons le plus souvent, en dehors

de la flexibilité et du coût, c'est la disponibilité », comme le temps de disponibilité de l'application ou l'atteinte d'objectifs spécifiques de récupération après une panne. Cela est particulièrement vrai, selon Michael Fuller, pour les petites et moyennes entreprises, dont les ventes sont comprises entre 500 millions et 3 à 4 milliards de dollars. En effet, 59 pour cent des répondants au sondage ont cité « protéger les applications ou les sites Web contre les compromissions/temps d'arrêt » comme l'une de leurs principales exigences du cloud en matière de sécurité.

Lorsqu'il leur a été demandé quels étaient leurs critères de sécurité concernant l'infrastructure d'un fournisseur cloud, les répondants ont cité tous les critères possibles. En substance, ils veulent tout.

« Nous savons que les professionnels de la cybersécurité priorisent le chiffrement des données, à la fois au repos et en transit, pour protéger les données dans le cloud », déclare Holger Schulze, fondateur de la Information Security Community (« Communauté pour la sécurité des informations ») composée de 350 000 membres sur LinkedIn. Dans notre enquête, près de 80 répondants

ont indiqué qu'il était relativement important ou très important pour leurs organisations de gérer la complexité du chiffrement ou de gérer le processus de chiffrement lui-même. Toutefois, décider si les clés de chiffrement sont contrôlées par l'entreprise ou le fournisseur de cloud est souvent un « objet de contentieux très important », affirme Michael Fuller.

La possibilité pour un client d'utiliser le chiffrement d'un fournisseur de cloud mais de gérer ses propres clés « est en quelque sorte le Saint Graal » du chiffrement, affirme Jim Reavis. « Mais ce n'est pas toujours réaliste en fonction de l'architecture des applications ». Il a également déclaré que cela était plus difficile avec les applications nécessitant une gestion de l'accès (et des clés de chiffrement) pour de nombreux utilisateurs.

Sceptiques

Malgré cette large adoption et confiance dans le cloud computing, une minorité de répondants considérait toujours les problèmes de sécurité comme un obstacle à l'adoption (voir la Figure 5 « Parmi les sceptiques, les problèmes de sécurité constituent encore une barrière au déploiement dans le cloud », à droite). Pour les répondants, la sécurité était la principale raison pour laquelle ils ne déplaçaient pas leurs données stockées, leurs sites Web destinés à leurs clients ou partenaires et leurs données IdO vers le cloud. Et seulement 59 % des décideurs des entreprises ont déclaré que leur confiance dans le cloud avait augmenté au cours des deux dernières années, contre 81 % des répondants travaillant dans l'informatique.

Dans l'ensemble, les répondants travaillant dans l'informatique faisaient davantage confiance à la sécurité du cloud que leurs homologues des fonctions métier, les membres d'équipes de direction étant les plus

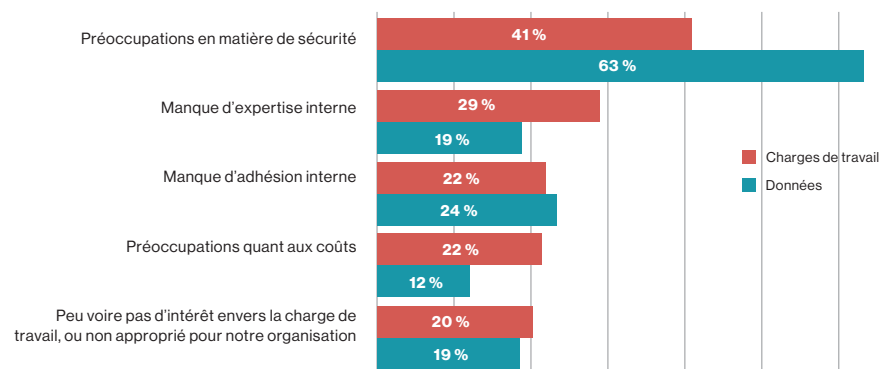
sceptiques. Les grandes entreprises ont également tendance à être davantage préoccupées par la sécurité du cloud que les plus petites entreprises (voir la Figure 6 « Les cadres supérieurs des grandes entreprises sont les plus sceptiques à l'égard du cloud » page 11).

Selon Doug Cahill, de la société de conseil Enterprise Strategy Group, l'un des facteurs pouvant accroître les préoccupations en matière de sécurité est le « manque de visibilité » des contrôles de la sécurité du cloud pour les entreprises habituées à gérer leurs propres infrastructures en interne. L'impossibilité de pouvoir simplement « intégrer les contrôles de sécurité auxquels ils sont habitués, comme un pare-feu périmétrique de pointe » peut selon lui déconcerter.

Selon Michael Fuller, de The Hackett Group, l'une des principales raisons des craintes des entreprises en matière de sécurité est « un manque de confiance dans leurs propres capacités architecturales ». Sans une compréhension approfondie de leurs architectures, de nombreuses entreprises ne savent pas comment les sécuriser dans le cloud.

Figure 5 Parmi les sceptiques, les problèmes de sécurité constituent encore une barrière au déploiement dans le cloud

Il a été demandé aux répondants : Quelles sont les principales raisons pour lesquelles vous avez choisi de ne PAS déployer des charges de travail ou des données dans le cloud ? (Réponses multiples autorisées.)

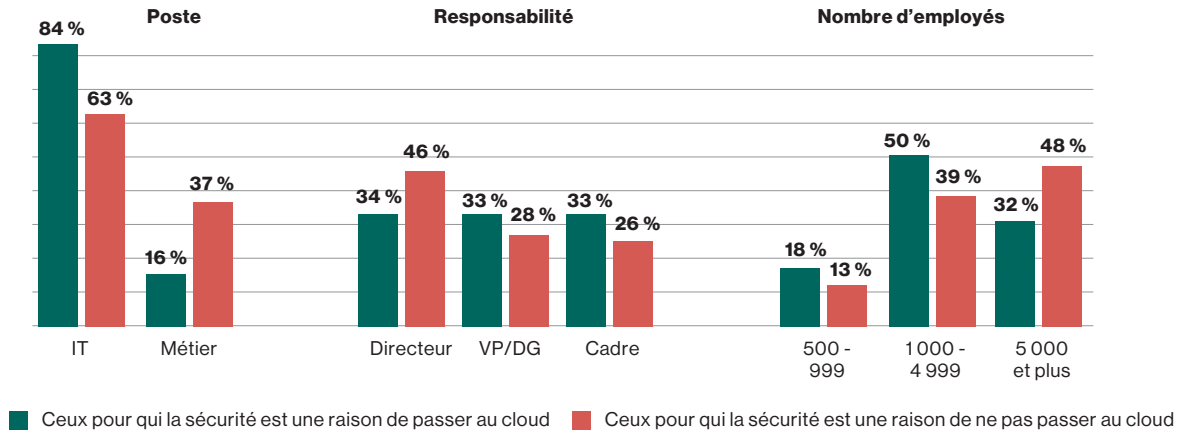


N = 295, N = 230
Base : enquête auprès de 509 dirigeants et responsables informatiques d'entreprises de taille moyenne et de grandes entreprises à travers le monde
Source : MIT SMR Custom Studio/Google, juin 2017 Cloud Security Survey

Figure 6

Les cadres intermédiaires et ceux des grandes entreprises sont les plus sceptiques à l'égard du cloud

Parmi les répondants à l'enquête, les membres des équipes de direction et les répondants des entreprises de plus de 5 000 employés sont ceux qui se disent les plus préoccupés par la sécurité du cloud.



N = 285, N = 184

Base : enquête auprès de 509 dirigeants et responsables informatiques d'entreprises de taille moyenne et de grandes entreprises à travers le monde
Source : MIT SMR Custom Studio/Google, juin 2017 Cloud Security Survey

Utilisation future du cloud

Au fur et à mesure que l'univers des données se développera et que les organisations chercheront à exploiter ces données, l'évolutivité et la flexibilité du cloud deviendront de plus en plus importantes.

Les résultats de l'enquête montrent que le Machine learning et l'intelligence artificielle seront les charges de travail à la croissance la plus rapide en termes de déploiement dans le cloud. 35 % des répondants ont déclaré qu'ils déployaient actuellement, ou prévoyaient de déployer, le ML/l'IA dans le cloud au cours des deux prochaines années. D'ici à 2019, 87 % de cette charge de travail sera déployée dans le cloud. La continuité de l'activité/la récupération après sinistre et les charges de travail liées à l'IdO afficheront également une forte croissance en matière de déploiement dans le cloud au cours de la même période.

Les répondants ont indiqué que ceux qui souhaitent déployer le ML/l'IA dans le cloud étaient particulièrement attirés par la rapidité, la flexibilité et les capacités

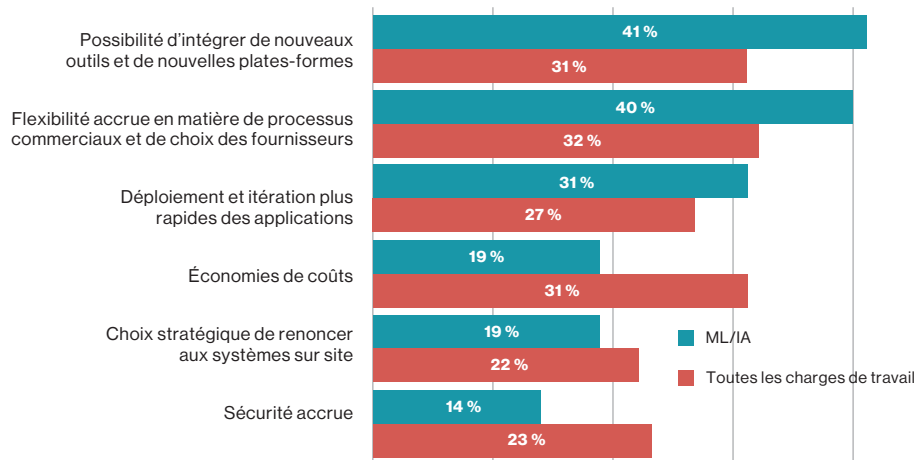
d'intégration offertes (voir Figure 7 « Les données de type ML/IA parfaitement adaptées au cloud » page 12).

« Le calcul à la demande et le stockage disponible dans le cloud sont très utiles pour les tâches de calcul à forte utilisation de données, comme le Machine learning et l'intelligence artificielle », explique Doug Cahill. L'évolutivité du stockage de données dans le cloud est également un atout, car plus il y a de données disponibles pour le Machine learning, plus le résultat sera bon. Le Machine learning et l'analyse de données dans le cloud peuvent être utilisés non seulement à des fins de recherche et d'analyse commerciale, mais également pour améliorer la sécurité informatique en identifiant des signes d'attaques potentielles parmi les données normales, affirme-t-il. De plus, Jim Reavis, de Cloud Security Alliance, affirme qu'une telle sécurité automatisée pourrait aider les utilisateurs du cloud à sécuriser les quantités croissantes de données nécessaires pour le ML et l'IA.

Figure 7

Les données de type ML/IA parfaitement adaptées au cloud

Il a été demandé aux répondants les raisons pour lesquelles ils déploient leurs charges de travail dans le cloud. Ceux déployant ou prévoyant de déployer des fonctionnalités de Machine learning ou d'intelligence artificielle ont souvent cité la flexibilité, la vitesse et les possibilités d'intégration comme critères déterminants. Ces critères ont été moins cités par les répondants déployant d'autres types de charges de travail. Le coût et la sécurité, en revanche, font moins partie des raisons qui poussent à passer au cloud dans le domaine du ML et de l'AI.



N = 155, N = 1 822

Base : enquête auprès de 509 dirigeants et responsables informatiques d'entreprises de taille moyenne et de grandes entreprises à travers le monde

Source : MIT SMR Custom Studio/Google, juin 2017 Cloud Security Survey

Selon Jim Reavis, les fournisseurs de cloud peuvent également aider les entreprises à migrer vers le cloud avec des bibliothèques d'algorithmes d'analyse faciles à utiliser ainsi que des interfaces de programmation d'applications (API) afin de faciliter l'échange de données entre fournisseurs de cloud. Beaucoup d'entre eux fournissent de solides plates-formes et des capacités importantes, ce qui permet aux entreprises de faire des économies de matériel et de personnel tout en effectuant leurs analyses eux-mêmes, explique Stuart Madnick, du MIT Sloan.

Conclusion

Selon les résultats de notre enquête, les fortes tendances qui rendent le cloud si indispensable - le besoin d'agilité, de flexibilité et de sécurité pour des quantités toujours croissantes de données - continuent de s'accélérer. Quels que soient le secteur, le domaine d'activité et le pays, le cloud est de plus en plus plébiscité par les entreprises qui cherchent à se mouvoir rapidement, à rester flexible et à sécuriser les données de leurs clients. De plus, les technologies de transformation renforceront

cette tendance. Le Machine learning est parfaitement adapté à la flexibilité, l'évolutivité et les capacités d'intégration du cloud car il nécessite des données et une puissance informatique importantes. C'est également le cas des données IdO, si les fournisseurs de cloud parviennent à mettre en place les réseaux décentralisés nécessaires à une analyse rapide des données et à l'envoi des résultats.

Bien que certains n'utilisent toujours pas le cloud et ne lui fassent pas confiance, les résultats de l'enquête indiquent que ceci est davantage dû à un manque de connaissances et de sensibilisation qu'à de réelles lacunes en matière de sécurité du cloud, en particulier chez les répondants qui sont des utilisateurs métier.

Pour les entreprises qui sont déjà passées au cloud, la sécurité et les coûts ne sont plus un sujet d'inquiétude. Elles voient désormais le cloud comme un moyen de fournir des applications et services toujours plus efficaces, agiles et novateurs. ■