

Le point sur l'adoption et les défis du cloud

Conseils pratiques et état de la sécurité du cloud




Rapport de synthèse


À l'heure où l'informatique, le stockage et la collaboration migrent vers le cloud, il subsiste des doutes chez les professionnels quant au niveau de sécurité qu'offre cet environnement. 97 % des entreprises à travers le monde utilisent une forme quelconque de service de cloud et s'attendent à résoudre des problèmes de visibilité et de contrôle. Compte tenu du manque de visibilité sur le cloud, certains dirigeants sont plus frileux à l'adopter tandis que d'autres ont choisi de foncer, même en sachant qu'ils risquent d'être confrontés à des incidents de sécurité.

En fin d'année 2017, McAfee® a interrogé 1 400 responsables informatiques pour établir ce compte rendu annuel de l'état de l'adoption et de la sécurité du cloud, couvrant un large éventail de secteurs, pays et tailles d'entreprises. L'un des principaux objectifs du rapport de cette année visait à introduire un nouveau volet consacré aux meilleures pratiques de sécurité du cloud. Dès lors, nous nous sommes penchés sur les modèles d'utilisation actuels, les préoccupations des responsables et les incidents survenus pour formuler des recommandations d'experts ciblant les problèmes les plus urgents rencontrés par les entreprises.


Le rapport nous permet de conclure que les incidents de sécurité sont monnaie courante. Pas moins d'une entreprise sur quatre utilisant des services IaaS (Infrastructure-as-a-Service) ou SaaS (Software-as-a-Service) a été victime d'un vol de données. Par ailleurs, une sur cinq a fait l'objet d'une attaque avancée contre son infrastructure de cloud public.

Principales observations¹

 **97 %** des entreprises ont recours à des services de cloud (public, privé ou hybride), contre 93 % il y a un an.

 **65 %** possèdent une stratégie de priorisation du cloud, un pourcentage en baisse par rapport aux 82 % de l'année dernière.

 **83 %** stockent des données sensibles dans le cloud public.

 **69 %** font confiance au cloud public pour assurer la sécurité de leurs données sensibles.

 **1 entreprise sur 4** a été victime d'un vol de données dans le cloud public (pour les services IaaS et SaaS).

 **1 entreprise sur 5** a été la cible d'une attaque avancée contre son infrastructure de cloud public.

RAPPORT DE SYNTHÈSE

Comme un certain nombre d'entreprises se préparent à l'entrée en vigueur du règlement général sur la protection des données (RGPD), l'une de nos questions portait aussi sur son impact escompté sur l'adoption du cloud à l'avenir.

Les participants à l'étude étaient des décideurs techniques issus de petites (500 à 1 000 employés), moyennes (1 000 à 5 000 employés) et grandes entreprises (plus de 5 000 employés) situées en Allemagne, en Australie, au Brésil, au Canada, aux États-Unis, en France, en Inde, au Japon, au Mexique, au Royaume-Uni et à Singapour.

Conclusions et recommandations

Une meilleure visibilité permet aux entreprises d'adopter plus rapidement et en toute confiance des services de cloud porteurs d'innovation, d'intervenir plus rapidement face aux menaces de sécurité et de profiter des économies réalisées grâce au cloud. Il est préférable d'avoir une visibilité complète sur le cloud, plutôt que de tenter d'en contrôler une partie seulement.

Les entreprises qui ont fait de la visibilité une priorité utilisent un éventail complet de services de cloud afin d'identifier la meilleure solution pour chaque besoin métier. Elles ont tendance à avoir une attitude plus décontractée face à l'informatique de l'ombre, qu'elles considèrent comme un indicateur précoce des tendances émergentes et des nouveaux services et applications utiles, au lieu de la voir comme une rivale ou une menace à écarter le plus rapidement possible. Elles veulent avoir accès à tout, puis prendre des décisions informées sur la meilleure approche à adopter en matière de contrôle.

Sur la base des observations recueillies cette année, le rapport recommande trois meilleures pratiques que nous encourageons toutes les entreprises à adopter :

1. Processus DevSecOps. Il ne fait aucune doute que les outils DevOps et DevSecOps améliorent la qualité du code et réduisent les exploits et autres vulnérabilités. L'intégration des processus de développement, de contrôle qualité et de sécurité au sein de la division ou de l'équipe de développement des applications est essentielle pour soutenir le rythme imposé par l'environnement actuel des entreprises.
2. Outils de gestion et d'automatisation des déploiements comme Chef, Puppet ou Ansible. Même les responsables informatiques les plus expérimentés éprouvent des difficultés à gérer seuls le volume et la cadence des déploiements de cloud. L'automatisation en complément de l'humain est un aspect essentiel de l'informatique moderne.
3. Sécurité unifiée avec gestion centralisée pour tous les fournisseurs et services de cloud. Lorsque les outils de gestion se multiplient, il est facile pour une menace de passer entre les mailles du filet. Un système de gestion unifiée pour plusieurs clouds allié à une structure d'intégration ouverte réduit la complexité.

Pour télécharger le rapport complet, [cliquez ici](#).



40 % des décideurs informatiques mettent un frein à l'adoption du cloud en raison d'une pénurie de compétences en cybersécurité.



2 x plus probable que l'entreprise élabore une stratégie de protection des conteneurs et de l'environnement sans serveur en présence d'une fonction DevSecOps.



27 % des budgets informatiques sont affectés à la sécurité du cloud, un pourcentage qui devrait atteindre 37 % d'ici un an.



Moins de 10 % des entreprises en moyenne prévoient de diminuer les investissements dans le cloud en conséquence du RGPD.

¹Consultez l'annexe du rapport complet pour plus de détails sur la méthodologie de l'enquête et l'échantillon démographique.



11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr

McAfee, le logo McAfee, ePolicy Orchestrator et McAfee ePO sont des marques commerciales ou des marques commerciales déposées de McAfee, LLC ou de ses filiales aux États-Unis et dans d'autres pays. Les autres noms et marques sont la propriété de leurs détenteurs respectifs.
Copyright © 2018 McAfee, LLC. 3873_0418
AVRIL 2018