Livre blanc

Les questions à poser à votre fournisseur de services de cloud

Pour tout savoir sur la manière dont vos données seront protégées dans le cloud

intel Security

Sommaire

De nombreuses entreprises font aujourd'hui appel à des fournisseurs de services de cloud pour satisfaire leurs besoins en services d'infrastructure (IaaS, Infrastructure-as-a-Service), de plate-forme (PaaS, Platform-as-a-Service) et de logiciels (SaaS, Software-as-a-Service). Le choix des fournisseurs et des services adéquats est essentiel car il peut affecter vos pratiques de sécurité, la confidentialité de vos données et vos capacités opérationnelles. N'hésitez donc pas à passer au crible les fournisseurs de services de cloud potentiels et à leur poser des questions précises sur leurs pratiques de sécurité des informations critiques.

Face à l'essor continu des services de cloud, le choix du ou des fournisseurs de services de cloud appropriés revêt une importance cruciale pour les professionnels de la sécurité et de l'informatique en entreprise. Nombre de fournisseurs proposent des services de cloud, qu'il s'agisse de grandes entreprises internationales offrant un large éventail de services de cloud ou de petites agences spécialisées dans un nombre limité de fonctionnalités. Il existe même des cabinets de courtage de services de cloud qui regroupent des services de cloud proposés par une série de fournisseurs différents suivant des modèles de distribution variés, des intégrateurs système et entreprises d'externalisation aux revendeurs à valeur ajoutée, en passant par les éditeurs de logiciels indépendants.

Les entreprises peuvent se retrouver submergées par la multiplicité des options et avoir du mal à identifier le fournisseur de services de cloud le mieux adapté à leurs besoins. Pour clarifier les nombreuses différences entre les fournisseurs potentiels, vous devez les interroger de façon systématique sur des points clés. Lors de la sélection des fournisseurs de services de cloud qui accompagneront votre migration vers le cloud, la sécurité doit impérativement figurer au premier plan de vos priorités.

Les aspects essentiels de la sécurité doivent faire l'objet d'une série de questions qui vous permettront de restreindre vos choix. Ces questions vous aideront à déterminer quels fournisseurs de services de cloud ont une compréhension approfondie des problèmes de sécurité et de leurs implications, et quels sont ceux dont l'approche est le plus en accord avec les priorités, les pratiques et la tolérance aux risques de votre entreprise. Nous consacrerons l'essentiel de ce livre blanc aux questions spécifiques à trois domaines liés à la protection des données : la sécurité, la confidentialité et les opérations. En suivant ces suggestions et en passant les résultats de votre recherche au filtre de votre expérience, de votre jugement et des conseils de collègues ayant déjà suivi ce processus, vous augmenterez vos chances d'identifier un ou plusieurs fournisseurs de services de cloud à même de vous aider à renforcer la sécurité de vos données les plus critiques.

Approbation des fournisseurs de services de cloud à un haut niveau

Tout d'abord, il est essentiel d'éviter de se perdre en conjectures sur le niveau de sécurité offert par un fournisseur potentiel. Chaque fournisseur de services est différent et applique ses propres règles, conditions générales et accords de niveau de service (SLA). Assurez-vous de bien comprendre l'engagement de chaque fournisseur de services à votre égard en tant que client.

Veillez ensuite à poser des questions sur la gestion de la sécurité et de la confidentialité des données. Vous devez déterminer, entre autres, ce que le fournisseur attend exactement de votre entreprise, les services qu'il offre en tant que fournisseur et la manière dont il le fait.

Prenez soin également d'examiner les conditions générales en détail. Personne n'apprécie de devoir lire les nombreuses pages en petits caractères d'un contrat. Ces détails sont pourtant essentiels pour pouvoir choisir un fournisseur à même de garantir le service et le niveau de confiance appropriés. Évitez donc de vous soustraire à cette corvée en cliquant sur « Accepter » pour passer à autre chose. Plongez-vous dans la lecture des conditions générales et étudiez chaque section en détail en ciblant plus spécifiquement les aspects relatifs aux données.

Enfin, ne partez pas du principe que chaque service de cloud est soumis aux mêmes directives et objectifs de fourniture de service, et ce même chez un fournisseur de services donné. Lisez les conditions générales de chaque service. Parcourez-les toutes et ne faites pas des suppositions sans fondement si vous ne voulez pas avoir de mauvaises surprises en termes de coûts.

Questions de sécurité

Ces dernières années, les problèmes de sécurité liés au cloud ont considérablement diminué grâce à l'adoption de pratiques de sécurité appropriées par les fournisseurs de services de cloud. Néanmoins, de nombreux cadres dirigeants et conseils d'administration s'inquiètent de savoir si les données d'entreprise sont véritablement protégées dans le cloud. Vous devez donc poser des questions spécifiques aux fournisseurs de services de cloud afin d'atteindre le niveau de confiance nécessaire pour réduire les risques et apaiser les craintes.

Qui a accès à mes données, que ce soit physiquement ou virtuellement ?
L'accès physique et l'accès virtuel sont deux aspects totalement différents. Il est par conséquent important de se renseigner sur les deux.

- De quelle protection l'entreprise dispose-t-elle eu égard à l'accès à son centre de données ?
- Le personnel est-il soumis à un contrôle de sécurité et l'accès physique aux données est-il protégé contre les personnes externes à l'entreprise ?
- Quelles sont les stratégies de l'entreprise ou du centre de données, et de quelle manière sont-elles protégées ?
- Qui bénéficie d'un accès virtuel aux données ? D'où ces personnes accèdent-elles aux données et pour quelles raisons ?
- Comment y accèdent-elles ? Utilisent-elles un VPN et les données sont-elles chiffrées ? Si elles sont chiffrées, comment les clés de chiffrement sont-elles sécurisées ?

Le fournisseur de services de cloud externalise-t-il le stockage des données ?
De nombreuses entreprises s'appuient sur l'externalisation pour fournir des services, mais il est possible que votre fournisseur de services de cloud externalise vos données vers un autre emplacement, voire un autre fournisseur. Le cas échéant, vous devez décider si ce type d'arrangement vous convient.

Comment le fournisseur traite-t-il les requêtes judiciaires de consultation de données ?
Que ces requêtes émanent des clients du fournisseur ou d'organismes gouvernementaux et concernent des problèmes juridiques ou réglementaires, leur traitement exige de la finesse, de l'expérience et une grande réceptivité aux stratégies de gouvernance d'entreprise et aux obligations de conformité. Dans la mesure où il n'est pas rare que la qualité de vos données soit affectée par des requêtes judiciaires, vous devez comprendre la traçabilité des données et le traitement réservé à ces requêtes.

Quand et comment les données sont-elles supprimées ?
Chaque fournisseur étant différent, il est essentiel de bien comprendre qu'au vu du volume de données actuellement en circulation dans le monde, le stockage peut s'avérer problématique. Vous devez savoir quelle quantité de données stocke votre fournisseur de services de cloud et, en particulier, quel volume de vos données spécifiques est stocké. Vous devez en outre déterminer pendant combien de temps vos données sont stockées, quand elles sont supprimées et sur quels critères les décisions de suppression sont prises.

Quelle est l'architecture des données ?
Renseignez-vous de manière précise sur la manière dont vos données sont isolées de celles des autres clients dans un environnement en multilocation. Demandez à votre fournisseur de vous expliquer comment vos données sont séparées de celles des autres clients, et ce qui peut changer à l'avenir à cet égard.

Quelles sont les certifications obtenues et/ou quels sont les types d'audits tiers effectués ?
Les certifications vous permettront de mieux cerner le degré de maturité du fournisseur, d'identifier les aspects qui le préoccupent et de déterminer s'il est engagé dans un processus d'amélioration continue. Concernant les audits tiers, vous devez savoir à quelle fréquence le fournisseur vérifie l'existence de modifications et fait en sorte de répondre aux attentes de ses clients et fournisseurs.

Questions sur la confidentialité

Bien que la sécurité et la confidentialité soient étroitement liées, il existe un certain nombre de questions propres à la confidentialité à poser à votre fournisseur de services de cloud. Gardez à l'esprit que, même si elles trouvent clairement leur origine dans la problématique de la conformité, les questions relatives à la confidentialité ne se limitent pas aux problèmes réglementaires.

Quelles sont les données de votre entreprise qui sont collectées et comment sont-elles protégées ?
Chaque entreprise a une notion légèrement différente de la confidentialité. C'est pourquoi il est particulièrement important de déterminer ce que ce concept signifie pour les principales parties prenantes de votre entreprise.

À quelles fins les données sont-elles utilisées ?
Les différentes utilisations faites de vos données sont souvent étonnantes. Certaines pourraient vous surprendre, voire vous inquiéter. Assurez-vous que votre fournisseur de services de cloud comprend vos stratégies de gouvernance en matière d'utilisation acceptable des données.

Combien de temps le fournisseur de services de cloud conserve-t-il ces données ?
Les conditions générales peuvent stipuler que ces données sont collectées pendant 30 jours, 90 jours ou même un an. Néanmoins, cela ne vous renseigne pas nécessairement sur le temps durant lequel l'entreprise est habilitée à conserver vos données. Cette durée sera très différente selon le fournisseur, le service et le type de donnée collectée. Certaines données peuvent être anonymisées, stockées et utilisées à des fins de test pendant de très nombreuses années. Veillez dès lors à vous renseigner sur la politique de conservation des données.

Le fournisseur de services de cloud chiffre-t-il les données et, si oui, de quelle manière ?
Cette information est cruciale si vous tenez à vous assurer qu'aucune des données que vous considérez comme classifiées ou confidentielles, ou qui vous préoccupent pour une raison ou une autre, ne sera exploitée à d'autres fins par le fournisseur de services de cloud.

Où les données sont-elles stockées ?
Êtes-vous soumis à des règles ou réglementations en matière de localisation du stockage des données qui doivent être respectées par les fournisseurs de services de cloud ? Les fournisseurs de services de cloud stockent les données dans un grand nombre d'endroits et à de nombreuses fins différentes. Vous devez comprendre la politique de votre fournisseur en la matière et déterminer si elle est compatible avec les pratiques de votre entreprise.

Les données sont-elles regroupées et transmises à d'autres entités internes ou externes ?
Nous savons tous que cette pratique est très répandue sur Internet et qu'il existe de nombreux programmes d'autorisation/de refus différents. Il est extrêmement important de déterminer si le fournisseur de services de cloud partage les données avec des tiers et, le cas échéant, de comprendre comment, quand et pour quelles raisons les données sont partagées, et où elles sont transmises.

Questions sur les opérations

Au-delà de la sécurité et de la confidentialité, les activités de votre fournisseur de services de cloud recouperont bon nombre des opérations quotidiennes de votre entreprise. Une bonne compréhension de ces interactions vous aidera à déterminer si la manière dont le fournisseur de services de cloud gère vos données et les met à la disposition de vos utilisateurs favorise ou affecte vos opérations.

Quel est le modèle de redondance de l'architecture de stockage et de la base de données ?
La redondance est particulièrement importante parce qu'elle régit la façon dont le fournisseur peut gérer une défaillance de l'infrastructure sans affecter la continuité des activités.

Quelle est la fréquence de sauvegarde ?
Depuis l'apparition des ordinateurs, nous avons tous eu droit à la litanie suivante : sauvegardez, sauvegardez, sauvegardez. C'est pourquoi il est crucial de connaître la fréquence à laquelle les fournisseurs de services de cloud effectuent des sauvegardes. Il va de soi que plus les sauvegardes sont fréquentes, plus la redondance est élevée, et plus il est facile pour votre fournisseur de restaurer le service à un état et un moment spécifiques en cas de défaillance.

Quel est le délai de récupération en cas de défaillance ?
Il est inévitable que votre fournisseur rencontre un problème à un moment ou un autre. Vous devez impérativement savoir combien de temps il lui faudra pour récupérer vos données. Le délai de récupération se compte-t-il en minutes, en heures, en jours, voire en semaines ? Les défaillances sont inéluctables mais lorsque vous vous appuyez sur un fournisseur de services, vous devez savoir combien de temps il lui faudra pour rétablir une situation normale.

Comment faire pour accéder aux données ou les télécharger depuis le service ?
Cette question vous permet de cerner la philosophie des différents fournisseurs de services et de déterminer si les étapes nécessaires sont compatibles ou non avec vos processus opérationnels.

Quels sont les outils analytiques disponibles pour visualiser nos données ?
Le fournisseur de services peut détenir une quantité considérable de vos données dans son service, et vous ne souhaitez pas forcément devoir les extraire toutes et utiliser des outils d'analyse tiers pour les compresser et les analyser. Idéalement, le fournisseur de services doit également proposer ce service, de façon à vous permettre d'agréger et de modéliser facilement les données.

En cas de corruption de données, à quel volume maximal de perte de données devons-nous nous attendre ?
Cette question est directement liée à celles portant sur la redondance et la récupération abordées précédemment, et doit être en adéquation avec celles-ci. Combien de temps faudra-t-il pour récupérer les données en cas de défaillance et en quoi ce processus de récupération affecte-t-il la qualité des données ?

En résumé

Les questions suggérées dans ce livre blanc visent à vous aider à identifier, à évaluer et à sélectionner des fournisseurs de services de cloud, ainsi qu'à collaborer avec. Elles vous permettent également de jauger votre processus d'évaluation continue des performances de votre fournisseur de services de cloud actuel, et servent d'outil de mesure périodique pour les nouveaux services dont vous pourriez avoir besoin à mesure que votre entreprise évolue.

Gardez à l'esprit que la sélection d'un fournisseur de services de cloud n'est pas une tâche anodine. Un mauvais choix peut avoir des conséquences graves, voire catastrophiques sur votre entreprise si le niveau de sécurité du fournisseur de services de cloud ne répond pas à vos besoins actuels et à venir. En revanche, le choix de fournisseurs de services de cloud appropriés peut bénéficier de nombreuses façons à votre entreprise : sur le plan financier, de l'allocation des ressources internes, de la confiance dans la sécurité et l'intégrité de vos données, et à bien d'autres égards.

Utilisées dans le cadre du processus d'évaluation de fournisseurs de services de cloud potentiels, ces questions sur la sécurité, la confidentialité et les opérations peuvent accroître votre confiance à l'heure de choisir vos fournisseurs de services de cloud partenaires. Il va de soi que ces questions doivent être pondérées et adaptées au modèle économique, aux priorités opérationnelles et à la culture de votre entreprise. Elles constituent toutefois un moyen efficace de choisir des partenaires adaptés lors de l'adoption de nouveaux services de cloud.

Ces questions peuvent paraître très nombreuses mais faites-nous confiance : à terme, vous serez ravi d'avoir pris le temps de les passer en revue une à une. Il est clairement préférable de disposer des informations que ces questions peuvent fournir que de devoir deviner les réponses.

Pour plus d'informations, consultez la page **www.mcafee.com/fr/solutions/secure-cloud/index.aspx**.

L'auteur

Jamie Tischart
Directeur des technologies cloud/SaaS, Intel Security

Jamie Tischart est Directeur des technologies cloud/SaaS chez Intel Security et responsable du développement des solutions de cloud de nouvelle génération d'Intel Security. Il a également pour mission d'amener Intel Security à se démarquer durablement de la concurrence. En poste chez Intel Security depuis plus de dix ans, il a occupé diverses fonctions techniques, dont celle de Directeur de l'ingénierie de cloud, des opérations et de la recherche et de Directeur de McAfee® Labs, de l'ingénierie de qualité et des opérations. Avant de rejoindre ce qui était encore McAfee, il a occupé diverses fonctions de direction, d'architecte QA, de gestion et d'ingénierie auprès de sociétés telles que MX Logic, Blackbaud, Openwave, Newbridge Networks et Corel. James Tischart est titulaire d'une maîtrise en administration des affaires obtenue à l'Université d'Aspen. Il vit avec sa famille au Colorado, où il assouvit sa passion pour le développement SaaS, les méthodologies DevOps et les opérations de cloud, et promeut le développement Agile et l'ingénierie de qualité, tout en s'adonnant au ski, à l'écriture et au hockey. Il œuvre également en tant que bénévole auprès de nombreuses organisations caritatives, dont Habitat for Humanity, Ronald McDonald House Charities of Denver, Inc. et Food Bank of the Rockies.

À propos d'Intel Security

La gamme de produits McAfee d'Intel Security est conçue pour rendre le monde numérique plus sûr pour chacun d'entre nous. **www.intelsecurity.com**. Intel Security est une division d'Intel.

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com

62487wp_questions-cloud-service-provider_0616