FIREEYE™

EBOOK

SÉCURITÉ DANS LE CLOUD : 5 MYTHES DÉCONSTRUITS

Migration vers le cloud

Les mythes passés au révélateur des faits

Le cloud a déjà séduit de nombreuses entreprises par ses promesses d'innovation et de réduction des coûts.

Côté adoption, les tendances actuelles montrent que beaucoup de grandes structures optent pour une approche mixte, à savoir une stratégie hybride combinant cloud public et cloud privé pour répondre à leurs besoins métiers. Les PME, elles, préfèrent opter pour un ou plusieurs clouds publics.

Mais malgré les avantages du cloud en termes d'agilité, son adoption crée également des tensions en interne, le plus souvent par méconnaissance et par manque d'expérience sur ce genre de solution.

Ainsi, malgré sa forte progression, la bataille entre partisans et détracteurs a vu émerger un certain nombre de mythes et idées reçues, parmi lesquelles :

- **Le cloud, c'est dangereux**
- **Mon entreprise n'utilise pas le cloud**
- **Mon fournisseur cloud assurera ma sécurité**
- **Le cloud n'est ni plus ni moins que l'ordinateur d'un autre**
- **Les cybermalfaiteurs ne s'en prennent pas au cloud**

Alors que le marché mondial du cloud public n'en finit plus de croître, l'heure de la démythification a sonné pour permettre aux organisations de prendre enfin le contrôle de leurs opérations cloud.

Mythe n° 1 : Le cloud, c'est dangereux

Le cloud n'est pas dangereux en soi. Si on sait s'en servir, il est au moins aussi sûr qu'un data center traditionnel. De toutes les missions de réponse à incident conduites par FireEye Mandiant sur des clouds publics, aucune n'a encore mis en cause l'infrastructure cloud elle-même. Dans certains cas, une mauvaise configuration ou une vulnérabilité du code client était en cause, mais nous n'avons trouvé aucune faille dans le code ou l'infrastructure du fournisseur cloud.

Comparé aux PME, les grandes entreprises semblent moins confiantes quant à la sécurité de leurs données dans le cloud public. Cette frilosité s'explique notamment par l'impossibilité de migrer en raison de la complexité du réseau ou de l'incompatibilité des systèmes et applications historiques avec les environnements de cloud public.

94 % des PME font état d'avantages en termes de sécurité depuis qu'elles ont migré vers le cloud[1]

1 Microsoft. Driving Growth Together: Small Business and the Cloud.

Mythe n° 1 : Le cloud, c'est dangereux

En général, les vulnérabilités sont introduites lors de la personnalisation d'un environnement cloud. Par exemple, lorsque vous créez un bucket de stockage avec AWS S3 ou Azure Blob Storage, ces environnements sont verrouillés par défaut et uniquement accessibles aux administrateurs et au créateur du bucket. Par contre, pour exploiter les données de ce bucket, il faut fournir un accès aux serveurs ou directement aux utilisateurs. Et c'est là que le bât blesse pour la plupart des entreprises.

Ce problème de sécurité n'est fondamentalement pas différent de ce que l'on rencontre dans les data centers traditionnels, où les erreurs de configuration, les vols d'identifiants et les failles de code constituent les principaux vecteurs d'accès non autorisés. Toutefois, dans un data center classique, les pare-feu bloquent par défaut les accès entrants aux ressources internes, alors que des services cloud (à l'exception des machines virtuelles) autorisent les trafics authentifiés quelle qu'en soit la provenance. Certains services peuvent être paramétrés de façon à n'autoriser les accès qu'à une certaine plage d'adresses IP. Mais cela n'est pas la configuration par défaut.

Un moyen de balayer cette crainte vis-à-vis du cloud consiste à s'appuyer sur le modèle Zero Trust. Rendu célèbre par Google et Microsoft, ce modèle abandonne les pare-feu au profit d'une authentification et d'une autorisation de tous les accès.

> En vérité, le cloud fait peur parce que tout le réseau Internet y a accès.

Les architectures Zero Trust éliminent l'idée d'une confiance basée sur le simple fait de se trouver à l'intérieur du périmètre d'un réseau. Au lieu de cela, elles se basent sur les niveaux de confiance que peuvent justifier les utilisateurs et leurs équipements pour octroyer ou non l'accès aux données et ressources organisationnelles.[2]

Pour les adeptes du cloud en général, et de l'approche Zero Trust en particulier, les pare-feu ont trop longtemps servi de cache-misère aux systèmes vulnérables, incitant les entreprises à sombrer dans une certaine complaisance. Ces dernières pensent, à tort, que la menace se situe forcément en dehors du périmètre du pare-feu et que, par conséquent, les systèmes vulnérables sont à l'abri. À l'inverse, le modèle Zero Trust suppose que les intrus se situent déjà à l'intérieur du périmètre et qu'il ne faut surtout pas se fier aux pare-feu.

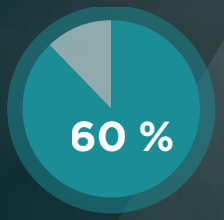
Si le modèle Zero Trust peut paraître extrême pour ce qui est des serveurs et machines virtuelles, il représente la voie à suivre pour la protection des services cloud. Sans périmètre, les services doivent considérer tous les clients comme non fiables. Et même si le code qui sous-tend ces services n'est pas vulnérable en soi, leur configuration ou leurs identifiants d'accès le sont.

2 Microsoft (14 juin 2018). Building Zero Trust Networks with Microsoft 365.

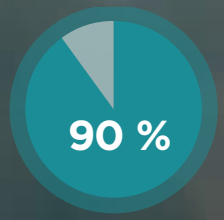
Mythe n° 2 : Mon entreprise n'utilise pas le cloud

Le terme « cloud » comprend aussi les logiciels SaaS (Software-as-a-Service). Or, la quasi-totalité des entreprises actuelles utilise ce genre de service sous une forme ou une autre : gestion des ressources humaines, transactions bancaires, expéditions, gestion de contenus, hébergement web, etc. Même si aucune politique interne n'autorise explicitement les services cloud, ou s'il n'existe aucune preuve manifeste de leur usage, votre entreprise est d'une manière ou d'une autre dans le « nuage ».

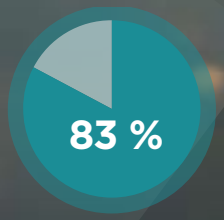
Une grande partie des entreprises sont déjà adeptes du cloud



60 % des grandes entreprises en France utilisaient des services cloud en 2018[3]



Plus de 90 % des entreprises de la région APAC exploitent ou envisagent d'exploiter un environnement multicloud[4]



D'ici la fin de cette année, les entreprises américaines devraient exécuter 83 % de leurs workloads dans le cloud[5]

3 https://www.insee.fr/fr/statistiques/4126592?sommaire=4238635#titre-bloc-10
4 451 Research (janv. 2019). Going Hybrid: Demand for Cloud and Managed Services Across Asia-Pacific.
5 Forbes (janv. 2018). 83% of Enterprise Workloads Will Be In The Cloud By 2020.

Mythe n° 2 : Mon entreprise n'utilise pas le cloud

L'un des principaux défis des experts en sécurité consiste à non seulement protéger ces services contre tout mauvais usage involontaire, mais aussi, et avant tout, à détecter leur utilisation en interne. Le manque de visibilité sur les pratiques de « Shadow IT » et l'utilisation non autorisée de services cloud sont des problématiques courantes en entreprise. Même les CASB (Cloud Access Security Brokers) sont incapables de détecter les utilisations occasionnelles (mais parfois critiques) de services cloud par des salariés depuis chez eux.

La majorité des salariés ont à un moment donné eu besoin d'utiliser un service comme Google Drive pour partager un fichier avec un interlocuteur externe. Une méthode d'accès protégé peut avoir été validée par l'entreprise. Mais en général, les processus d'autorisation créent des obstacles au bon déroulement de l'activité. C'est ainsi que, même armés des meilleures intentions, certains collaborateurs peuvent commettre certaines entorses aux politiques de sécurité.

La solution à ce problème passe par deux axes :

Une méthode validée par l'entreprise permettant aux salariés d'atteindre leurs objectifs.

Une visibilité et des contrôles appropriés sur les services cloud autorisés.

La sécurité du cloud est avant tout une question de visibilité. Lorsqu'un développeur déploie un nouveau service cloud, il doit être en mesure de facilement centraliser les données de télémétrie correspondantes. Les analystes peuvent ainsi vérifier l'état de sécurité de tous les services cloud sur une seule et même console.

Côté conformité, la meilleure manière de se mettre en règle consiste à encourager les développeurs à se rapprocher des équipes de sécurité, et non l'inverse. Et pour cela, la télémétrie doit également servir à la surveillance opérationnelle. Autrement dit, elle doit être aussi utile à la sécurité qu'aux opérations.

Une visibilité sur tous les services cloud ne sera peut-être pas toujours possible. L'hermétisme de certains services pourra empêcher toute télémétrie, tandis que d'autres proposeront ce service uniquement en option. Par exemple, la version "Premium" de Microsoft Azure Active Directory ne permet de voir que les journaux de connexion, tandis que Salesforce exige l'achat de sa version "Shield" pour pouvoir consulter les données d'audit. Peu importe la facilité avec laquelle les développeurs de votre entreprise accèdent à leur télémétrie, ils pourront toujours avoir des raisons (bonnes ou mauvaises) de ne pas le faire. Le seul fait d'être mis au courant de l'utilisation de certains services cloud est déjà une bonne chose en soi, surtout pour la modélisation des menaces (c.-à-d. imaginer le déroulement d'une attaque).

Mythe n° 3 :
Mon fournisseur cloud assurera ma sécurité

Dans le cadre du modèle de responsabilité partagée, le locataire (c.-à-d. le client) est l'ultime gardien de ses données. Le rôle du fournisseur cloud est de garantir la sécurité de sa propre infrastructure, l'intégrité du matériel, et la protection des systèmes d'exploitation et logiciels qui sous-tendent les services offerts. De fait, c'est au client que revient la responsabilité d'appliquer les correctifs sur les machines virtuelles, de combler les failles sur ses applications et d'établir les permissions adéquates.

La sécurisation du cloud se décline en trois grandes parties :

- **Protection des identifiants d'accès aux ressources et détection d'éventuelles compromissions**
- **Prévention des erreurs de configuration**
- **Centralisation des données de télémétrie pour la surveillance et les audits de sécurité**

Mythe n° 3 : Mon fournisseur cloud assurera ma sécurité

Les fournisseurs cloud proposent de nombreux outils intégrés en natif, mais le gros des responsabilités demeure entre les mains des clients des services cloud. Par exemple, un fournisseur cloud peut offrir des outils de détection des configurations à risque ou de rétablissement à un état antérieur (rollback), mais c'est aux clients d'intégrer ces outils aux politiques et procédures de leur entreprise. C'est également à eux d'aligner ces outils sur les systèmes de visibilité et de contrôle de sécurité appliqués à tout autre service cloud de l'entreprise.

Par ailleurs, les fournisseurs cloud ne maîtrisent pas forcément la nature des métiers de chaque client. C'est pourquoi les questions de conformité restent au final du ressort de l'entreprise cliente.

D'ici 2022, au moins 95 % des failles de sécurité dans le cloud seront de la faute du client.[7]

Tous les points de partage des données au-delà les limites de l'entreprise constituent une faille potentielle dans le dispositif de défense, car les accès doivent d'abord être autorisés, puis audités, plutôt qu'uniformément refusés. Chaque point d'accès se transforme ainsi en un travail d'audit pour l'équipe de sécurité qui doit également bénéficier d'une visibilité complète pour s'assurer que toutes les données accessibles font l'objet d'autorisations appropriées.

Cette visibilité se traduit par un accès direct et programmatique des équipes de sécurité à toutes les données de télémétrie, qu'elles peuvent par la suite réexploiter pour leurs procédures opérationnelles standard. Cela va bien au-delà d'audits ponctuels pour s'étendre à la surveillance continue d'éventuelles anomalies.

6 Gartner (oct. 2019). Clouds Are Secure: Are You Using Them Securely?

Mythe n° 4 : Le cloud n'est ni plus ni moins que l'ordinateur d'un autre

Sécuriser le cloud, ce n'est pas pareil que sécuriser un ordinateur situé dans le data center de quelqu'un d'autre. La réponse à une simple demande peut mobiliser des centaines, voire des milliers d'ordinateurs pendant quelques microsecondes. Il ne s'agit pas d'un seul serveur stockant votre fichier dans un environnement statique, mais de dizaines de serveurs dans une configuration hyper-dynamique. Outre les machines virtuelles, il faut également tenir compte des services de stockage, des containers et d'autres services non traditionnels. Ces derniers peuvent être composés de centaines, voire de milliers de serveurs répartis sur une multitude de data centers, tout cela pour traiter une seule et même demande de service.

Côté sécurité, les analyses forensiques, qui procédaient autrefois serveur par serveur, doivent désormais s'effectuer sur ces environnements hyper-distribués. Il faut donc davantage de visibilité et de planification pour fournir les contrôles et instruments de sécurité nécessaires. Il se peut aussi que ces services propose une API, mais les concepts relatifs aux adresses IP et aux systèmes d'exploitation ne s'appliquent généralement pas.

Mythe n° 4 : Le cloud n'est ni plus ni moins que l'ordinateur d'un autre

Les contrôles et configurations de sécurité de ces services ne s'appuieront pas sur des dispositifs traditionnels comme les pare-feu et les antivirus.

Par ailleurs, des exigences en matière de chiffrement peuvent obliger certains services à chiffrer les données stockées. Tous les principaux services cloud utilisent le protocole SSL/TLS pour les communications, mais lorsque les données sont soumises à de strictes réglementations, il est tout aussi important de savoir où les données sont écrites d'un service à un autre.

L'élasticité intrinsèque du cloud peut également soulever de nouvelles problématiques de protection des ressources contre les utilisations abusives ou malveillantes. Dans un data center traditionnel, une application est rattachée à une quantité définie de ressources. On peut utiliser cela comme un filet de sécurité en cas d'utilisation abusive d'un service exposé publiquement : l'application cessera de fonctionner et sera réduite à un état de service refusé. En revanche, une application développée dans le cloud sur des ressources élastiques (groupes « Auto Scaling », fonctions sans serveur, containers, etc.) continuera à monter en capacité au lieu de s'arrêter. C'est en général une bonne chose pour une utilisation légitime, mais les conséquences peuvent être désastreuses en cas de requêtes malveillantes.

Exemple : si une application de traitement photo reçoit une avalanche de requêtes indésirables, elle pourra certes uploader toutes les photos sans problème, mais ce sera au propriétaire de l'appli d'en payer les conséquences. Les infrastructures cloud affichent certaines limites dans leurs capacités à gérer ce genre de problématique. Il faut donc en être conscient et prendre les dispositions nécessaires à l'avance.

Mythe n° 5 : Les cybermalfaiteurs ne s'en prennent pas au cloud

Les attaquants vont là ont sont les données. Si elles sont dans le cloud, ils iront dans le cloud. Près d'un quart des missions de réponse à incident (IR) de Mandiant concernent des ressources hébergées sur un cloud public, et presque toutes ont un rapport plus ou moins direct avec un cloud public. Le cloud n'est nullement un obstacle pour les attaquants. Ils n'ont aucune difficulté à adapter leurs modes opératoires pour compromettre des comptes cloud et ainsi accéder à des données confidentielles, détourner des ressources informatiques ou encore espionner leurs cibles.[8].

N'importe quelle entreprise peut gagner en flexibilité et réduire ses coûts grâce au cloud. Mais elle doit également être consciente que toute ressource qu'elle y stocke devient une cible potentielle et doit être protégée en conséquence. Concrètement, il s'agit pour elle d'appliquer de bonnes pratiques de sécurité de base, mais pas seulement. Elle doit aussi donner à ses équipes de sécurité les moyens de traquer activement les attaquants qui cherchent à accéder aux données stockées dans le cloud.

Près d'un quart des missions de réponse à incident (IR) de Mandiant concernent des ressources hébergées sur un cloud public.

8 FireEye (février 2020), M-Trends 2020

Mythe n° 5 : Les cybermalfaiteurs ne s'en prennent pas au cloud

La neutralisation de ces menaces passe d'une part par les données de télémétrie servant à alimenter les opérations de sécurité, et d'autre part par des modèles de menaces qui définissent les outils, tactiques et procédures des attaquants à traquer. Tout ceci peut être reparti en quatre catégories de fonctionnalités :

Threat Intelligence
Application d'indicateurs de Threat Intelligence aux données de télémétrie

Règles
Application de schémas de menaces connus aux données de télémétrie

Analytique
Organisation de la télémétrie pour mettre en évidence les anomalies

Traque
Recherche basée sur des hypothèses

Ensemble, ces fonctionnalités peuvent assurer la protection d'une entreprise contre les menaces connues et repérer des comportements symptomatiques de nouvelles menaces. Bien que certaines de ces activités (Threat Intelligence, règles et analytique) soient automatisées, toutes nécessitent une intervention humaine à un moment donné pour prendre la mesure des événements les plus graves.

Traquer les menaces exige de mettre en place des équipes de sécurité expérimentées, capables d'utiliser leurs connaissances sur des groupes d'attaquants spécifiques et d'opérer une distinction claire avec ce qu'il faut considérer comme "normal" dans les données de télémétrie. Par exemple, si une politique indique que toutes les ressources cloud doivent être instanciées à partir de modèles, la traque pourra consister à examiner toutes les ressources créées sans modèle. Si cette traque est suffisamment simple à engager et apporte des résultats, elle pourra être convertie en règle afin d'être automatisée.

Conclusion

Le cloud permet aux structures de toutes tailles de faire plus avec moins, tout en bénéficiant d'une évolutivité quasi illimitée. Mais attention : le cloud comprend aussi sa part de risques auxquels il faut se préparer pour repousser les attaques avancées et protéger vos données dès le premier jour. Si le déploiement d'une stratégie cloud est relativement simple, il ne faut surtout pas sous-estimer la complexité des aspects sécurité et gestion. Les erreurs de configuration et le manque de visibilité sur l'ensemble de l'environnement cloud peuvent avoir des conséquences coûteuses.

Les opérateurs cloud doivent certes veiller à la sécurité de leurs infrastructures, mais c'est aux utilisateurs de protéger leurs données. Cette responsabilité partagée entre le fournisseur et l'utilisateur peut entraîner des problèmes de visibilité et de contrôle. C'est là qu'une plateforme de sécurité centralisée prend tout son sens. Elle donnera aux organisations toute la visibilité nécessaire pour identifier clairement les problèmes potentiels, satisfaire aux exigences de conformité et prendre les décisions garantes de la protection des données.

Les ressources cloud ont des spécificités qui imposent des outils de protection dédiés et spécialisés. D'où l'importance pour les professionnels de la sécurité de miser sur ces nouveaux outils et de se former pour tenir le rythme dans cet environnement en perpétuelle mutation.

Pour en savoir plus sur la sécurité dans le cloud, rendez-vous sur **www.FireEye.com/cloud**

FireEye, Inc.
Nextdoor Cœur Défense,
110 Esplanade du Général de Gaulle,
92931 Paris La Défense Cedex 92974
+33 1 70 61 27 26
france@FireEye.com

À propos de FireEye, Inc.

FireEye est spécialisé dans la cybersécurité axée sur la Cyber Threat Intelligence (CTI). Prolongement naturel et évolutif des opérations de sécurité des clients, la plateforme unique de FireEye combine des technologies de sécurité innovantes, des services de CTI d'envergure internationale et les services réputés de Mandiant® Consulting. FireEye simplifie ainsi la cybersécurité et son administration, devenant un allié précieux des entreprises confrontées au casse-tête que représentent la prévention et la neutralisation des cyberattaques.

FIREEYE™