

La sécurité empêche-t-elle d'atteindre le plein potentiel du Cloud ?

Sécurité

Posté par : JPilo

Publié le : 11/2/2022 15:00:00

La décision à laquelle sont confrontées les entreprises aujourd'hui n'est pas de savoir si elles doivent déplacer les applications et l'infrastructure dans le Cloud, mais quel Cloud utiliser.

Dans son rapport 2021 sur l'état du Cloud, Flexera a constaté que 92 % des utilisateurs du Cloud ont une stratégie multi-cloud.

Cependant, ces mêmes décideurs reconnaissent que passer au multi-cloud s'accompagne de nombreux défis.

Plus précisément, le rapport de Flexera note que 81 % de ces décideurs considèrent la sécurité et la conformité comme le principal obstacle à l'obtention de tous les avantages du Cloud public.

Qu'on le veuille ou non, ces décideurs ont raison. A mesure que les clouds deviennent plus complexes et que Kubernetes devient plus omniprésent, les réseaux deviendront ingérables sans automatisation de la sécurité.

A l'heure actuelle, la sécurité est perçue comme le maillon faible de la chaîne DevOps, et non sans raison.

Le développement d'applications agiles nécessite des changements continus, notamment des modifications des contrôles d'accès.

S'il faut des jours aux équipes réseau et sécurité pour examiner et approuver (ou refuser) ces modifications, le processus tombe en panne. Et c'est exactement ce qui se passe dans les entreprises du monde entier.

La solution n'est pas de contourner la sécurité. Et ce n'est certainement pas pour limiter les investissements dans le cloud.

Les entreprises ont initialement adopté le Cloud pour réduire leurs coûts, mais ont réalisé au fil du temps que même s'ils ne réalisaient pas d'économies significatives, le Cloud pouvait offrir un avantage concurrentiel en accélérant la mise sur le marché, en améliorant la satisfaction des clients grâce à des réponses plus rapides et en répondant à l'évolution du marché.

A une époque où la plupart des entreprises se considéraient comme étant avant tout numériques, elles ont besoin de l'agilité du Cloud, mais elles doivent également reconnaître que le Cloud s'accompagne de nouveaux défis en matière de sécurité.

Concilier l'agilité avec la sécurité

Au fur et à mesure que le réseau s'étend dans le cloud, la surface d'attaque augmente également. Traditionnellement, les entreprises ont déployé davantage de pare-feux pour sécuriser les points du réseau ainsi que, plus récemment, la segmentation du réseau. Mais cette approche entraîne une complexité et des coûts de gestion supplémentaires.

Une solution de gestion de politique de sécurité centralisée et automatisée peut concilier sécurité et agilité dans un monde multi-cloud hybride.

Avec une couche de gestion de la sécurité centralisée qui se trouve au-dessus de toute l'infrastructure, les entreprises peuvent facilement visualiser, analyser, créer et mettre en œuvre des politiques de sécurité sur l'ensemble du réseau hybride.

Une fois automatisées, les politiques de sécurité peuvent être intégrées au processus de modification du réseau et intégrées aux flux de travail ITSM, de sorte que les modifications de sécurité puissent être examinées et approuvées/refusées en seulement quelques minutes.

Les avantages de l'automatisation des politiques de sécurité

Apporter de l'agilité à la sécurité, qui change la donne pour les entreprises qui luttent pour rationaliser la transformation numérique et souffrent de changements complexes à mettre en œuvre.

Fournir une meilleure visibilité de la sécurité dans l'ensemble de l'entreprise, qu'une application soit hébergée dans un datacenter ou sur l'une des nombreuses plateformes cloud.

Autoriser les équipes réseau et sécurité à intégrer la sécurité dans le processus DevOps sans compter sur les développeurs pour configurer les paramètres.

Faciliter le concept de conformité continue, où les politiques de sécurité peuvent être rapidement mises à jour et appliquées de manière cohérente pour répondre à l'évolution des exigences réglementaires et commerciales.

A l'heure actuelle, la plupart des entreprises sont coincées entre le marteau et l'enclume : sécurisées, mais lentes, ou agiles, mais risquées. Il faut créer un terrain qui équilibre sécurité et agilité grâce à l'automatisation.

L'objectif de chaque organisation devrait être d'apporter la sécurité dans ses processus de développement agiles, où que ces processus se déroulent : dans le Datacenter, dans un cloud privé ou dans les clouds publics.

Stéphane HAURAY chez TUFIN