6 façons de renforcer la sécurité grâce au cloud computing

Le cloud computing oblige les entreprises à choisir entre, d'une part, la rentabilité, la flexibilité et la commodité offertes par ce type d'environnement, et, d'autre part, le confort que représente l'hébergement des données et des applications sur ses propres serveurs sécurisés. Mais, l'hébergement sur site est-il vraiment plus sûr que le cloud computing ? De nombreux experts pensent que non. Voici six arguments qui vous montreront pourquoi vous pouvez passer sans crainte au cloud computing.

1 La sécurité coûte cher

La sécurité représente un investissement important. Alors, demandez-vous combien votre entreprise peut se permettre de dépenser dans ce domaine. Il s'avère que le coût du déploiement d'un système de sécurité adapté à votre datacenter sur site est prohibitif, surtout pour une PME. En outre, il est quasiment impossible d'atteindre ainsi un niveau de sécurité comparable à celui que proposent les hyperscalers.

2 La sécurité monopolise vos équipes

La gestion de la sécurité requiert l'embauche de spécialistes supplémentaires. Les fournisseurs de cloud à grande échelle emploient des équipes de sécurité 24 h/24, 7 j/7. Ils disposent également d'un centre opérationnel de sécurité complet qui surveille en permanence les infrastructures et le matériel sous leur responsabilité. À titre d'exemple, Microsoft Azure est protégé par une équipe de plus de 3 500 experts en cybersécurité. La plupart des entreprises ne disposent pas du personnel nécessaire pour assurer le même niveau de sécurité que les hyperscalers.

3 Les fournisseurs de cloud sont spécialisés dans la sécurité

La sécurité est importante à vos yeux, mais ce n'est pas votre cœur de métier. Pour vous, il s'agit d'une préoccupation parmi d'autres, tandis qu'elle constitue une priorité absolue pour les fournisseurs de cloud. En fait, s'ils souhaitent rester compétitifs et conserver leur clientèle, les fournisseurs de cloud doivent offrir le plus haut niveau de sécurité possible. Par exemple, Google Cloud propose une « infrastructure sécurisée dès la conception » avec systèmes de protection intégrés et chiffrement des données par défaut[1].

Microsoft Azure contribue à l'identification des menaces en ligne « en analysant de vastes sources, notamment 18 milliards de pages web Bing, 400 milliards d'e-mails, 1 milliard de mises à jour d'appareils Windows et 450 milliards d'authentifications mensuelles »[2], à l'aide de l'apprentissage automatique, de l'analyse comportementale et des informations recueillies via les applications grâce à la fonctionnalité Microsoft Intelligent Security Graph.

Les fournisseurs de cloud doivent également respecter les normes les plus strictes, détenir des certifications émises par des organismes internationaux indépendants et se soumettre à différents programmes rigoureux d'audit menés au niveau de leurs équipes ainsi que de leurs processus et technologies de sécurité. Amazon Web Services (AWS), par exemple, fait régulièrement appel à un organisme tiers pour la validation de plusieurs milliers de critères associés à des normes de conformité internationales. La plupart des entreprises ne disposent pas du temps, des ressources ou du budget nécessaires pour atteindre un tel niveau de sécurité[3].

1 *« Confiance et sécurité » Google, consulté le 29 avril 2022.*

2 *« Renforcez votre posture de sécurité avec Azure » Azure, consulté le 29 avril 2022.*

3 *« Sécurité dans le cloud AWS », Amazon, consulté le 29 avril 2022.*

4 Outils de sécurité avancés

Les fournisseurs de cloud peuvent déployer un arsenal avancé d'outils de sécurité pour protéger les applications et les données de leur clientèle. AWS fournit notamment des contrôles d'identité et d'accès d'une grande précision, une surveillance continue, ainsi que des systèmes de détection des menaces, de protection du réseau et des applications, sans oublier des couches de chiffrement multiples et des mécanismes automatisés de résolution d'incidents et de récupération. Les hyperscalers donnent accès à des centaines de solutions de sécurité complémentaires disponibles auprès de leurs partenaires. Il est pratiquement impossible de rassembler un ensemble d'outils de sécurité aussi avancés dans votre propre réseau et datacenter. Le coût, le personnel, le temps et les efforts nécessaires représentent des investissements trop importants pour une entreprise qui n'est pas spécialisée dans la sécurité.

5 Segmentation du réseau

Les environnements cloud offrent automatiquement un autre avantage : l'isolation des postes de travail des utilisateurs. Une méthode courante de cyberattaque consiste à cibler des utilisateurs précis sur un système par le biais d'e-mails ou via des sites web. Pour pénétrer dans le système, les pirates passent par les postes de travail des utilisateurs.

Dans un environnement cloud, en revanche, les postes de travail disposent uniquement de la connectivité nécessaire pour permettre aux utilisateurs de travailler. Ils n'ont pas d'accès direct au réseau de l'entreprise. Ainsi, même si un poste de travail est compromis, le pirate ne peut pas s'en servir pour accéder au reste de l'entreprise, à ses applications, ni à ses données.

6 Sécurité physique

La sécurité physique reste un enjeu majeur. Les personnes qui disposent d'un accès physique direct à votre matériel informatique présentent potentiellement un sérieux risque de sécurité. Si vos données et applications se trouvent dans un environnement cloud, elles ne seront plus accessibles et ne risqueront plus de subir des attaques volontaires de la part, par exemple, d'un employé malveillant, ou des dommages accidentels d'une personne tierce intervenant dans vos locaux. En effet, il est bien plus difficile de localiser des données dans un environnement cloud.

En outre, les hyperscalers disposent des ressources nécessaires pour empêcher le vol physique des données, notamment des agents de sécurité, des cages de serveurs et d'autres systèmes de sécurité physique de pointe dont la plupart des entreprises ne disposent pas.

En savoir plus

Lisez le livre blanc « Empowering developers through cloud services » pour en savoir plus sur la façon dont Red Hat® Cloud Services peut vous aider tout au long de votre parcours d'adoption des applications cloud-native.

À propos de Red Hat

Red Hat aide ses clients à standardiser leurs environnements, à développer des applications cloud-native et à intégrer, automatiser, sécuriser et gérer des environnements complexes en offrant des services d'assistance, de formation et de conseil primés.

facebook.com/redhatinc
@RedHatFrance
linkedin.com/company/red-hat

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)
00800 7334 2835
europe@redhat.com

FRANCE
00 33 1 41 91 23 23
fr.redhat.com

fr.redhat.com
#F31540_0522