

Cloud sécurisé : 5 plateformes au top, selon Forrester

Les fournisseurs étudiés et classés dans le rapport [Forrester Wave*](#) (payant) génèrent au moins 50 millions de dollars de revenus par an chacun grâce à leur offre de sécurité native cloud dédiée, rapporte [CRN](#). Ils doivent également afficher une croissance d'au moins 15% par an pour cette activité et déclarer 3000 organisations clientes ou plus en production.

Les capacités de sécurité native de plateformes de cloud public ont été évaluées en fonction de 37 critères répartis en trois catégories (offre, stratégie, présence sur le marché).

Partant de là, la société américaine d'études de marché a retenu et classé 7 fournisseurs cloud d'infrastructure en tant que service ([IaaS](#)). Le classement au T2 2018 est le suivant :

Les plateformes cloud du top 5

1. **Google** Cloud (son offre est notée 4,5 sur 5 ; stratégie : 4,18 sur 5 ; marché : 3,8 sur 5).

Le plus : Google propose de nombreuses certifications de sécurité et s'appuie sur un vaste écosystème de partenaires, selon Forrester. De plus, sa plateforme offre un support natif étendu pour les systèmes d'exploitation (OS) invités et les conteneurs Kubernetes.

Le moins : le contrôle d'accès basé sur les rôles peut être complexe. Google Cloud Platform n'offre pas encore de modules de sécurité matériels, mais cela devrait bientôt changer.

2. **AWS** (Amazon Web Services) (offre : 4,9 sur 5 ; stratégie : 3,64 ; marché : 4,2).

Le plus : la flexibilité de la console d'administration AWS pour la gestion d'identité et d'accès. La robustesse d'Amazon Virtual Private Cloud (VPC).

Le moins : AWS Key Management Service (KMS) est plus difficile à utiliser que les outils concurrents, toujours selon Forrester.

3. **Microsoft** Azure (offre : 3,6 sur 5 ; stratégie : 3,2 ; marché : 4,6).

Le plus : les administrateurs Windows peuvent s'appuyer sur les scripts PowerShell pour une grande partie des fonctionnalités de sécurité de la console de gestion Azure.

Le moins : l'authentification multifacteur et le paramétrage de l'administration basée sur les rôles dans la console Microsoft n'est pas simple, estime la société d'études.

4. **Alibaba** Cloud (offre : 3,1 sur 5 ; stratégie : 2,92 ; marché : 2,6).

Le plus : Alibaba Cloud fournit un chiffrement efficace pour les OS invités.

Le moins : la plateforme n'est pas encore certifiée ISO 270017/19 (sécurité cloud public).

5. **IBM** Cloud (offre : 2,4 sur 5 ; stratégie : 3,04 ; marché : 3,4).

Le plus : IBM Cloud dispose d'un ensemble étendu de certifications de conformité réglementaire et d'un vaste écosystème de partenaires d'intégration.

Le moins : Big blue peut manquer de transparence sur les tarifs, relève le cabinet d'études.

Les fournisseurs à la traîne

6. **CenturyLink** Cloud (offre : 2,4 sur 5 ; stratégie : 2,24 ; marché : 1,4).

Le plus : le support de l'hyperviseur VMware ESX et de la technologie d'automatisation Ansible (Red Hat).

Le moins : CenturyLink est à la traîne en ce qui concerne le stockage chiffré, la prise en charge des conteneurs et la gestion des identités et des accès.

7. **Rackspace** (offre : 1,82 sur 5 ; stratégie : 2 ; marché : 2,4).

Le plus : Rackspace propose son propre système de gestion de conteneurs Carina.

Le moins : la configuration et la gestion de la politique de sécurité native de la plateforme.

Forrester adresse son rapport aux responsables de la sécurité informatique et aux professionnels de la gestion du risque. Pour les aider à « faire le bon choix ».

**Forrester Wave : Public Cloud Platform Native Security, Q2 2018.*

(crédit photo © Shutterstock)