***SÃ©curiser le cloud hybride : mission impossible ?***
**SÃ©curitÃ©**
PostÃ© par : JerryG
PubliÃ©e le : 18/3/2024 15:00:00

Selon la 5e Ã©dition du rapport Enterprise Cloud Index de Nutanix publiÃ©e en 2023, les entreprises franÃ§aises sont en transition progressive vers le cloud hybride, et sont 57% Ã  avoir recours Ã  plusieurs modes dâ□□exploitation informatique.Â
Une tendance qui ne sâ□□observe pas quâ□□en France : ainsi, Alstom a rÃ©cemment fait part de sa volontÃ© dâ□□approfondir sa stratÃ©gie de cloud hybride ; Cisco sâ□□est alliÃ©e Ã  Hitachi Vantara en vue de dÃ©velopper la leur, et HPE a rÃ©cemment annoncÃ© la crÃ©ation dâ□□un dÃ©partement dÃ©diÃ© Ã  lâ□□hybridation.

Certes, la stratÃ©gie de cloud hybride, qui combine des dÃ©ploiements Ã  la fois publics et privÃ©s, sâ□□impose de plus en plus puisquâ□□elle peut offrir flexibilitÃ©, personnalisation et conformitÃ© le tout, Ã  moindre coÃ»t. En revanche, cette stratÃ©gie complexifie grandement la cybersÃ©curitÃ© des entreprises.Â
Câ□□est pourquoi, la sÃ©curitÃ© du cloud hybride doit englober un ensemble de politiques et technologies visant Ã  protÃ©ger les donnÃ©es, les applications et l'infrastructure associÃ©es Ã  cet environnement.

Mais comment sâ□□y prendre ?Â

Yann Samama, Senior Engineer chez Gigamon France, dÃ©voile quelques clÃ©s de comprÃ©hension pour rÃ©pondre Ã  cette problÃ©matique :

Â Â« Une sÃ©curitÃ© efficace du cloud hybride est essentielle en raison de la complexitÃ© inhÃ©rente Ã  ces environnements, des mouvements frÃ©quents des donnÃ©es entre le cloud public et privÃ©, du modÃ¨le de responsabilitÃ© partagÃ©e avec les fournisseurs de cloud public, et des exigences de conformitÃ© rÃ©glementaire. Les avantages de la sÃ©curitÃ© du cloud hybride incluent donc une meilleure sÃ©curitÃ© grÃ¢ce Ã  la segmentation, permettant l'isolation des donnÃ©es sensibles dans le cloud privÃ© tout en profitant de la scalabilitÃ© et de la rentabilitÃ© du cloud public. De plus, cela offre une base robuste pour la continuitÃ© des activitÃ©s et la reprise aprÃ¨s sinistre Â».

Toutefois, selon Yann Samama, la sÃ©curitÃ© du cloud hybride reste aujourdâ□□hui perfectible : Â« des dÃ©fis subsistent : la complexitÃ© et les risques liÃ©s Ã  l'utilisation de plusieurs clouds restent des prÃ©occupations majeures pour les experts de la sÃ©curitÃ© informatique. De mÃªme, le cloud hybride complexifie la bonne confidentialitÃ© des donnÃ©es et de conformitÃ©. Enfin, maintenir une connectivitÃ© transparente entre les clouds public et privÃ© demeure un autre enjeu de taille.Â

Afin sâ□□affranchir de ces contraintes, Yann Samama dÃ©voile plusieurs conseils : Â« les entreprises doivent dâ□□abord anticiper le contexte Ã©volutif qui les entoure, tel que lâ□□accÃ©lÃ©ration de lâ□□IA gÃ©nÃ©rative pour la cybersÃ©curitÃ©, lâ□□adoption accrue de la souverainetÃ© du cloud en Europe - via la directive Nis2 et la Cybersecurity Act -, ou encore la tenue de manifestations sportives dâ□□envergure tels que les JO de Paris. Ensuite, il convient mettre en place une stratÃ©gie de sÃ©curitÃ© holistique, câ□□est-Ã -dire : renforcer les contrÃ´les d'accÃ¨s et la gestion des identitÃ©s, surveiller en continu et en temps rÃ©el, et adopter l'automatisation pour amÃ©lioration de l'efficacitÃ© opÃ©rationnelle. Toutefois, gardons en tÃªte que mettre en place cette stratÃ©gie holistique nÃ©cessite en premier lieu de bÃ©nÃ©ficier dâ□□une parfaite visibilitÃ© de son infrastructure IT et de son rÃ©seau informatique. Câ□□est lÃ  que lâ□□observabilitÃ© entre en jeu Â».Â

La sÃ©curitÃ© du cloud hybride passe donc par le dÃ©veloppement de solutions dâ□□observabilitÃ© avancÃ©e que Gigamon propose , en vue d'obtenir des insights approfondis, de surveiller le trafic rÃ©seau en temps rÃ©el et de dÃ©tecter les menaces de faÃ§on proactive.Â