Environnements hybrides et multi-clouds : un défi et une chance pour la cybersécurité

Hormis quelques pionnières dans le all-cloud, la plupart des entreprises font cohabiter des systèmes qui leur sont propres avec des ressources opérées dans le cloud par un ou plusieurs fournisseurs. Ces environnements hybrides et multi-clouds posent de nouveaux défis en matière de cybersécurité mais, paradoxalement, ils offrent aussi l'opportunité de renforcer ses pratiques et d'accéder à de meilleurs outils.

De nouvelles menaces

Accélérée notamment par l'essor du télétravail et l'utilisation croissante de logiciels en mode SaaS, l'expansion du système d'information hors du data center est assurément une source de nouvelles menaces. Avec une surface d'exposition démultipliée, l'entreprise est plus vulnérable aux fuites et aux vols de données, qui débutent souvent par ceux des identifiants des utilisateurs via des techniques de phishing ou de password spraying. Elle perd aussi une partie du contrôle que lui apportait la sécurité périmétrique, par exemple sur les données techniques, très prisées des hackers.

Enfin, les environnements hybrides créent des risques spécifiques, liés par exemple à l'hétérogénéité des dispositifs de sécurité ou à la multiplicité des interconnexions, lesquelles peuvent permettre à des malwares ou ransomwares de se propager.

Ces risques ne doivent cependant pas dissuader les entreprises de poursuivre leur adoption du cloud. D'une part, parce qu'ils ne sauraient faire oublier les bénéfices qu'elles peuvent en attendre en termes d'innovation, de croissance et de compétitivité. Et, d'autre part, parce que des réponses existent, dont beaucoup proviennent de la démocratisation et l'accessibilité des outillages de sécurités proposés par les Cloud Provider eux-mêmes.

En revanche, les infrastructures hybrides et multi-clouds imposent de revoir un modèle de sécurité qui était conçu pour le « on-premise » et dont il faut faire évoluer les organisations, les architectures et les outils.

Organisation : décentraliser les responsabilités

L'un des principaux avantages du cloud réside dans l'autonomie qu'il donne aux équipes, qui peuvent explorer de nouvelles idées à moindre coût. Mais si les développements sont facilités, les sécuriser convenablement est plus délicat. Or, l'équipe sécurité n'a ni les ressources ni l'agilité pour intervenir partout comme il le faudrait. Il faut donc décentraliser les responsabilités et les confier en partie aux équipes projets. Ceci est d'autant plus souhaitable – et faisable – que le cloud permet de différencier davantage les mesures de sécurité et de les imputer avec précision.

Les équipes projets (DevOps ou classiques) doivent être formées pour intégrer la sécurité dès la phase de conception (approche « security by design »), des outils de sécurité doivent être intégrés

aux pipelines de développement, et, il est primordial de nommer des relais dans les équipes, les fameux « Security Champions ».

Architecture : clarifier les relations avec les fournisseurs de cloud

Pour sécuriser les environnements hybrides et multi-clouds, il faut commencer par clarifier le partage des responsabilités entre le cloud provider et l'entreprise pour que celle-ci sache exactement ce qui lui incombe. On s'interrogera aussi sur le niveau de confiance que l'on accorde à ce fournisseur, et donc sur les mesures de protection à prendre y compris vis-à-vis du fournisseur lui-même.

Enfin, il faut identifier les services que l'on souhaite utiliser et les passer au crible des exigences réglementaires (RGPD, données de santé…). Une fois ce cadre posé, on pourra s'attacher à transposer dans le cloud les règles d'architecture en vigueur, par exemple en matière de gestion des identités ou de cloisonnement des réseaux.

Technologie : utiliser au maximum les outils proposés par les cloud providers

D'emblée confrontés à la défiance des entreprises, les grands opérateurs de cloud ont massivement investi en cybersécurité, de sorte qu'ils proposent aujourd'hui des outils performants, accessibles et très bien intégrés à leurs services.

Le cloud permet ainsi à des entreprises aux moyens et aux compétences limitées d'accéder à des fonctionnalités et/ou à des niveaux de protection inédits : anti-DDos, load balancing, authentification multi-facteurs, gestion des certificats… Il facilite également la mise en place d'approches Zero Trust, indispensables dans les environnements interconnectés et difficilement contrôlables. Enfin, il démocratise les outils d'intelligence artificielle/machine learning que développent les plateformes pour anticiper les risques.

Dès l'origine, et encore aujourd'hui, la sécurité est apparue comme l'un des freins majeurs à l'essor du cloud. Pourtant, en soulevant de nouvelles questions, le cloud a contribué à faire sortir la cyber-sécurité de l'entre-soi des experts. Même s'il reste du chemin à parcourir, la maturité sur ce sujet a considérablement progressé au sein des organisations au cours des dernières années et le niveau global de protection s'est nettement renforcé.

En prenant à bras-le-corps les défis posés par les environnements hybrides et multi-clouds, les entreprises ont aujourd'hui l'opportunité de franchir une nouvelle étape.