Sécurité du Cloud : quelles sont les capacités indispensables d'un Next-Gen CASB ?

Selon le Gartner, 60 % des grandes entreprises utiliseront une solution de type Cloud Access Security Brokers (CASB) pour régir leurs services Cloud d'ici 2020, contre moins de 10 % aujourd'hui1. Elles l'utilisent notamment pour appliquer les politiques de gouvernance et de conformité propres à l'utilisation des environnements Cloud.

Au-delà de cet aspect, les entreprises prennent également en compte la capacité des solutions CASB à évoluer, à s'intégrer à l'infrastructure existante et à répondre aux exigences en matière de confidentialité des données lors de l'évaluation des différentes offres du marché. Dans le cadre de la mesure d'une solution à maintenir la sécurité et la confidentialité des données des clients, les RSSI évoquent souvent la faculté de la solution à fournir des capacités de contrôle d'accès basé sur les rôles (RBAC).

Le RBAC : un incontournable dans le déploiement du CASB en entreprise

Comme pour les systèmes RBAC traditionnels, les capacités de contrôle d'accès basé sur les rôles au sein d'un CASB réglementent l'accès à des caractéristiques du produit spécifiques en fonction des rôles assignés aux différents profils d'utilisateurs. En entreprise, la personne qui gère les incidents de politique DLP (Data Loss Prevention) peut être différente de celle qui les définit, nécessitant donc des capacités de segmentation ou de séparation des rôles d'administration.
De même, l'utilisateur qui traite les analyses de l'utilisation Cloud de l'entreprise et génère des rapports peut être différent de l'administrateur de sécurité qui régit l'accès à aux applications Cloud. Un administrateur peut attribuer des rôles distincts au sein d'un CASB – au même titre que pour l'ensemble des solutions de sécurité -pour chacun de ces utilisateurs, de sorte qu'ils ne puissent accéder qu'à la fonction du service qui leur est autorisée.

La séparation des rôles en matière de sécurité est souvent un prérequis pour les grandes entreprises, qui disposent généralement de plusieurs équipes, parfois dans plusieurs pays, chacune d'entre elles ayant une responsabilité sur une partie du Système d'Information. Une équipe d'analyse peut avoir besoin de différentes autorisations d'accès pour analyser les mesures d'utilisation des applications Cloud afin de repérer les indicateurs d'utilisation anormale. L'équipe de conformité quant à elle aura besoin de permissions d'accès distinctes pour créer des groupes de services et définir des politiques de gouvernance pour l'ensemble de la structure. La séparation des rôles permet de rationaliser les opérations de sécurité de l'entreprise. De plus, les contrôles RBAC permettent à ces équipes de fonctionner selon le principe du 'moindre privilège', afin que chacune d'elle dispose d'une exposition limitée à l'information contenue au sein de la plateforme CASB.

Next-Gen RBAC ou la juridiction de données

Comme les plates-formes CASB sont utilisées pour répondre à des exigences de sécurité complexes, les clients exigent davantage de contrôle dans la façon de régir leur utilisation pour/par

l'interne. Bien que le RBAC soit essentiel à la mise en œuvre d'un système structuré et d'un flux de travail au niveau des rôles, les principaux CASB du marché proposent davantage de granularité à ce niveau, ce qui permet aux clients de mettre en œuvre des restrictions sur les ensembles de données auxquels les utilisateurs peuvent accéder. Par exemple, un utilisateur peut être limité à l'analyse des données utilisées pour la filiale de l'Amérique du Nord, et un autre uniquement pour celles de la zone EMEA. Il s'agit donc ici d'un principe de juridiction sur l'accès aux informations, dans la continuité des principes de conformité souvent imposes aux entreprises dans les textes de régulation.

Le RBAC au niveau des données, ou juridiction des données, est de plus en plus mis en œuvre par les entreprises, en particulier dans les secteurs hautement réglementés (secteur public, finance et énergie), à mesure qu'elles étendent leur gestion de la conformité.

D'après le Gartner, 40 % des déploiements d'Office 365 s'appuieront sur des outils tiers pour combler les lacunes en matière de sécurité et de conformité cette année, ce qui représente une augmentation majeure par rapport à 2015 où le taux était inférieur à 10 %. Alors que les administrateurs de sécurité introduisent de nouvelles solutions pour sécuriser les services Cloud utilisés par les employés, ils doivent également mettre en place des contrôles pour réduire le risque d'exfiltration de données applicatives de sécurité. En appliquant les contrôles RBAC au niveau des données dans leurs déploiements CASB, ils peuvent ainsi limiter l'exposition aux données sensibles et réduire le risque d'exfiltration par des tiers malveillants.

A mesure que de nouvelles vulnérabilités apparaissent chaque jour, les exigences liées à la sécurité et à la conformité des environnements Cloud se multiplient et se complexifient.

Pour y répondre, les équipes dédiées à la sécurité IT doivent mettre en œuvre des stratégies et applications en mesure de répondre à la fois aux enjeux de sécurité et de conformité, ainsi qu'à leurs évolutions. Dans ce contexte évolutif, les offres CASBs sont promis à un bel avenir.