Symantec

CASB : 6 atouts pour sécuriser les applications cloud en entreprise

D'ici à 2022, 65 %[1] des outils de productivité des entreprises devraient être transférés dans le cloud, c'est-à-dire en dehors de votre périmètre de sécurité traditionnel.

Une solution CASB (Cloud Access Security Broker) telle que Symantec CloudSOC vous permet de maîtriser le chaos du cloud sur l'ensemble des applications et données. Voici comment.

Avec un CASB, l'entreprise profite du cloud en toute sécurité

1 Identifiez les applications cloud que vos collaborateurs utilisent et évaluez le risque

La plupart des DSI estiment entre 30 et 40 le nombre d'applications cloud utilisées dans leur entreprise[2]. En réalité, elles sont plus de 1 232[3], entre les applications validées par le département informatique et celles, non approuvées, qui peuvent présenter un risque de sécurité élevé (le « Shadow IT »).

Pour déterminer si les applications découvertes sont sûres pour l'entreprise, il faut vérifier qu'elles respectent ses exigences, notamment ses politiques de sécurité et de conformité.

Avec un CASB, vous pouvez recenser et évaluer les applications que vos collaborateurs utilisent. Nombre d'entreprises aujourd'hui évaluent les usages cloud au cas par cas, en passant au crible les données issues des outils réseau et de sécurité comme les proxys, les pare-feu et les journaux DNS. Un CASB peut consolider automatiquement ces données et apporter une visibilité bien plus profonde, avec une analyse détaillée portant sur des milliers d'applications cloud.

2 Appliquez des politiques de gestion des applications cloud sur les proxys web ou pare-feu existants

À partir des informations fournies par le CASB, vous pouvez faire le tri entre les applications cloud à approuver, celles qui peuvent être autorisées sous surveillance et celles qu'il faut bloquer totalement.

Ensuite, vous pouvez affiner vos politiques de proxy web et de pare-feu pour bloquer les applications à risque qu'il n'y a pas lieu d'utiliser dans l'environnement de l'entreprise. L'intégration du CASB avec votre proxy web rationalise ce processus.

3 Encadrez l'utilisation des informations sensibles, notamment les contenus concernés par la conformité

L'aspect crucial des applications cloud réside dans les données d'entreprise qui y transitent. Par conséquent, veiller à la sécurité de ces données est le rôle le plus important du CASB. Outre l'encadrement des applications cloud utilisées, vous devez surveiller et contrôler la manière dont les données sont exploitées, même au sein des applications validées.

Pour identifier et classifier les contenus sensibles transférés et stockés dans les applications cloud, les CASB de pointe recourent à des techniques avancées, comme le traitement des langues naturelles et l'analyse contextuelle.

Les solutions CASB évoluées identifient de manière dynamique et précise les catégories importantes de documents et de données, qu'il s'agisse de fichiers de conformité, commerciaux ou juridiques, ou d'informations d'identification, de santé ou de cartes bancaires, même dissimulés derrière un lien partagé. Ce degré de visibilité vous permet de créer et d'appliquer des politiques de sécurité tout en laissant les utilisateurs profiter de la liberté du cloud.

4 Chiffrez ou « tokenisez » le contenu sensible pour veiller à la confidentialité et à la sécurité des données

Les pouvoirs publics et les autorités de régulation sectorielles sont de plus en plus attentifs aux conditions de transfert et de stockage des données sensibles, ou exigent des entreprises qu'elles renforcent la protection de ces informations. Face à ces exigences, le caractère ouvert et l'ambiguïté géographique du cloud obligent les entreprises à reconsidérer son utilisation pour partager des informations.

Avec le chiffrement et la « tokenisation », elles peuvent continuer à recourir au cloud en instaurant une couche de protection supplémentaire. Au lieu d'empêcher purement et simplement le transfert de ces données dans le cloud, ces technologies remplacent les données sensibles par des valeurs tokenisées ou chiffrées avant qu'elles ne quittent l'environnement de votre entreprise.

Veillez à choisir une solution qui n'a pas d'impact sur la fonctionnalité de l'application cloud elle-même. Avec une solution CASB appropriée, vos équipes pourront utiliser des plates-formes cloud courantes, comme Salesforce et Oracle, en toute sécurité, de manière productive et dans le respect des politiques de confidentialité et de conformité.

[1, 2] Symantec Internet Security Threat Report, avril 2017

[3] Rapport Symantec Shadow Data du 1er semestre 2017

D’après le dernier rapport [avril 2017], une entreprise en moyenne utilise 1232 applications cloud, contre 928 précédemment, soit une hausse de 33 %.

Rapport Symantec Shadow Data du 1er semestre 2017

5 Détectez et bloquez les comportements inhabituels qui indiquent une activité malveillante

Les services cloud offrent de nouvelles cibles aux cyber criminels qui, s’ils mettent la main sur des informations d’authentification, peuvent accéder aux données de l’utilisateur sans être détectés par la plupart des contrôles de sécurité. En effet, ces derniers ne recherchent aucune activité suspecte de la part d’un utilisateur légitime lorsqu’il se connecte ni lors des opérations qu’il effectue après connexion.

Les malwares et menaces persistantes avancées peuvent se propager par le biais d’applications cloud, et le transfert de fichiers vers le cloud via des liens chiffrés rend ces attaques invisibles pour les moteurs d’analyse traditionnels. S’ils ne sont pas détectés et traités rapidement, de tels malwares peuvent envahir toute l’entreprise.

Une bonne solution CASB doit aussi fonctionner en continu. Elle doit offrir une visibilité approfondie sur l’activité des utilisateurs, développer des points de comparaison et rechercher les anomalies par une analyse des comportements qui apporte de réelles capacités de détection des menaces et de réponse à incident pour le cloud.

6 Intégrez la visibilité et la maîtrise du cloud dans vos solutions de sécurité existantes

Pour porter ses fruits, la sécurité cloud doit réunir plusieurs technologies pour offrir un niveau adéquat de visibilité, de contrôle, de protection des données et de prévention des menaces. Une solution CASB avancée telle que Symantec CloudSOC est le point de départ idéal pour gagner en visibilité et mieux appréhender l’usage des applications cloud dans votre entreprise.

En intégrant CloudSOC avec Symantec ProxySG et Symantec DLP et avec l’appui du Global Intelligence Network, vous pouvez obtenir la protection complète dont vous avez besoin. Ces solutions Symantec vous apportent la maîtrise, la protection des données et la protection contre les menaces indispensables pour bénéficier d’une sécurité à 360 degrés à l’heure de la génération cloud. L’ensemble de l’entreprise peut alors profiter des côtés pratiques du cloud sans les risques.

Prêt à couper court au chaos du cloud ?

Pour commencer, demandez votre évaluation du risque Shadow IT »

Symantec™