SÉCURISER LE CLOUD, par le cloud

Christophe Estebanez, Manager Avant-Vente pour l'Europe du Sud (SE Manager Iberia and France) au sein de Netskope, répond à nos questions sur la sécurité et le cloud. Il revient notamment sur les enjeux relatifs à ce sujet et le positionnement de son entreprise et son offre dans ce cadre. Entretien.

Christophe Estebanez

L'accélération du développement du cloud soulève des problématiques de sécurité. Quels sont les principaux enjeux pour les entreprises ?

Depuis quelques années, nous assistons à une explosion du trafic à destination des applications executées dans le cloud. Il s'agit essentiellement d'applications hébergées en mode SaaS, c'est-à-dire hors de l'infrastructure et de la responsabilité de l'entreprise, chez des fournisseurs de services comme Google ou Amazon. Pour une entreprise de taille moyenne (de 500 à 2 000 personnes), on recense environ 805 applications dans le cloud utilisées au quotidien. On compte parmi elles des applications dites managées, dont l'utilisation est régie par une relation contractuelle entre l'entreprise et le fournisseur, mais aussi des applications dites non managées utilisées par les collaborateurs.

Ces applications non-managées sortent du périmètre de contrôle de l'entreprise. En parallèle, nous notons une hausse des menaces sur ces vecteurs applicatifs dans le cloud. Ce risque est renforcé par un changement de paradigme : les utilisateurs ne travaillent plus forcément depuis leur bureau, mais sont de plus en plus en situation de nomadisme. En plus d'utiliser des applications qui ne sont pas forcément contrôlées par leur entreprise, ils peuvent également se connecter à partir de terminaux qui ne sont pas non plus contrôlés par l'entreprise et cela n'importe où dans le monde (maison, lieu de vacances, en voyage…).

Pour s'adapter à ce nouvel environnement, quels sont les prérequis pour les entreprises ?

Plus que jamais, les entreprises doivent mettre en place des mécanismes, des moteurs de contrôle et des politiques de sécurité plus adaptés. On entend ainsi de plus en plus parler de l'approche « any device, any where, any user » qui vise à sécuriser avec pertinence et efficacité les applications dans le cloud. Il y a aussi le concept Zero Trust qui consiste à ne plus se reporter à la notion de périmètre physique en matière de sécurité. Les firewalls, les routeur et les infrastructures physiques qui permettaient de maîtriser et contrôler le trafic applicatif sont devenus obsolètes, car ce trafic passe dorénavant directement entre l'utilisateur et le cloud.

Les nouveaux critères de sécurité sont aujourd'hui très différents : qui est l'utilisateur, quel est le niveau de conformité de son poste, est-ce qu'il dispose des droits pour utiliser une application donnée, est-ce que cette application est utilisée de manière conforme, peut-il télécharger un fichier et le partager…?

La gestion des accès et des autorisations devient, en effet, extrêmement importante. Et au-delà d'avoir une bonne visibilité sur le trafic des applicatifs, les entreprises doivent aussi pouvoir avoir le contrôle sur le comportement de l'utilisateur.

Qu'en est-il de la donnée ? Comment garantir sa sécurisation dans l'environnement cloud, notamment SaaS ?

La donnée représente le patrimoine digital de l'entreprise et souvent leur matière première. Il faut donc être en mesure de la lire, de la détecter et de la comprendre. Au-delà des mécanismes classiques de déchiffrement et d'interception, l'entreprise doit aussi déployer des mécanismes de détection et de prévention de pertes et de fuites de la donnée (solutions DLP).

Des modèles de données personnalisés ou appliqués par défaut sont aussi nécessaires pour détecter des données sensibles (numéro de carte bancaire, numéro de sécurité sociale, numéro de téléphone, adresse…) dans des documents word, excel ou autre. Dans le cadre du contrôle de la mobilité de cette typologie donnée, l'idée est de pouvoir garantir qu'elles ne sont pas téléchargées puis ré-uploadées sur des instances personnelles par exemple.

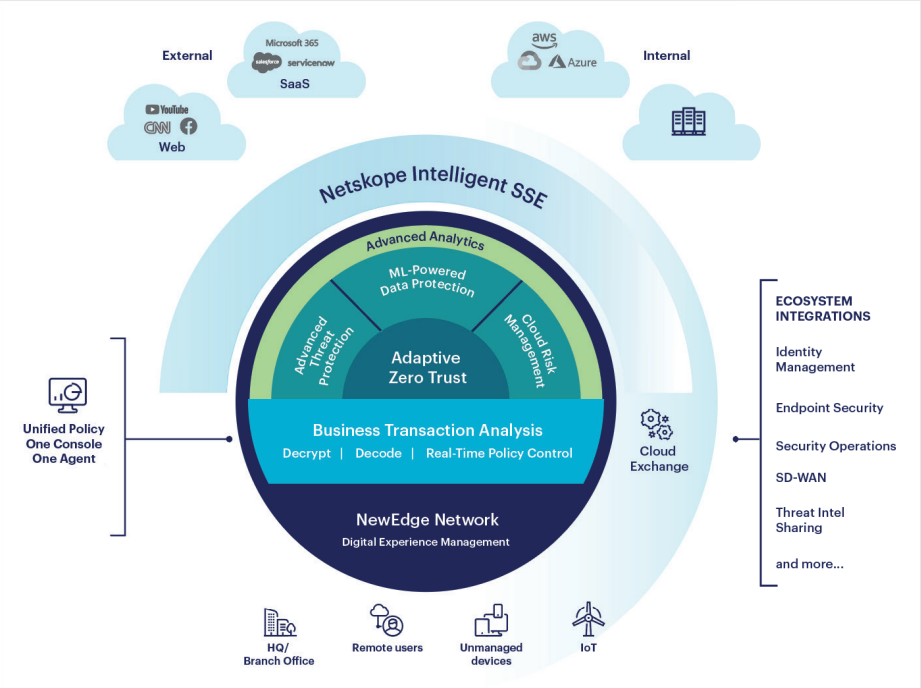
Il faut également s'assurer de la conformité de la configuration des applications SaaS, c'est-à-dire que les accès et les possibilités d'utilisation aient été correctement confi-

gurés par les équipes informatiques. On parle alors de SSPM (SaaS Security Posture Management) et de CSPM (Cloud Security Posture Management) si on se réfère aux infrastructures IaaS.

Dans cette continuité, quels sont les critères et les services qu'une solution SSE performante doit proposer ?

Le SSE (Security Service Edge) est un sous-ensemble du SASE (Secure Access Service Edge) qui permet aux utilisateurs de se connecter de manière sécurisée depuis n'importe où dans le monde de manière efficace et assez rapidement avec des liens réseaux, des mécanismes d'optimisation, de priorité de trafic... Le SSE représente un ensemble de services de sécurité hébergés dans le cloud et qu'il est très difficile de contrôler avec une interface client unifiée. La seule option est de sécuriser le cloud par le cloud. Et c'est exactement ce que Netskope propose au travers de services qui sont embarqués dans son SSE :

- Le filtrage d'URL ;
- Le déchiffrement SSL pour déchiffrer le trafic afin de l'inspecter ;
- La SandBox pour exécuter des fichiers afin de s'assurer qu'ils ne sont pas dangereux ;
- Le Cloud Access Security Broker / CASB pour intercepter le trafic vers les applications SaaS afin de s'assurer qu'elles sont correctement utilisées ;
- Le User and Entity Behavior Analytics pour faire de l'analyse de comportement ;
- Le Data Loss Prevention / DLP pour détecter les types de données avec un certain formalisme ;
- L'Intrusion Prevention System / IPS pour détecter les menaces comme les malwares, les virus... ;
- Les API qui vont permettre de se connecter à Google, à Azure... mais aussi à des applications SaaS afin de s'assurer que les paramètres de sécurité sont correctement configurés, mais aussi contrôler les données et fichiers déjà stockées dans le cloud ;
- Le Remote Browser Isolation / RBI qui permet de naviguer sur une page web et d'avoir un rendu vidéo de la navigation. La page n'étant pas exécutée sur le poste, c'est le cloud qui prend tous les risques.



Que proposez-vous à ce niveau ?

Entreprise dite cloud native, Netskope a cette capacité à déployer l'ensemble de ces services de sécurité sans avoir d'impact sur la performance. Nous avons ainsi développé un réseau mondial, NewEdge, qui s'appuie sur une cinquantaine de points de connexion locaux. Ce réseau, qui est au cœur de notre valeur ajoutée, est en continuelle expansion avec de nouveaux déploiements régulièrement.

En outre, NewEdge est connecté à tous les grands fournisseurs de services SaaS dans le monde. Cela permet d'avoir une latence extrêmement faible entre l'utilisateur et l'application finale malgré la filtration du trafic, mais aussi une expérience client optimale. En effet, la sécurité ne doit pas impacter la performance et l'agilité de l'entreprise au niveau du déploiement et de l'utilisation de nouvelles applications, de la maîtrise des coûts et des risques.

Quelles pistes de réflexion pourriez-vous partager avec nos lecteurs ?

Les dirigeants doivent aborder ce sujet en se concentrant sur trois dimensions complémentaires :

- Une bonne visibilité de la valeur digitale de leur entreprise et de son exploitation afin notamment d'optimiser la prise de décision ;
- L'implémentation de mécanismes de sécurité qui ne freinent pas l'agilité, la performance de l'entreprise et au service de l'expérience utilisateur. L'idée est aussi de pouvoir mesurer le ratio entre le risque pris et l'investissement réalisé ;
- La conformité avec l'ensemble des règlements en vigueur (RGPD, hébergement des données de santé...).

EN BREF

Netskope a été fondé en 2012 en Californie. Actuellement plus de 30 % des entreprises du Fortune 100 font confiance à Netskope qui a développé le plus gros cloud privé au monde permettant d'assurer des performances supérieures au marché. Extrêmement innovant, avec un focus sur la protection des données, Netskope est leader dans le Magic Quadrant dédié au Security Service Edge (SSE), défini par Gartner.