Malgré les récentes violations, le cloud ne faiblit pas

Plusieurs récentes violations à grande échelle dans les environnements de cloud computing, touchant plus de 100 millions de clients au total, ont ébranlé cette confiance et ravivé le malaise relatif à la confidentialité et à la sécurité des données.

Les gros titres et les réseaux sociaux ne cessent de remettre cette question sur le devant de la scène : certains d'entre nous sont-ils allés trop loin et trop vite vers le cloud ?

Gestion et surveillance des sessions dans le cloud

Le cloud est-il plus sécurisé que le « on-prem » (sur site) ? Ça dépend. Et cette question nécessite bien plus que cette tribune pour être adressée correctement. Si les outils de sécurité cloud natifs évoluent et s'améliorent, de même que l'écosystème croissant des fournisseurs proposant des outils cloud, de nombreuses lacunes subsistent. Et un élément reste manquant ou incomplet dans de nombreux environnements de cloud computing : la gestion et surveillance des sessions.

La surveillance de session est une capacité essentielle pour les environnements cloud afin d'assurer la sécurité, l'auditabilité et la responsabilité. C'est la seule méthode pour observer, documenter, enregistrer et détecter les comportements inappropriés lorsque l'accès est toujours initié à distance. Alors que d'autres techniques peuvent surveiller d'autres protocoles ou un accès au cloud basé sur des API, seule la surveillance de sessions peut capturer le comportement en temps réel des utilisateurs et de leurs activités. Et, si les utilisateurs savent qu'ils sont enregistrés (ou surveillés), la dissuasion seule peut suffire à enrayer certains comportements malveillants.

Le contrôle et la gestion des sessions constituent une capacité essentielle de cybersécurité pour les environnements cloud qui, de manière native, ne sont pas fournies ou ne sont fournies que sous une forme de base largement insuffisante qui est de loin dépassée par les solutions modernes fournies par des fournisseurs tiers. Les meilleures solutions tierces peuvent permettre aux organisations de surveiller et de gérer les sessions avec l'exigence que le cloud requiert, c'est-à-dire des centaines, voire des milliers, de sessions simultanées.

Avec la surveillance de session dans le cloud, tout le texte à l'écran et toutes les frappes au clavier sont enregistrés (à l'exclusion des mots de passe) et inspectés en temps réel pour rechercher des correspondances de modèle critiques. Les flux de travail automatisés peuvent permettre à la solution de localiser une session anormale et d'y mettre fin, ou de la suspendre / la verrouiller jusqu'à ce qu'une décision soit prise pour déterminer si cette activité est appropriée ou non.

Certaines solutions fournissent également une liste prédéfinie, clé en main, pour les commandes de base de données, les mouvements latéraux, les commandes sensibles du système d'exploitation et tout autre comportement suspect.

En plus de renforcer la sécurité, le contrôle et la gestion des sessions sont importantes pour tout environnement cloud, car les réglementations et exigences de conformité nécessitent qu'un nombre croissant de sessions, telles que les sessions privilégiées sur des systèmes sensibles, soient pleinement auditables (journalisation, surveillance d'activité, etc.). La surveillance de session fournit la documentation nécessaire pour examiner, analyser et déterminer si la session était autorisée, si elle contenait un comportement malveillant et si elle était correctement conduite.

Voici une liste non exhaustive de quelques façons dont les solutions modernes peuvent aider à sécuriser un environnement cloud :

- Gérer les accès privilégiés et appliquer le principe du moindre privilège. Cela permet aussi d'optimiser l'utilisation des listes de contrôle d'accès natives pour sécuriser les sessions d'accès distant et éviter qu'elles ne soient initiées par des utilisateurs inappropriés.
- Surveiller et gérer les sessions dans le cloud et les activités privilégiées.
- Effectuer une surveillance de l'intégrité des fichiers pour s'assurer que les fichiers ne sont pas altérés, et pour identifier et alerter les activités non fiables.
- Gérer les comptes IAM dans le cloud pour assurer que la rotation des accès et des identifiants est effectuée conformément aux politiques de sécurité.
- Gérer l'accès aux ressources de l'entreprise exploitant des consoles de gestion Web, notamment pour Amazon Web Services, Azure, Google Cloud, VMware vSphere, Citrix XenServer, Microsoft Hyper-V, Microsoft Azure, IBM Softlayer et Rackspace.
- Scanner et analyser les environnements cloud tels qu'Amazon®, GoGrid®, IBM®, Rackspace®, VMware® etc. pour découvrir des actifs (y compris IoT) et identifier, hiérarchiser et corriger les erreurs de configuration et autres vulnérabilités.

La mauvaise presse récente autour des incidents de sécurité liés au cloud incitera de nombreuses entreprises à faire une pause et à revoir (intelligemment) leurs stratégies et technologies de sécurité dans le cloud. Toutefois, les entreprises qui couvrent correctement leurs déploiements dans le cloud, qui identifient et corrigent les vulnérabilités à l'aide d'outils de qualité, continueront à tirer parti des nombreux avantages du cloud.