Akamai

LIVRE BLANC

Protéger les charges de travail dans AWS avec une segmentation complète - Sécurité plus simple et plus rapide

Ne laissez pas les problèmes de sécurité devenir un frein à l'adoption du cloud. Une solution unique peut gérer la visibilité, la prévention des mouvements latéraux, ainsi que la détection et le traitement des violations dans AWS.

Plus de 60 % des entreprises dans le monde citent la sécurité comme obstacle majeur à l'adoption du cloud. Transférer des charges de travail critiques vers AWS présente des avantages évidents : allègement des coûts d'infrastructure et des tâches de maintenance, évolutivité et souplesse optimisées avec une puissance et des ressources presque illimitées, et utilisation des toutes dernières innovations (apprentissage automatique et IA, par exemple) pour optimiser les performances et les analyses. Cependant, les problèmes de sécurité freinent de nombreuses entreprises.

Garantir la sécurité dans AWS

Lorsque vous envisagez un tout nouvel environnement, il n'est pas surprenant d'avoir à revoir intégralement votre sécurité. Que vous soyez nouveau dans le cloud, changiez de fournisseur, choisissiez une nouvelle solution hybride ou ajoutiez AWS à votre écosystème existant, le cloud requiert son propre ensemble d'outils spécifiques pour relever les défis uniques que présente cette infrastructure. Certains facteurs sont communs à tous les fournisseurs de cloud, tandis que d'autres seront propres à Azure, Google Cloud Platform (GCP) ou AWS. Voici quelques-unes des principales préoccupations des entreprises utilisant le cloud ou un cloud hybride incluant la technologie AWS :

Compréhension de la responsabilité partagée : lorsque vous transférez vos charges de travail vers AWS, vous devez admettre que vous avez encore beaucoup de responsabilités. Vous devrez sécuriser les plateformes, les applications et les données des clients. Le manque de compréhension du modèle de responsabilité partagée explique la prévision de Gartner selon laquelle 99 % des défaillances de sécurité dans le cloud seront imputables au client jusqu'en 2025.

Manque de visibilité : vous ne pouvez pas contrôler ce que vous ne voyez pas. Dans le cloud, la visibilité est beaucoup plus compliquée, surtout lorsqu'il s'agit de protéger et de visualiser le trafic réseau est-ouest et nord-sud. Il ne suffit pas d'étudier uniquement les flux. Vos ressources critiques peuvent être réparties sur plusieurs groupes de sécurité réseau, conteneurs ou comptes AWS. Sans mise en contexte, il peut s'avérer impossible d'avoir une idée précise des flux et des interdépendances.

Contrôle limité pour la création des règles : si votre entreprise bénéficie habituellement d'une visibilité au niveau de la couche 7 sur site, vous ne voudriez pas revenir à la couche 4 et perdre le contrôle et la visibilité granulaires maintenant que vos charges de travail sont dans le cloud. Les groupes de sécurité Amazon prennent en charge le contrôle du trafic jusqu'à la couche 4. Quelle que soit l'infrastructure sous-jacente, la visibilité et le contrôle au niveau de la couche 7 vous permettent de ne pas vous reposer uniquement sur les ports et adresses IP, qui sont très insuffisants pour détecter et traiter les violations.

Sécurité des conteneurs : AWS utilise des groupes de sécurité Amazon pour appliquer la règle de sécurité des conteneurs, mais cela est limité aux clusters plutôt qu'aux pods individuels. Pour avoir un aperçu complet des communications, vous avez besoin d'une solution qui reconnaisse le contexte d'un réseau superposé qui s'exécute au-dessus d'un autre réseau et qui puisse effectuer une analyse détaillée jusqu'au niveau du pod. Cela se complexifie lorsque vous souhaitez créer des règles de réseau qui incluent des machines virtuelles et des conteneurs, ce qui conduit souvent les entreprises à gérer deux ensembles de contrôles de sécurité.

Lutter contre ces problèmes avec une plateforme de sécurité tout-en-un

Amazon fournit des outils intégrés, tels que des groupes de sécurité Amazon, qui permettent de relever certains défis liés à la migration de votre infrastructure vers le cloud. Nous encourageons les entreprises à tirer le meilleur parti d'AWS IAM (gestion des identités et des accès), en utilisant des groupes pour attribuer des autorisations, en renouvelant régulièrement les informations d'identification et en utilisant des groupes IAM à des fins de simplicité. Cependant, ces outils seuls ne sont qu'un point de départ dans le cloud public dynamique d'aujourd'hui, en particulier lorsque vous envisagez un environnement hybride qui couvre tout, de l'infrastructure existante au multicloud, en passant par la technologie des conteneurs. Une solution de sécurité sophistiquée vous permettra de compléter l'offre d'AWS avec une technologie qui supprime les angles morts et fonctionne en toute transparence avec le reste de votre système de sécurité, même dans un environnement hybride. Voici les avantages offerts par Akamai Guardicore Segmentation :

Visibilité totale des instances AWS

Plus votre infrastructure informatique se complexifie, plus il est important d'en avoir une visibilité approfondie et automatisée. Peu fiables et sources de failles et d'erreurs, les suppressions, modifications, ajouts et déplacements manuels constituent également un facteur de ralentissement et, par conséquent, un obstacle à l'adoption du cloud. En revanche, une visibilité améliorée et automatisée permet d'identifier l'ensemble des applications et des flux, ajoutant ainsi une visibilité à vos instances jusqu'au niveau de chaque processus.

La solution Akamai Guardicore Segmentation inclut une puissante API AWS qui extrait les données d'orchestration, vous donnant ainsi un contexte précieux que vous pouvez utiliser pour l'étiquetage et le mappage des applications. Les balises EC2 sont extraites automatiquement pour visualiser les instances EC2. Lorsque vous analysez votre

infrastructure, vous disposez des informations dont vous avez besoin pour bien comprendre comment vos applications communiquent entre elles, où se trouvent les interdépendances et comment créer des règles pour assurer fluidité et agilité. Au lieu d'avoir une solution de sécurité distincte pour chaque environnement ou fournisseur de cloud, les utilisateurs peuvent visualiser des informations cloud natives et des données spécifiques à AWS sur le même tableau de bord. Notre solution est compatible avec l'ensemble des plateformes, infrastructures et clouds, vous garantissant ainsi l'absence d'angles morts.

Segmentation et application : une règle qui suit la charge de travail

Une fois que vous disposez d'un « environnement de surveillance unique » pour tous vos environnements, vous pouvez commencer à concevoir et déployer une règle de sécurité. Une règle orientée applications va plus loin que ce que les groupes de sécurité Amazon seuls peuvent accomplir, fournissant une granularité de couche 7 au lieu d'une granularité de couche 4. Alors que certaines entreprises tentent d'utiliser des pare-feu nouvelle génération sur site pour limiter les mouvements latéraux, cette solution ne prend en charge qu'une segmentation approximative du trafic est-ouest. Il est extrêmement difficile de trouver une solution qui assure des contrôles de segmentation granulaires, et ce en raison des modifications importantes à apporter à l'infrastructure et au réseau pour réacheminer le trafic via le pare-feu. Même si cette solution était possible sur site, les entreprises doivent veiller à conserver le même niveau de contrôle sur le cloud. La microsegmentation au niveau de la couche 7 est la solution idéale, car elle ne nécessite pas de modifier l'infrastructure réseau sous-jacente et propose une règle conçue pour les charges de travail dynamiques. Étant donné que la règle suit la charge de travail, votre entreprise n'aura plus à apporter de modifications manuelles, bénéficiera d'une meilleure agilité et pourra adopter de plus en plus de processus DevOps en constante évolution. Simplifiant un environnement hybride, une seule stratégie de microsegmentation peut appliquer des règles dans l'ensemble des régions, des VPC, des conteneurs, des machines virtuelles et des sites, le tout de manière cohérente. En bénéficiant de la visibilité que nous offrons, vous pouvez définir et appliquer des règles de segmentation en quelques minutes seulement. Votre processus de création de règles est également amélioré par des recommandations de règles automatiques qui fournissent des protocoles de sécurité de pointe sur le cloud public.

Détection des violations et réponse aux incidents sur le cloud d'AWS

Une solution complète comme Akamai Guardicore Segmentation vous permet d'aller encore plus loin en matière de sécurité AWS que la segmentation ou la visibilité seules. La détection des violations de règle est une partie importante de la détection des violations. Elle vous permet de réagir à une cybermenace potentielle en temps réel, avec des détails au niveau des applications. Nous proposons plusieurs méthodes de détection des violations qui peuvent immédiatement vous alerter en cas d'intention malveillante dans un environnement de cloud hybride :

- **Analyse de la réputation :** permet de détecter automatiquement les informations suspectes dans les flux : noms de domaine, adresses IP, hachages de fichiers et lignes de commande.
- **Leurres dynamiques :** permet de mobiliser les attaquants à leur insu, en les détournant vers un environnement de type pot de miel à forte interaction où vous pouvez apprendre beaucoup de leur comportement et ce, en toute sécurité.
- **Outils pour accélérer la réponse aux incidents :** l'intégration à AWS permet d'envoyer en temps réel toute violation de règle ou tout incident de sécurité à l'AWS Security Hub.
- **Recherche de menaces personnalisée :** tirez parti de l'infrastructure d'Akamai Guardicore Segmentation et de la masse d'informations mondiales sur les menaces d'Akamai pour contrecarrer les menaces les plus évasives dans votre environnement de cloud hybride grâce au service Akamai Hunt.

Tout regrouper pour bénéficier d'une sécurité renforcée sur AWS et au-delà

Migrer vers le cloud ne signifie pas nécessairement que votre entreprise doit se contenter de niveaux de sécurité, de visibilité ou de contrôle inférieurs à ceux dont elle bénéficie sur site. Avec Akamai Guardicore Segmentation, vous bénéficiez d'une visibilité complète de vos instances AWS et de l'ensemble de votre infrastructure. Cette carte fondamentale assure la création de règles en toute transparence et améliore les groupes de sécurité AWS pour garantir un contrôle granulaire sans assistance manuelle. Complétée par des fonctionnalités de détection des violations et de réponse aux incidents, vous disposez d'une plateforme de bout en bout qui couvre toutes vos bases sur le cloud d'AWS.

Pour plus d'informations, consultez le site akamai.com/guardicore.