PRÉSENTATION DE LA SOLUTION AKAMAI

Protéger les charges de travail dans AWS avec Akamai Guardicore Segmentation

Les entreprises continuent de mettre à profit les ressources PaaS dans Amazon Web Services (AWS), et beaucoup migrent leurs charges de travail critiques vers le cloud public. Ces entreprises constatent des avantages, tels que la réduction des coûts, ainsi qu'une évolutivité, des performances et une agilité supérieures. Cependant, cette ruée vers le cloud soulève des préoccupations urgentes du point de vue de la sécurité, dont les suivantes :

Nouvel ensemble d'outils

Le fonctionnement dans un environnement cloud nécessite un tout nouvel éventail de contrôles de sécurité. Ces contrôles doivent prendre en charge AWS dans le cloud et par le biais d'outposts AWS sur site, ainsi que les charges de travail sur cloud hybride. Si les groupes de sécurité cloud existants peuvent suffire pour les actifs et les ressources dans le cloud AWS, ces contrôles ne permettent pas de protéger les ressources ou les actifs associés dans d'autres environnements. Pour cette raison, votre équipe doit gérer plusieurs outils de sécurité, ce qui peut entraîner des failles de sécurité potentielles.

Nouveau modèle d'opérations de sécurité

Au titre du Modèle de responsabilité partagée d'AWS, l'utilisation de ressources AWS dans le cloud ou sur site implique qu'Amazon est uniquement en charge de la protection de l'infrastructure qui exécute tous les services proposés dans le cloud AWS. Cependant, tous les logiciels applicatifs ou utilitaires installés sur ces instances, ainsi que la configuration des groupes de sécurité, relèvent de la seule responsabilité de l'utilisateur. Cela inclut également la protection et la surveillance du trafic, nord-sud et est-ouest, et le déploiement de contrôles permettant de prévenir les violations, de les détecter et d'y répondre.

Visibilité et contrôle réduits sur l'infrastructure

Les avantages qui rendent l'environnement AWS attractif sur le plan opérationnel peuvent également réduire le contrôle et la visibilité sur les actifs répartis entre plusieurs comptes AWS, clouds privés virtuels (VPC) et groupes de sécurité réseau, ainsi que sur l'écosystème hybride au sens large d'une organisation.

Principaux avantages

- Solution offrant une protection de bout en bout des charges de travail dans AWS, y compris les ressources PaaS, permettant aux équipes DevOps et de sécurité de concentrer leurs ressources limitées sur des tâches stratégiques plutôt que sur la gestion de la sécurité du centre de données
- Gérez et appliquez des règles de microsegmentation strictes qui s'étendent au-delà d'AWS pour inclure les actifs disséminés sur site et même dans des clouds publics
- Détectez de manière fiable les violations de règles et répondez-y en temps réel
- Prémunissez vos environnements contre les failles potentielles en utilisant plusieurs méthodes de détection et de prévention des intrusions, y compris l'analyse de réputation et les techniques de leurres dynamiques en temps réel

Akamai Guardicore Segmentation au service de la sécurité d'AWS

Akamai Guardicore Segmentation fournit une solution unifiée de visibilité et d'application des règles pour les charges de travail et les ressources PaaS s'exécutant dans votre cloud AWS, vos outposts et vos environnements hybrides. Cette solution offre une microsegmentation et une visibilité au niveau des applications, ainsi que des capacités de détection des failles de sécurité et de réponse à celles-ci.

Découverte et visibilité automatiques

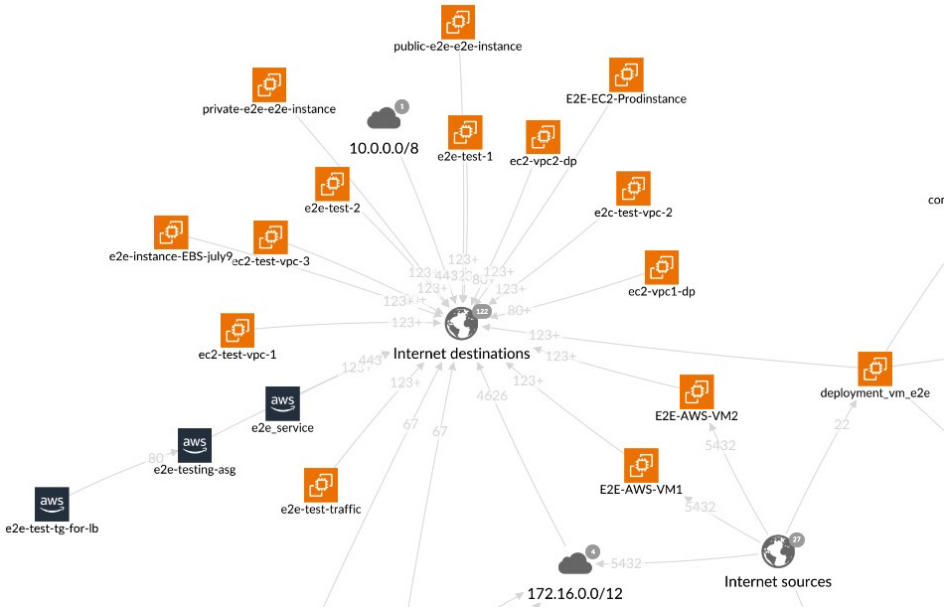
- Visualisation automatique des applications, des ressources et de leurs flux de communication
- Compréhension rapide et détermination d'un niveau de référence pour le comportement des applications
- Cartographie des dépendances des applications avec une visibilité granulaire jusqu'au niveau du processus (couche 7)

Segmentation et mise en œuvre performantes

- Définition de règles de segmentation en seulement quelques minutes
- Recommandations de règles automatiques
- Étiquetage et regroupement intelligents, facilitant la navigation dans des environnements complexes

Détection des menaces et réponse aux incidents

- Aucune configuration requise ; génération de valeur dès le premier jour
- Plusieurs méthodes de détection couvrant tous les types de menaces
- Techniques de leurres dynamiques fournissant une couverture réseau complète



Visualisez et protégez les applications et les ressources dans AWS avec Akamai Guardicore Segmentation

> En choisissant Akamai Guardicore Segmentation, nous avons pu combler les failles de sécurité critiques en matière de microsegmentation et de visibilité au niveau des applications, mais aussi de détection et réponse concernant les violations, couvrant à la fois les serveurs AWS et sur site.
>
> **— Chef d'équipe DevOps**
> **Entreprise de biotechnologie**

Protégez en toute fluidité les charges de travail et les ressources PaaS dans AWS. Pour en savoir plus, rendez-vous sur akamai.com/guardicore.