PRÉSENTATION DE LA SOLUTION AKAMAI

Segmentation pour les environnements de cloud hybride

Contenez les attaques à l'aide de la segmentation pour votre infrastructure cloud

Avec la transition croissante des applications et des charges de travail vers le cloud, les équipes cloud et de sécurité font face à des défis de plus en plus nombreux. L'un d'entre eux consiste à étendre la segmentation et les principes Zero Trust aux applications et charges de travail dans les environnements cloud. Grâce à Akamai Guardicore Segmentation, les entreprises peuvent réduire leur surface d'attaque et contenir les attaques visant les applications et les charges de travail dans leurs environnements de cloud public, sans installer d'agents. Cela est rendu possible par la découverte automatique des applications, la visualisation complète des flux cloud, des règles de segmentation précises et des alertes de sécurité réseau, le tout à partir d'un seul écran.

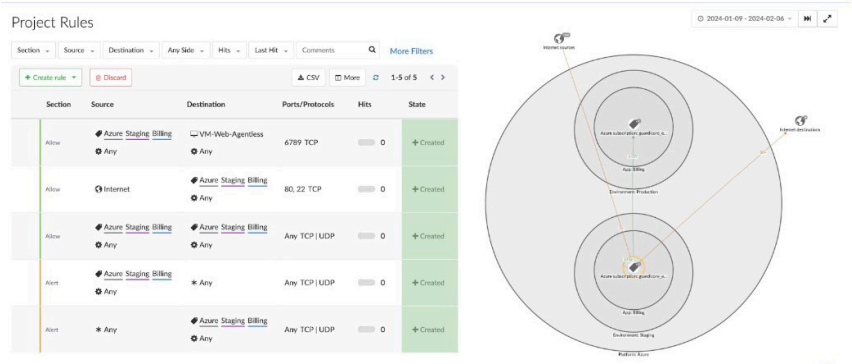
Les défis uniques du cloud

De nos jours, les entreprises ont de plus en plus recours au cloud pour gérer leurs systèmes critiques et stocker leurs données les plus précieuses.

Selon le rapport IBM sur le coût d'une violation de données 2023, 82 % des violations concernaient des données stockées dans le cloud (public, privé ou les deux). Les attaquants ont souvent réussi à accéder à plusieurs plateformes cloud, avec 39 % des violations couvrant plusieurs environnements et engendrant un coût supérieur à la moyenne de 4,75 millions de dollars.

Du fait de la nature unique et dynamique du cloud, les charges de travail du cloud sont plus exposées aux menaces externes que les ressources sur site. Les équipes de sécurité sont donc confrontées à plusieurs défis uniques :

- **Mauvaise visibilité** : la visibilité du fournisseur de cloud repose sur des journaux bruts des flux entre différentes charges de travail. Sans une compréhension claire des relations entre les différentes charges de travail et applications au sein des environnements cloud, la création de règles de sécurité efficaces devient presque impossible.
- **Absence de stratégie unique** : la création de règles cohérentes dans les environnements de cloud hybride à l'aide d'outils de sécurité cloud natifs est extrêmement complexe. En effet, chaque instance de cloud possède ses propres objets et règles, et donc ses propres stratégies, ce qui entraîne une fragmentation des règles.
- **Manque d'unification de la gouvernance** : la sécurité n'est pas toujours une priorité dans le cloud. Cela crée des frictions entre les équipes de sécurité et les propriétaires d'applications, qui font tourner les charges de travail sans toujours prendre en considération la sécurité.



Cloisonnez une application Azure à l'aide de suggestions de règles automatisées

Avantages pour votre entreprise

Visualisez les flux cloud à l'aide d'une interface unique
Approfondissez votre compréhension de la façon dont vos charges de travail et applications cloud interagissent à l'aide d'une carte de dépendance réseau dynamique, et appliquez facilement des contrôles de sécurité.

Appliquez des règles de segmentation cohérentes
Déployez une solution de segmentation unique qui fonctionne de manière cohérente dans les environnements de cloud hybride, en évitant les solutions spécifiques aux fournisseurs qui créent des silos de sécurité.

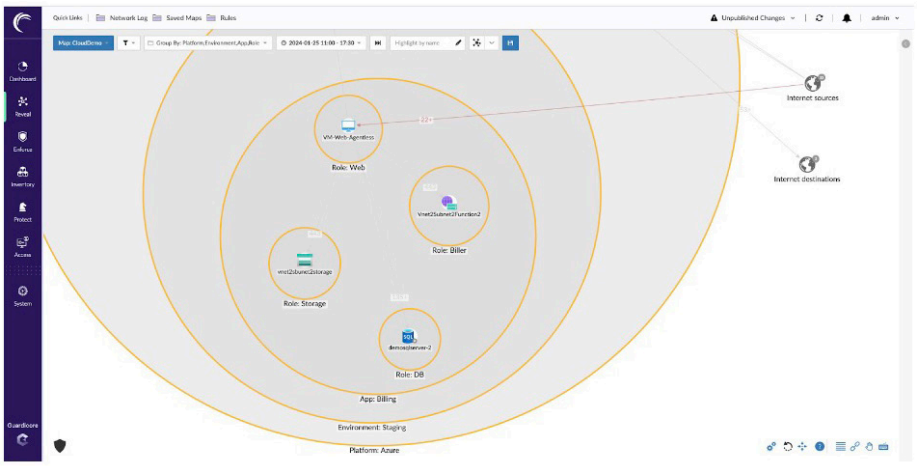
Stoppez les violations
Adaptez les règles de sécurité à tout changement au sein de votre environnement cloud et épargnez à votre équipe le fardeau des mises à jour manuelles.

Prévenez les menaces de sécurité dans le cloud

Akamai Guardicore Segmentation étend sa segmentation de pointe aux applications et charges de travail dans le cloud. En étendant la segmentation à vos actifs cloud, toute connexion non autorisée est automatiquement interrompue, limitant ainsi les mouvements latéraux et les dégâts causés par les violations ou les incidents de ransomware.

Principales fonctionnalités

- **La visibilité et l'application complètes et natives du cloud sans agent** permettent aux administrateurs de visualiser les charges de travail cloud à l'aide d'une carte interactive en temps quasi réel des flux réseau réels, de comprendre les dépendances des applications et de rassembler les équipes DevOps et SecOps dans la gouvernance de la sécurité du réseau cloud.
- **Un moteur d'application hybride exploitant plusieurs points d'application** permet à une entreprise de définir simplement l'intention d'une règle réseau et de laisser le moteur de règles d'Akamai Guardicore Segmentation s'occuper du reste, en décidant dynamiquement quels points d'application basés sur des agents et sans agent sont utilisés dans le centre de données.
- **Les fonctionnalités intégrées d'analyse de réputation et de renseignement sur les menaces du pare-feu** sont conçues pour réduire le temps de détection et le temps de réponse aux incidents en cas de violation.
- **Une solution évolutive et sécurisée** garantit que les données ne quittent pas votre environnement cloud et que l'architecture de la solution évolue automatiquement au sein de celui-ci.



Une carte unique pour les environnements de cloud hybride et sur site

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

 | Assistance | | Publication : 02/24