PRÉSENTATION DE LA SOLUTION AKAMAI

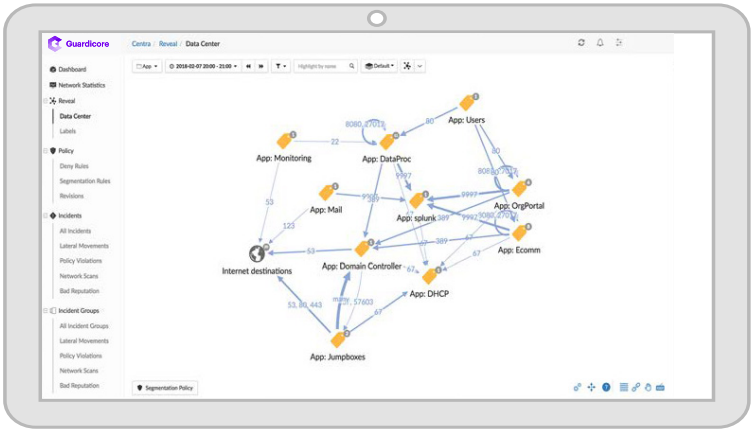
Microsegmentation rapide dans les environnements hybrides avec Akamai Guardicore Segmentation

Le processus de mise en œuvre de la microsegmentation n'est pas linéaire. La route pour identifier, comprendre et contrôler les flux des applications dans votre environnement informatique est semée d'embûches. Mais sans la bonne approche pour vous frayer un chemin, vous pouvez rencontrer un certain nombre de difficultés en cours de route. Les angles morts du réseau rendent souvent impossible l'identification et le mappage des communications des applications, des charges de travail et des processus sous-jacents. Des moteurs de règles rigides peuvent forcer des décisions radicales, qui risquent de nuire aux applications. Une application incohérente des règles entre les systèmes d'exploitation peut entraîner des failles de sécurité dangereuses. Enfin, des intégrations complexes, et souvent manuelles, des données de violations de règle avec les outils de détection des violations peuvent ralentir les investigations relatives aux incidents et la réponse à ces derniers. Akamai Guardicore Segmentation vous aide à réaliser la microsegmentation en trois étapes.

Étape 1 : Révéler

Identification automatique des applications et visualisation des flux

Grâce au contexte qu'elle fournit au niveau des processus, la solution Akamai Guardicore Segmentation offre une visibilité exceptionnelle qui permet d'identifier et de visualiser automatiquement l'ensemble des applications, des charges de travail et des flux de communication, quel que soit leur emplacement. Vous disposez de la même visibilité pour les ressources qui sont sur site, dans le cloud, sur plusieurs clouds, et autres. Cette visualisation, associée à l'importation automatique des métadonnées d'orchestration, permet à vos équipes de sécurité d'étiqueter et de regrouper rapidement et facilement toutes les ressources et applications, rationalisant ainsi le développement des règles.



Applications critiques sécurisées quel que soit leur emplacement

Solution indépendante de la plateforme
Akamai Guardicore Segmentation peut visualiser des ressources et appliquer des règles de sécurité sur l'ensemble des infrastructures : sur site, dans le cloud et sur plusieurs clouds.

Mise en œuvre rapide des règles
Grâce à des suggestions de règles automatisées, à un moteur de règle flexible et à une interface utilisateur intuitive, la création et l'application des règles prennent moins de temps.

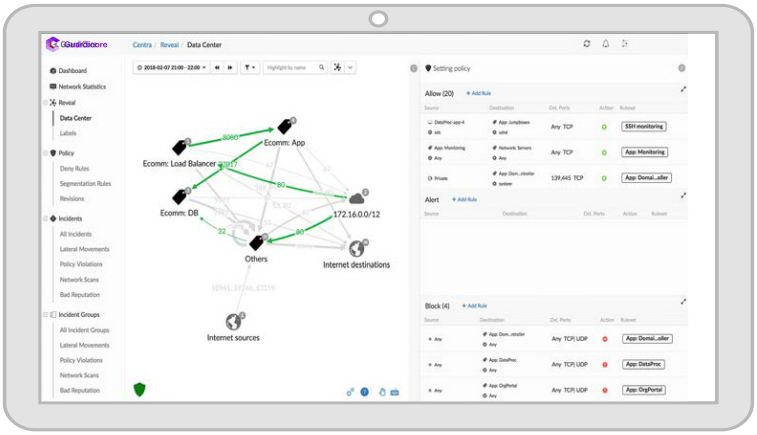
Fonctionnalités intégrées de détection et de traitement des violations
Visualisez les violations de règle et répondez rapidement aux menaces actives pour protéger vos ressources les plus critiques, quel que soit leur emplacement.

Akamai

Étape 2 : Créer

Conception, test et déploiement rapides des règles

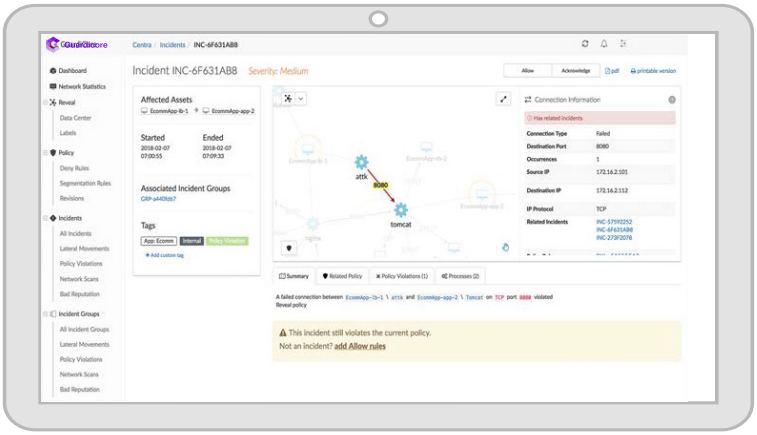
Akamai Guardicore Segmentation simplifie le développement et la gestion des règles de microsegmentation. Il suffit de cliquer sur un flux de communication sur la carte de l'étape 1 pour générer des suggestions de règles automatisées basées sur des observations historiques. Vous pouvez ainsi créer rapidement une règle solide. Un flux de travail intuitif et un moteur de règle flexible permettent d'affiner les règles en continu et de réduire les erreurs coûteuses.



Étape 3 : Appliquer

Niveau de sécurité élevé assuré dans n'importe quel environnement

Grâce à sa capacité à appliquer les règles de communication au niveau du réseau et des processus sur l'ensemble des systèmes, Akamai Guardicore Segmentation assure la sécurité, quelles que soient les limitations imposées par le système d'exploitation. En outre, les capacités intégrées de détection et de traitement des violations vous permettent de voir les violations de règle dans le contexte d'une violation active, et donc d'identifier rapidement la méthode d'attaque et d'y remédier.



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

 | Assistance | | Publication : 06/23