GUIDE DE COMPARAISON

Akamai Guardicore Segmentation face aux solutions de microsegmentation traditionnelles

Visibilité inégalée

Pour comprendre ce qui se passe dans votre environnement, il est essentiel d'avoir une visibilité sur les communications entre les charges de travail. Une visibilité réellement efficace signifie être capable, à tout moment, de connaître la charge de travail dans chaque environnement. En outre, les fonctionnalités de regroupement et de filtrage des actifs et des règles sont des composants essentiels pour élaborer rapidement et efficacement des règles.

Akamai	Microsegmentation traditionnelle
Visualisez votre environnement global en toute simplicité L'agent Akamai Guardicore Segmentation est un pare-feu basé sur l'hôte qui fonctionne sur les systèmes d'exploitation récents et anciens, offrant une visibilité totale des flux réseau au niveau du processus et du service sous Windows et Linux, ainsi qu'une couverture des points de terminaison MacOS.	**Visibilité partielle des anciens systèmes** Pas de visibilité sur les systèmes Microsoft Windows antérieurs à Windows 2002. Cela est dû au fait que l'agent des solutions de microsegmentation traditionnelles repose sur un pare-feu Windows qui n'était disponible qu'avec les systèmes postérieurs à 2002. Pour les systèmes Linux, leurs agents prennent uniquement en charge la visibilité L4.
Contexte riche et sans égal En ce qui concerne la visibilité, il est essentiel d'avoir un contexte et des détails appropriés. Notre solution collecte, en plus des données de flux, du contexte critique tel que les informations sur les processus, les fichiers, le niveau de correctifs et plus encore.	**Contexte minimal** Seules les informations relatives aux flux et aux machines sont collectées, laissant de côté des détails contextuels critiques tels que le processus et le fichier. Cela rend le processus de compréhension des dépendances des applications plus laborieux et plus chronophage.
Aucune limitation sur le type ou le nombre d'étiquettes Nous n'imposons aucune restriction sur le nombre ou le type d'étiquettes dont vous pouvez disposer, ce qui permet de traiter des cas d'utilisation supplémentaires. Cette approche vous évitera d'avoir à traduire vos étiquettes existantes à partir de bases de données de gestion de configuration (CMBD) et d'autres sources de données.	**Étiquetage rigide** Avec une hiérarchie d'étiquetage fixe et prédéfinie, les solutions traditionnelles vous obligent à étiqueter vos applications en utilisant une quantité déterminée uniquement par elles, sans tenir compte des exigences de votre propre environnement et des besoins de votre entreprise.
Étiquetage déterminé par l'IA L'IA détecte et étiquette les applications pour vous aider à les identifier lorsqu'il n'y a pas de CMDB fiable, et leur attribue automatiquement la bonne étiquette.	**Pas de CMDB ? Vous êtes bloqué...** Avec un étiquetage manuel et une hiérarchie d'étiquetage préconfigurée, lorsqu'une organisation ne dispose pas de CMDB fiable, le processus d'étiquetage devient extrêmement compliqué.

Akamai

Couverture de pointe

L'un des éléments essentiels d'une bonne solution de microsegmentation est la capacité à protéger les actifs critiques, quel que soit l'endroit où ils sont déployés ou consultés : systèmes anciens ou récents, Windows ou Linux, sur site ou virtuels, conteneurs, et bien plus encore.

Akamai

Prise en charge complète de Windows et Linux

Les agents Akamai Guardicore Segmentation sont pris en charge sur tous les systèmes d'exploitation Windows et Linux, nouveaux et anciens, car notre solution ne dépend pas de l'infrastructure sous-jacente.

Prise en charge complète des conteneurs

Visibilité complète pour les environnements conteneurisés tout en exploitant les contrôles Container Network Interface (CNI) pour la mise en œuvre.

Microsegmentation traditionnelle

Prise en charge limitée de Windows et Linux

L'application des règles dépend du pare-feu Windows pour les environnements Windows et du pare-feu iptables pour les environnements Linux. Cela se traduit inévitablement par une protection limitée ou nulle pour certains systèmes d'exploitation Windows hérités, et pas de règles au niveau des processus L7 pour les environnements Linux.

Prise en charge limitée des conteneurs

La mise en application a recours à iptables et à des calculs de règles aller-retour qui ne sont pas évolutifs dans un environnement de conteneurs, ce qui entraîne une latence et des temps d'arrêt.

Créez des règles simples. Rapidement.

Un bon moteur de règles permet d'exprimer votre intention à l'aide d'un nombre de règles minimum, sans imposer de restrictions du langage des règles. Il contribuera également à minimiser le travail de gestion des règles en tirant parti de l'automatisation et des assistants.

Akamai

Autoriser et refuser

Nous prenons en charge les règles de type liste blanche et liste noire, ainsi que toutes les combinaisons intermédiaires. Cela permet aux équipes de sécurité et de RI de réagir rapidement à tout scénario de sécurité, en éliminant la nécessité de mettre d'abord chaque flux légitime sur une liste blanche.

Modèles de règles pour divers cas d'utilisation

Modèles prêts à l'emploi et flux de travail d'élaboration de règles pour les scénarios courants : atténuation des ransomwares, cloisonnement des applications, segmentation de l'environnement, etc. Les modèles permettent de gagner du temps et de réduire les erreurs humaines.

Critères de règles riches

Les critères de règles peuvent inclure la source, la destination, le port, le protocole, le processus, le service (par exemple, le planificateur de tâches couramment utilisé par les ransomwares), l'utilisateur et le nom de domaine qualifié complet (FQDN).

Microsegmentation traditionnelle

Liste blanche avec prise en charge limitée des règles de refus

L'adhésion au modèle de liste d'autorisation qui est sûr mais qui prend du temps, ne permet pas aux solutions de segmentation traditionnelles de répondre automatiquement aux menaces connues qui doivent être bloquées rapidement.

Un ensemble limité de modèles

Les modèles de segmentation sont principalement pris en charge dans les environnements Microsoft. Les modèles pour les cas d'utilisation de segmentation courants tels que le cloisonnement, ainsi que l'atténuation des ransomwares et leurs mesures correctives, ne sont pas pris en charge.

Critères limités

Pas de règles au niveau des processus L7 pour les systèmes d'exploitation Linux, ni de possibilité d'élaborer des règles basées sur les services Microsoft Windows.

La sécurité avant tout

La lutte contre les menaces de sécurité complexes telles que les ransomwares nécessite une approche globale de la sécurité. Bien que la segmentation soit préconisée comme réponse fondamentale par le National Institute of Standards and Technology (Institut national des normes et des technologies, NIST) et la Maison Blanche, une approche intégrée de la sécurité et de la détection des violations est nécessaire pour assurer la sécurité de votre organisation.

Akamai	Microsegmentation traditionnelle
Prévention et atténuation des ransomwares Akamai Guardicore Segmentation fournit des modèles prêts à l'emploi pour toutes les phases de la chaîne d'élimination des attaques, de la prévention à l'atténuation en passant par le confinement.	**Aucun modèle de ransomwares** Les solutions traditionnelles sont limitées dans leur capacité à bloquer les attaques de ransomwares avec des modèles prêts à l'emploi.
Interrogation des points de terminaison pour la détection des menaces et la mise en conformité Notre outil Insight, basé sur osquery, vous permet d'interroger les serveurs et les points de terminaison en temps réel pour la conformité et la détection des logiciels malveillants.	**Pas de détection en temps réel** Les solutions traditionnelles ne peuvent pas détecter les activités malveillantes dans le centre de données.
Capacités de leurre Basé sur une technologie brevetée, l'agent Akamai Guardicore Segmentation redirige les sessions bloquées et échouées vers un moteur de leurre dynamique pour les analyser plus en profondeur et les mettre en quarantaine.	**Aucune mise en quarantaine** Les solutions traditionnelles manquent de capacités de leurre ainsi que de détection ou de mise en quarantaine des machines présentant des signes connus de compromission.
Équipe gérée de recherche des menaces Akamai propose des services gérés de recherche des menaces qui étendent les capacités de votre équipe de sécurité et permettent à votre organisation de garder une longueur d'avance sur les menaces.	**Aucun service de recherche des menaces** Les fournisseurs traditionnels ne peuvent pas fournir de services de recherche de menaces basés sur leur solution, ce qui peut être un facteur de différenciation critique face à la puissance des ransomwares et des logiciels malveillants.
Pare-feu de renseignement sur les menaces Pour prévenir les comportements malveillants connus, Akamai Guardicore Segmentation bloque les IP, les fichiers et les hachages malveillants à l'aide de règles de pare-feu automatiques.	**Aucun flux de menace** En l'absence d'une capacité similaire, les solutions traditionnelles ne peuvent pas empêcher l'accès à des adresses IP et URL réputées malveillantes.

Opérations ou performances et latence

Une faible latence est essentielle à la réussite d'un projet de segmentation. Cela signifie que vous devez être en mesure de faire évoluer votre politique en ajoutant des règles, des étiquettes par actif et d'autres objets de règle, sans introduire de latence supplémentaire.

Akamai

Moteur à latence optimisée

Notre moteur de segmentation est conçu pour les scénarios à grande échelle. Pour ce faire, un mécanisme de filtrage optimisé permet d'obtenir un temps de latence relativement peu sensible à la taille de la règle.

Microsegmentation traditionnelle

Davantage de règles entraînent une latence accrue

Les agents introduisent davantage de latence à mesure que la quantité et la taille des règles augmentent. Linux iptables n'a tout simplement pas été conçu pour mettre à l'échelle pour le trafic est-ouest des entreprises. Il en résulte une latence importante qui augmente directement avec la taille de la règle.

Pour en savoir plus sur Akamai Guardicore Segmentation ou pour demander une démonstration personnalisée du produit, consultez notre site à l'adresse akamai.com/guardicore.