Akamai

Déconstruire les 7 mythes sur la microsegmentation

Cela peut sembler paradoxal de voir petit lorsqu'on prévoit grand, mais il existe beaucoup d'idées reçues concernant les solutions de microsegmentation actuelles.

Vous pensez que vous serez confronté à des interruptions de réseau ou à des difficultés pour mettre en œuvre un déploiement défini par logiciel ? Détrompez-vous. Voici ce qui est important en matière de granularité.

Mythe 1

Ma solution EDR suffit pour arrêter les attaques par ransomware

La détection et réponse aux points de terminaison (EDR) et la segmentation permettent toutes deux de lutter contre les attaques par ransomware, mais à différents stades de la chaîne d'attaque – et de différentes manières. Les solutions EDR visent à détecter la présence de ransomwares en cours d'exécution sur les terminaux ou sur les points de terminaison qu'elles surveillent. Lorsque l'EDR détecte un ransomware, elle peut arrêter le processus, mettre le terminal en quarantaine et parfois annuler un éventuel chiffrement. L'EDR et la segmentation sont complémentaires : si l'EDR ne détecte pas de ransomware, les solutions de segmentation divisent le réseau en compartiments cloisonnés afin de limiter le mouvement latéral (est-ouest) d'une attaque. Avec les ransomwares, un mouvement latéral doit se produire pour que l'attaque réussisse. La segmentation s'assure que les attaques ayant réussi à dépasser le point de terminaison se heurteront finalement à un obstacle, ce qui limite le rayon d'action d'une infection initiale. En savoir plus sur les différences entre EDR et segmentation.

1 heure et 42 minutes,

c'est le temps moyen que met un cybercriminel pour commencer à se déplacer latéralement dans le réseau une fois qu'il a pénétré dans une entreprise

(Rapport Microsoft Digital Defense 2022)

Mythe 2

Je pratique déjà la segmentation

La segmentation n'est pas un concept nouveau, elle est simplement de plus en plus sophistiquée. Depuis des décennies, les entreprises utilisent un patchwork de VLAN, de pare-feu internes, de listes de contrôle d'accès et de groupes de sécurité pour segmenter leurs environnements. Mais ces méthodes héritées n'ont pas évolué pour répondre aux exigences complexes des infrastructures hybrides et multicloud actuelles, ce qui a créé des failles défensives et des zones d'ombre causées par la sous-segmentation.

Par exemple : les pare-feu hérités ne procèdent pas à la cartographie et à l'évaluation des dépendances des flux de travail, ce qui rend difficile d'identifier les segmentations pour les applications, les charges de travail ou les utilisateurs. Les entreprises sont donc contraintes de mettre en œuvre des stratégies de segmentation étendues qui sont trop permissives et qui peuvent facilement – *et rapidement* – entraîner des erreurs de configuration dangereuses, difficiles et fastidieuses à dépanner.

Grâce à la microsegmentation, les entreprises peuvent segmenter et appliquer des règles jusqu'à la couche 7, bien plus que ce que permettent les outils de segmentation traditionnels.

2 millions de dollars

de frais de mise à niveau des pare-feu économisés en trois ans

(Forrester TEI)

Mythe 3

La microsegmentation est trop difficile à mettre en œuvre

La microsegmentation nouvelle génération est prête à être déployée dans les entreprises, aujourd'hui plus que jamais.

Akamai Guardicore Segmentation permet d'obtenir une efficacité opérationnelle maximale en utilisant une solution logicielle unique pour la segmentation, la visibilité, la création et l'exécution de règles dans tous les environnements, du data center au cloud en passant par les ressources basées sur des conteneurs. Lors du déploiement, Akamai Guardicore Segmentation crée une carte visuelle dynamique de l'ensemble de l'infrastructure informatique, qui permet aux équipes de sécurité de visualiser l'activité au niveau des processus individuels, en temps réel ou sur une base historique.

Ces informations détaillées sur le comportement des applications peuvent ensuite être utilisées pour créer rapidement des stratégies de microsegmentation granulaire via une interface visuelle intuitive. Les règles de refus au niveau mondial, le cloisonnement des applications critiques et la possibilité de segmenter immédiatement de grands environnements permettent de réduire les délais de rentabilisation – et les risques.

Avec les méthodes de segmentation existantes, vous n'avez pas la visibilité nécessaire pour savoir par où commencer.

Augmentation de

↑95 %

de la productivité SecOps

(Forrester TEI)

Mythe 4

La microsegmentation entraîne l'interruption des applications et du réseau

Avec les approches traditionnelles de segmentation, les applications sont souvent déplacées entre des sous-réseaux ou des VLAN, ce qui entraîne des temps d'arrêt et perturbe la continuité des activités. En conséquence, les ingénieurs réseau et les administrateurs de pare-feu doivent planifier des temps d'arrêt, un contrôle des modifications ou des fenêtres de maintenance, ce qui augmente le délai de déploiement des nouveaux services ou des mises à jour d'applications. Pire encore, ces retards peuvent entraîner un risque accru d'exposition et de vulnérabilité des ressources.

En revanche, la segmentation logicielle dissocie la sécurité de l'infrastructure et des systèmes d'exploitation sous-jacents, de sorte que la segmentation peut être effectuée indépendamment, sans toucher au réseau ou à l'application. En cas d'événement, au lieu d'isoler complètement les machines affectées, seul le vecteur d'attaque est bloqué afin de limiter les impacts négatifs sur l'entreprise.

La microsegmentation peut également être déployée en mode alerte pour permettre de tester les stratégies dans des environnements de production connectés, sans risque d'interruption. Résultat : les solutions de segmentation dernière génération n'obligent plus à choisir entre sécurité et flexibilité.

Mythe 5

La microsegmentation ne couvre pas mon environnement IoT ou OT

Saviez-vous que les stratégies Zero Trust pouvaient être appliquées sur les terminaux IoT et OT qui ne peuvent pas exécuter de logiciel de sécurité basé sur l'hôte ?

Nos capacités de segmentation sans agent permettent de combler les écarts de sécurité entre les terminaux qui ne peuvent pas exécuter d'agents pour éliminer les zones d'ombre, comme les points de terminaison soumis à un air gap. Cette couverture étendue revêt une importance majeure pour les environnements de santé, de commerce de détail et de fabrication qui ont de nombreux systèmes OT et terminaux IoT connectés au réseau (et donc vulnérables). L'intégration d'une segmentation sans agent à votre infrastructure réseau permet la détection automatique de nouveaux terminaux, l'utilisation de l'empreinte digitale et l'application de stratégies de réduction des risques tout en accélérant la migration vers le Zero Trust à l'échelle de l'entreprise.

Mythe 6

Un agent de microsegmentation augmente trop la latence

L'une des idées fausses les plus courantes concernant la microsegmentation est l'augmentation de la latence.

En réalité, utiliser des politiques de segmentation logicielles distribuées au lieu de forcer tout le trafic à passer par des points de contrôle propres au pare-feu élimine les goulots d'étranglement du réseau. De par sa conception, l'agent Guardicore d'Akamai est hautement optimisé pour fonctionner avec Linux, Unix, Windows OS et MacOS, et ne consomme pas de ressources importantes.

Et comme l'agent n'est pas en ligne, il ne réalise pas d'inspection en profondeur des paquets qui risque d'augmenter la latence.

L'agent Guardicore d'Akamai utilise un minimum d'informations de l'en-tête de paquets pour créer une vue riche de l'environnement du client. Vous souhaitez combiner vitesse *et* performances ? C'est *possible*.

Mythe 7

La microsegmentation suppose de recruter des ETP impossibles à trouver

Alors que les responsables de la sécurité des systèmes d'information sont sous pression pour « faire plus avec moins », les solutions de sécurité doivent alléger la charge de travail des défenseurs – et non consommer des ressources internes rares.

Les méthodes de segmentation traditionnelles, telles que la gestion des pare-feu et des VLAN, impliquent des processus en plusieurs étapes laborieux qui sollicitent l'intervention de nombreuses équipes chargées de manière individuelle de la commutation, du routage, de la mise en œuvre des pare-feu et de la création de stratégies de sécurité. La mise en œuvre de pare-feu hérités s'étend en moyenne sur 14 à 22 semaines, qui s'ajoutent aux délais du projet et soumettent l'entreprise à des coûts de main-d'œuvre et à des frais d'exploitation importants.

En revanche, le déploiement de la solution logicielle d'Akamai prend en moyenne deux semaines et nécessite l'intervention d'un seul employé à temps plein. En outre, l'ajout d'Akamai Hunt, notre service géré de détection des menaces, vous fait gagner du temps et des ressources en recherchant les attaques émergentes, les mouvements latéraux et les comportements d'attaque anormaux dans votre environnement.

De nos jours, il est difficile de recruter des cybertalents et encore plus de les retenir. Il est temps que les défenses travaillent au service de votre entreprise, *et non contre elle*.

Statistiques clés

106 %

Retour sur investissement éprouvé jusqu'à 106 % en 12 mois

(Forrester TEI)

Comment Akamai peut vous aider

Guardicore Segmentation d'Akamai est une solution logicielle de microsegmentation conçue pour vous aider à appliquer les principes Zero Trust de la manière la plus simple, la plus rapide et la plus intuitive qu'il soit. Grâce à des règles de segmentation bien précises, à la visualisation de l'activité dans votre environnement informatique et des alertes de sécurité réseau, elle vous permet d'empêcher tout mouvement latéral malveillant dans votre réseau. La solution Guardicore Segmentation d'Akamai est parfaitement adaptée à vos centres de données, à vos environnements multicloud et à vos points de terminaison. Plus rapide à déployer que la segmentation d'infrastructure, elle vous offre une visibilité et un contrôle accrus sur votre réseau.

Découvrez comment Akamai Guardicore Segmentation assure une protection granulaire, une visibilité approfondie et une application cohérente des stratégies de sécurité à grande échelle pour protéger vos données les plus sensibles.