Akamai

LIVRE BLANC

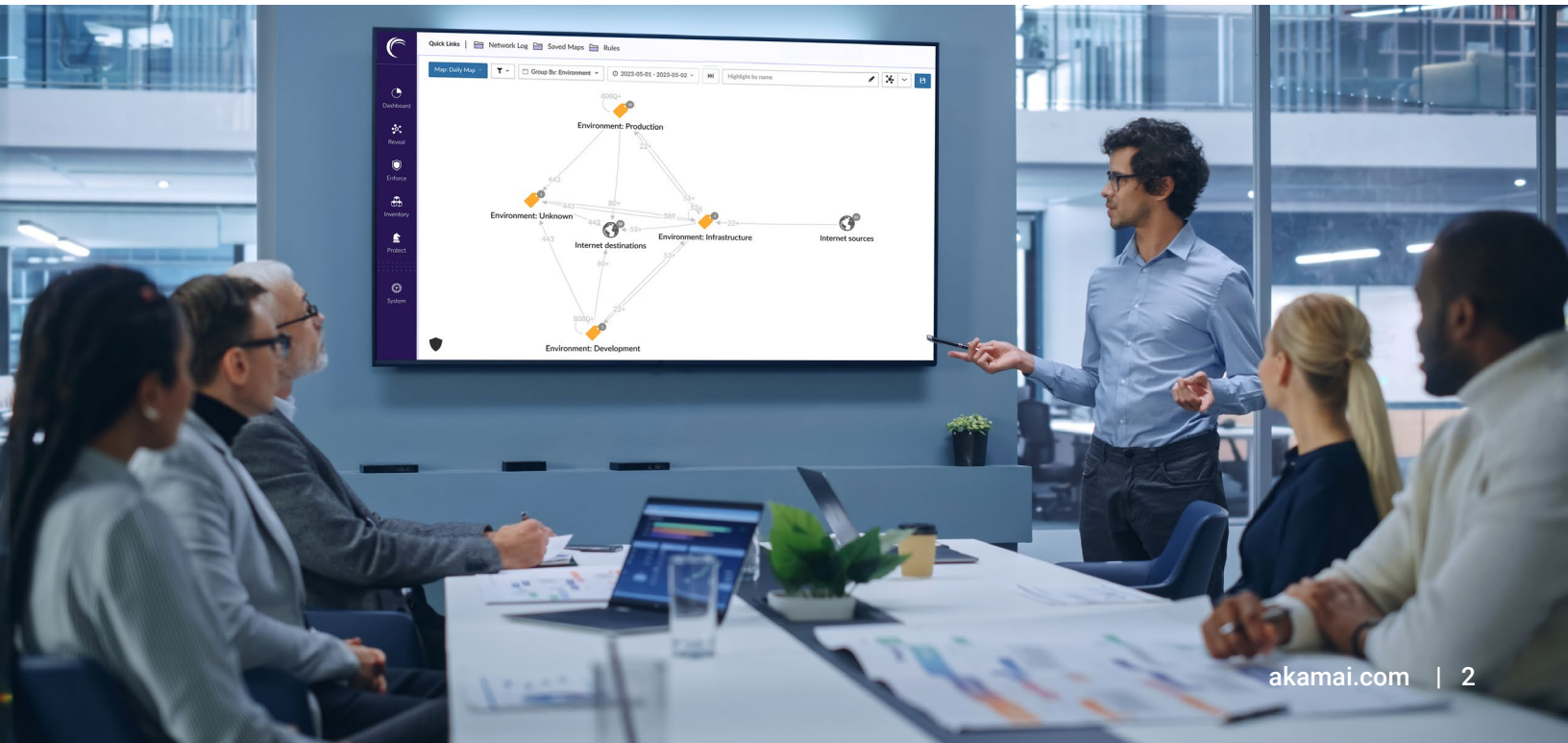
Segmentation logicielle pour les opérateurs de centre de données

Pour les opérateurs de centres de données multi-locataires, la segmentation des environnements informatiques n'est pas seulement importante, il s'agit également d'une composante fondamentale de leur modèle d'exploitation. Tout d'abord, ils doivent séparer leur propre infrastructure de l'environnement de leurs clients et partager certaines ressources tout en empêchant l'accès à d'autres. Ensuite, ils doivent prévenir la « contamination croisée » dans les environnements respectifs de leurs clients, qu'elle soit accidentelle ou malveillante. Cette démarche consiste notamment à empêcher que des violations réussies ou des infections par des logiciels malveillants ne se propagent de l'environnement d'un client vers d'autres. Enfin, ils doivent assurer un niveau de séparation adéquate pour limiter l'impact d'une violation potentielle au sein des applications opérationnelles détenues. En examinant plus en profondeur les réseaux opérationnels des fournisseurs de centres de données, il existe trois scénarios dans lesquels la segmentation, si elle est réalisée efficacement, peut améliorer considérablement la sécurité des systèmes et réduire les coûts.

1. **Séparer les réseaux opérationnels** (DCIM, BMS, …) du réseau d'entreprise (les systèmes internes du fournisseur, qui incluent la facturation) et des réseaux clients

2. **Réduire le risque de mouvement latéral à l'intérieur du réseau opérationnel**, qui comporte de nombreux systèmes difficiles à corriger et introduit des risques s'il n'est pas correctement segmenté

3. **Créer une connectivité efficace et sécurisée entre les réseaux en contact avec les clients**, comme la DMZ, où se trouve le portail personnalisé, qui nécessite un accès sécurisé aux données des réseaux opérationnels (lecture de l'état de l'alimentation, par exemple) et des réseaux d'entreprise (lecture des informations de facturation)



Ces éléments sont gérés aujourd'hui par des réseaux provisoires, des VLAN et des constructions de réseau très complexes, lents à mettre en œuvre et inefficaces. La mise en œuvre d'une solution logicielle indépendante de configurations réseau complexes entraînera des réductions de coûts significatives et introduira également un contrôle plus rigoureux et plus robuste de la connectivité.

Par ailleurs, bon nombre de clients peinent à mettre en place et à maintenir un niveau élevé de segmentation au sein de leurs applications (hébergées ou sur site). Les opérateurs de centres de données peuvent ainsi profiter d'une excellente occasion de tirer parti de leur expertise interne en matière de segmentation, de leurs outils et de leurs modèles opérationnels pour offrir des services gérés à leurs clients et créer un flux de revenus très attractif autour d'une activité de segmentation. En outre, grâce à sa capacité à étendre des règles de sécurité aux locaux des clients en utilisant une méthodologie, des outils et des processus appropriés, l'opérateur sera en mesure d'accéder aux applications non hébergées et d'en avoir une meilleure visibilité. Il pourra ainsi accélérer leur migration sécurisée vers le centre de données hébergé, et contribuer ainsi au développement de son cœur de métier.

Equifax : un scénario catastrophe

Si vous vous demandez quelle est la pire chose qui pourrait survenir avec une segmentation d'environnement faible, inefficace ou inexistante, la violation très médiatisée dont a été victime Equifax en 2017 en constitue un excellent exemple. Cette violation a compromis les renseignements personnels hautement sensibles de 143 millions d'Américains. Selon l'enquête du Government Accountability Office (GAO) des États-Unis, les hackers ont d'abord pénétré dans le portail de résolution des litiges clients du géant du crédit en exploitant une vulnérabilité, connue sous le nom de CVE 2017-5638, dans le framework web Apache Struts. Une fois à l'intérieur, ils ont parcouru librement les systèmes de l'entreprise pendant 76 jours. Le rapport du GAO attribuait cette liberté de mouvement latéral à un manque de segmentation, qui permettait d'accéder facilement aux bases de données, une surface d'attaque pratiquement illimitée.

La question est de savoir comment réaliser ce type de segmentation de la manière la plus efficace et la plus économique possible. Historiquement, les opérateurs s'appuyaient sur des pare-feu traditionnels ou des VLAN pour séparer les environnements au sein d'une architecture multi-locataires ou multi-utilisateurs. Toutefois, la mise en œuvre et le maintien des mesures de ce type constituent généralement une entreprise ardue, extrêmement manuelle, fastidieuse et coûteuse. De plus, ces techniques ne sont en aucune façon hermétiques et peuvent laisser une surface d'attaque substantielle exposée. L'efficacité des solutions conçues pour la défense périmétrique est particulièrement problématique au sein des centres de données, d'autant plus que la plupart de ces environnements comprennent bon nombre de machines virtuelles, d'hyperviseurs, de conteneurs et même de composants cloud, et que les charges de travail accélèrent et ralentissent automatiquement de manière dynamique. Un autre point important à prendre en compte dans le cadre de la segmentation par VLAN, c'est qu'elle nécessite l'arrêt des applications, ce qui, dans le cas de contrôles opérationnels critiques, peut constituer un véritable frein à la mise en œuvre.

Pour toutes ces raisons, les opérateurs d'environnements partagés s'intéressent de plus en plus aux techniques modernes de segmentation logicielle, y compris la microsegmentation. Les progrès dans le domaine des technologies de microsegmentation en ont fait une solution viable pour tous les types d'entreprises et, sans doute, une option de choix pour atteindre un modèle de sécurité Zero Trust. Autre point tout aussi important, avec les bons outils et une planification quelque peu réfléchie, la microsegmentation peut être mise en œuvre plus rapidement et plus facilement que les autres méthodes évoquées, et est également plus facile à gérer et à maintenir. Par ailleurs, des tests récents ont démontré que la microsegmentation peut réduire le délai de déploiement jusqu'à 30 fois par rapport à la mise en œuvre traditionnelle d'un pare-feu. Autre avantage déterminant : grâce à la segmentation logicielle, aucune modification du réseau ou interruption des applications n'est nécessaire. Ces gains de temps et d'efficacité se traduisent par une réduction significative des coûts tout au long du cycle de vie du déploiement.

Les écueils des approches conventionnelles

Pour comprendre les avantages de la segmentation ou microsegmentation logicielle, il est utile, à des fins comparatives, d'examiner certains des inconvénients et des limites des techniques standard utilisées à la fois sur site et dans le cloud. Il peut s'agir d'une combinaison de pare-feu physiques ou virtualisés et de configurations réseau comme les VLAN. En général, ces méthodes nécessitent beaucoup de ressources et de main-d'œuvre. La création de règles de sécurité est un processus fastidieux. Les ajouts et les modifications doivent être effectués manuellement, ce qui nuit à une efficacité opérationnelle constante et augmente le risque de vulnérabilité.

Les pare-feu internes, en particulier, sont coûteux à acquérir et complexes à mettre en place. Ils interfèrent également avec le flux normal du trafic, en modifiant les schémas et en créant des circuits en « chicane » qui finissent par entraver les performances du système. Comme l'industrie est en train de l'apprendre, les pare-feu ne sont pas destinés à être segmentés au sein des centres de données. Certains fournisseurs admettent même facilement que les pare-feu n'ont tout simplement rien à faire là.

L'un des défis les plus pénibles lors de l'introduction de la segmentation dans un environnement de production existant et en cours d'exécution, c'est que les méthodes traditionnelles nécessitent des temps d'arrêt pour chaque application. Et les temps d'arrêt sont coûteux. Ils ne peuvent avoir lieu que dans des fenêtres de temps spécifiques, et sont souvent tout simplement impossibles à mettre en œuvre.

Autre défi à relever : la création d'une segmentation interne nécessite une bonne connaissance des dépendances est-ouest entre les applications. En général, cette vision globale fait défaut. En l'absence d'un moyen simple de mapper les dépendances des applications, il est extrêmement difficile et risqué de séparer un environnement Brownfield.

Pourquoi la segmentation logicielle est-elle plus efficace ?

Efficacité opérationnelle et meilleure sécurité des systèmes : la segmentation logicielle permet de surmonter les inefficacités inhérentes aux techniques traditionnelles et, encore plus important, d'améliorer la sécurité des environnements multi-utilisateurs. Comme son nom l'indique, la segmentation logicielle reprend le concept de segmentation réseau et l'implémente sans qu'il soit nécessaire de modifier l'infrastructure. Elle implique la création de règles de sécurité autour d'applications individuelles ou groupées logiquement, quel que soit l'endroit où elles sont hébergées dans le centre de données hybride. Ces règles déterminent les applications qui peuvent et ne peuvent pas communiquer entre elles selon une véritable approche Zero Trust.

Pas de modification manuelle ni de temps d'arrêt : avec la segmentation logicielle, nul besoin de modifier le réseau ni de créer un VLAN, ce qui permet de réaliser d'importantes économies opérationnelles. Elle ne nécessite pas non plus de temps d'arrêt des applications ou de modification en raison d'une migration vers un nouveau VLAN. Il s'agit de détails qui ont toute leur importance. Dans de nombreuses applications pour lesquelles les temps d'arrêt sont très coûteux ou impossibles, il s'agit de la seule façon de fournir cette mesure de sécurité cruciale.

Visibilité étendue : en outre, les solutions avancées de segmentation logicielle, conçues pour relever les défis de segmentation de trafic est-ouest, fournissent un outil de visibilité intégré qui aide à identifier les limites des segments et les dépendances des applications. Il en résulte un processus efficace qui élimine les erreurs opérationnelles lors de la création des règles.

Automatisation des règles et des contrôles : la segmentation logicielle permet également d'appliquer des règles de manière dynamique, de sorte que, lorsque les charges de travail augmentent ou diminuent, elles soient automatiquement attribuées à la règle appropriée. Cette approche permet d'économiser des ressources considérables en éliminant le besoin de déplacements, d'ajouts ou de modifications manuels.

Indépendance par rapport à l'infrastructure : l'un des principaux avantages de la segmentation logicielle est qu'elle est indépendante de l'infrastructure. Le même outil qui offre visibilité et segmentation sur n'importe quelle infrastructure : bare metal, virtualisée, PaaS, cloud, conteneurs, etc., le tout dans un seul environnement de surveillance et avec un flux de travail singulier. Il en résulte une grande liberté opérationnelle qui permet d'atteindre des normes de sécurité sans aucune contrainte quant au choix de l'infrastructure sous-jacente.

Plus de revenus et des relations plus durables : plus important encore, la segmentation logicielle représente une opportunité considérable pour les opérateurs de centres de données. Bien qu'ils gèrent et fournissent la segmentation interne, ils peuvent tirer parti de la formation, des outils et des processus pour offrir à leur client un service géré dont ils ont largement besoin (en gérant la segmentation non seulement pour les applications hébergées, mais aussi pour les applications qui se trouvent sur les sites du client ou dans le cloud) au sein du même outil, dans le même environnement. Le potentiel de revenus supplémentaires qui en découle crée également une dépendance plus forte à l'égard de l'opérateur, qui se traduit alors par des relations plus durables et une augmentation des bénéfices.

Pourquoi Akamai

Pour présenter ces avantages, une solution de segmentation logicielle doit répondre à un certain nombre de critères essentiels. Elle doit offrir une visibilité approfondie au niveau des processus de toutes les applications exécutées dans l'environnement informatique et la possibilité de mapper tous les flux de données entre elles. La possibilité d'étiqueter correctement les actifs pour créer des règles et de modifier automatiquement les étiquettes au fur et à mesure de l'évolution des charges de travail sont également des facteurs déterminants pour un déploiement et une gestion efficaces. Et la solution doit être indépendante de la plateforme et de l'infrastructure. Les règles doivent pouvoir suivre leurs applications respectives et fonctionner de manière cohérente dans plusieurs environnements. Enfin, la solution doit permettre la mise en place d'un modèle opérationnel automatisé et simplifié pour la création, la gestion et l'application des règles.

Seule la solution Akamai Guardicore Segmentation répond à tous ces critères. La segmentation logicielle représente notre cœur de métier. Notre solution offre une visualisation graphique sans précédent de tous les actifs de l'environnement et de leurs dépendances, qu'il s'agisse de systèmes bare metal, de machines virtuelles, d'un cloud public, de conteneurs ou de terminaux IoT. Cette visibilité approfondie accélère considérablement le processus d'identification, de regroupement et de création de règles de sécurité autour de microsegments d'applications.

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