Akamai

LIVRE BLANC

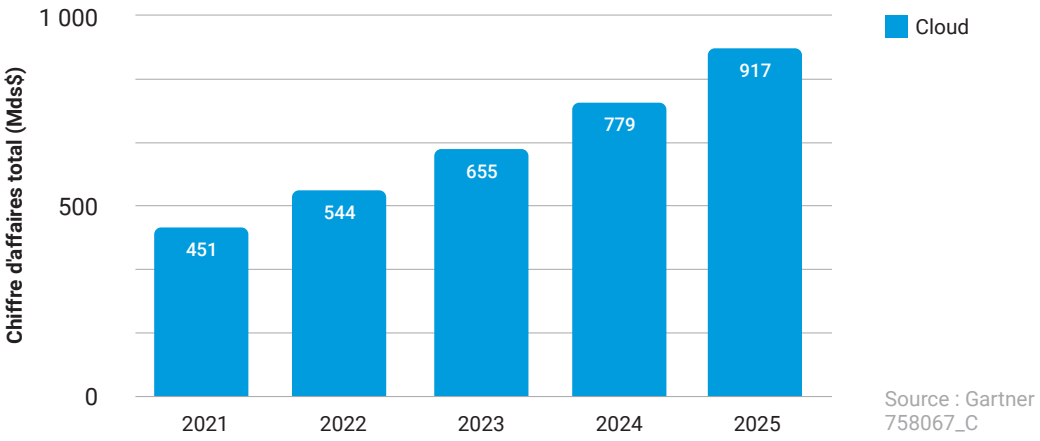
Ouvrir la voie à la microsegmentation

Guide stratégique de mise en œuvre de la microsegmentation dans les clouds hybrides

Davantage de clouds en prévision

La migration de grandes quantités de données et de traitement de données vers le cloud, ou plus précisément vers des clouds multiples, est sans doute le plus grand changement de l'informatique d'entreprise au cours de la dernière décennie. De plus en plus d'entreprises se tournent vers les clouds publics et, en général, vers des architectures de centres de données hybrides public-privé. Dans le même temps, elles tirent parti de l'infrastructure en tant que service (IaaS) dans leur quête d'une agilité toujours plus grande. L'analyste technologique Gartner prévoit que d'ici 2025, un peu plus de la moitié de toutes les dépenses informatiques dans les segments de marché adressables seront passées des solutions traditionnelles au cloud public, contre 41 % en 2022, et que le total des dépenses liées au cloud public devrait dépasser 900 milliards de dollars d'ici 2025.[1]

La distinction entre « le cloud » et les « clouds multiples » n'est pas anodine. De plus en plus, les entreprises adoptent des plateformes et des fournisseurs de services multicloud. Une chose est sûre : l'idée d'un centre de données d'entreprise en tant qu'espace physique unique et sécurisé est en train de subir le même sort que les dinosaures. Les centres de données actuels constituent de plus en plus un mélange hétérogène d'environnements et de technologies associant des serveurs physiques, des machines virtuelles et des conteneurs dans des installations sur site, des clouds privés et des fournisseurs IaaS de clouds publics. Ces installations disparates ne sont pas statiques : les entreprises déplacent constamment les données et les charges de travail entre leurs différents environnements sur site et dans le cloud, en fonction des niveaux de trafic et des demandes de traitement.



Prévisions de chiffre d'affaires des services cloud public à l'échelle mondiale (en milliards)

Cette complexité accrue génère de nouvelles vulnérabilités et élargit les surfaces d'attaque

Les clients du cloud bénéficient incontestablement de l'agilité, de l'élasticité et de l'évolutivité accrues que l'IaaS leur offre. Ces avantages constituent une grande partie de ce qui rend le cloud si attrayant. En contrepartie, la complexité de la gestion s'accroît considérablement, la visibilité sur les charges de travail dans les différents environnements diminue et un paysage de cybersécurité inconnu s'ouvre à eux. Travailler avec plusieurs fournisseurs de cloud signifie que les équipes de sécurité doivent faire face à des normes et fonctionnalités de sécurité très différentes. Les outils de sécurité traditionnels conçus pour les serveurs et les terminaux sur site ne peuvent tout simplement pas gérer l'échelle et la complexité du cloud. Les nouveaux outils proposés par les fournisseurs IaaS peuvent être efficaces dans l'environnement du fournisseur, mais sont peu utiles dans une infrastructure multi-fournisseurs.

En outre, même à l'ère de la virtualisation et du « tout logiciel », la mentalité en matière de sécurité (et donc la plupart des investissements) est toujours fondée sur la nécessité perçue de bloquer les attaques spécifiquement au point d'entrée. Il ne s'agit pas de critiquer les défenses périmétriques : elles sont toujours très pertinentes dans le système de sécurité informatique, mais elles ne sont plus aussi performantes lorsque le périmètre est en perpétuelle évolution. Les données et charges de travail vont et viennent entre les clouds publics et privés et les centres de données sur site, et les utilisateurs qui y accèdent travaillent de plus en plus à partir de sites distants qui peuvent ou non avoir mis en place les contrôles de sécurité appropriés.

Le nombre de violations de données signalées chaque année suffit à nous faire comprendre que des attaquants astucieux parviennent à franchir les défenses périmétriques presque à volonté. Et une fois à l'intérieur, ils découvrent un réseau relativement plat, où les actifs résidant dans le périmètre ne sont pratiquement pas surveillés. Malgré la flexibilité acquise par les entreprises, la complexité accrue de la gestion et de la sécurisation des infrastructures multicloud a multiplié de façon exponentielle la surface d'attaque ; avec peu ou pas de contrôles de communication en place, chaque serveur individuel devient une surface d'attaque en soi. Par conséquent, les attaquants peuvent passer plus de temps à se déplacer latéralement, sans être détectés, entre les charges de travail du trafic est-ouest pour atteindre vos ressources les plus critiques.

La segmentation du réseau est une pratique de sécurité bien comprise et bien établie, mais de nos jours, elle peut être difficile à mettre en œuvre dans des infrastructures informatiques dynamiques et à l'échelle du cloud, où les charges de travail communiquent et migrent souvent d'un segment à l'autre. Les clients d'entreprise du cloud ont pris conscience de la nécessité de segmenter davantage leurs applications et leurs charges de travail afin de contrôler étroitement les flux de communication en temps réel et de détecter et contrecarrer les menaces au sein du centre de données avant qu'elles ne fassent des dégâts. Il leur faut une solution qui réduise la complexité de la sécurité en travaillant de manière cohérente par-delà les frontières de l'infrastructure pour réduire la surface d'attaque globale, ce qui permet aux équipes de sécurité de détecter plus rapidement davantage de menaces et de limiter leur propagation.

C'est là que la microsegmentation entre en jeu.

Définition de la microsegmentation

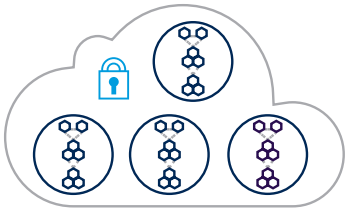
Gartner définit la microsegmentation comme « le processus de mise en œuvre de l'isolation et de la segmentation à des fins de sécurité au sein du centre de données virtuel ». En outre, la microsegmentation « réduit le risque de propagation latérale des attaques avancées dans les centres de données d'entreprise et permet aux entreprises d'appliquer des règles de segmentation cohérentes dans les charges de travail sur site et dans le cloud. »[2]

La microsegmentation fonctionne généralement en établissant des règles de sécurité autour d'applications individuelles ou de groupes d'applications, indépendamment de l'endroit où elles résident dans le centre de données hybride. Ces règles déterminent quelles applications et quels composants peuvent ou non communiquer entre eux. Ainsi, toute tentative de communication non autorisée constitue un indicateur instantané de menace. Dans le meilleur des cas, les technologies de microsegmentation sont indépendantes de l'infrastructure, si bien que les règles de sécurité peuvent continuer à protéger leurs applications respectives lorsqu'elles se déplacent d'un environnement cloud à l'autre.

Domaines de solution pour la segmentation

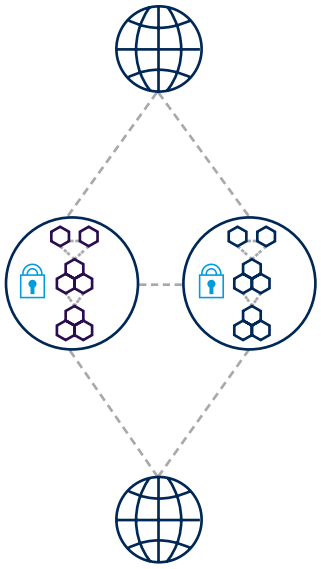
Segmentation de l'infrastructure

Trafic applicatif sécurisé au sein d'une infrastructure particulière.



Segmentation de l'application

Trafic sécurisé entre les applications et les réseaux externes.



Microsegmentation

Règles sécurisant le trafic au sein des applications avec un contexte supplémentaire comme l'attribution au niveau du processus.

2 Gartner, « Technology Insight for Microsegmentation », mars 2017 ; « Hype Cycle for Cloud Security 2017 », juillet 2017

Intérêt de la microsegmentation

Les centres de données dynamiques actuels obligent les entreprises à déplacer leur attention de la prévention des intrusions et de la gestion des accès vers les charges de travail et les applications elles-mêmes. Et cela semble se produire à un rythme accéléré. Dès 2017, Gartner a commencé à remarquer une tendance vers « une concentration accrue sur la protection des charges de travail des serveurs contre les menaces ciblées avancées qui contournent les protections traditionnelles basées sur le périmètre et les signatures. Généralement, ces attaques sont motivées par des raisons financières et ciblent les charges de travail des serveurs et des applications dans le but d'accéder à des données ou à des transactions sensibles. »[3]

L'un des principaux moteurs de la microsegmentation est la nécessité de protéger les applications et les charges de travail critiques. Cela peut sembler être une simple question d'intérêt personnel ou de bon sens commercial, mais dans de nombreux cas, cela est également imposé par des règles de sécurité et des exigences réglementaires.

Les équipes de sécurité doivent trouver des moyens de réduire la surface d'attaque qui s'étend dans les centres de données, ce qui implique de réduire la vulnérabilité des serveurs exécutant des applications. Les techniques d'authentification traditionnelles, comme le blocage des signatures ou la mise en liste des applications autorisées, sont trop facilement contournables par des attaquants chevronnés. La microsegmentation permet aux équipes de définir et d'appliquer des règles d'accès et de communication strictes et granulaires. Elle devrait également améliorer la visibilité des flux d'applications et permettre aux équipes de mieux évaluer leur position en matière de sécurité.

Avez-vous besoin de la microsegmentation ?

En répondant à quelques questions simples, vous pourrez déterminer si vous avez besoin de microsegmentation.

- Votre secteur d'activité est-il réglementé ou devez-vous vous conformer à des réglementations régissant la sécurité des données et des transactions ?
- Disposez-vous d'une infrastructure hybride dont les charges de travail s'étendent sur des clouds multiples ?
- Exécutez-vous des applications dans des machines virtuelles ou des conteneurs ?
- Ressentez-vous une perte de visibilité et de contrôle des charges de travail ?
- Pouvez-vous déterminer, à tout moment, qu'une menace est présente ou qu'une attaque est en cours dans votre centre de données ?
- Pouvez-vous contrôler la sécurité de l'ensemble de votre infrastructure par le biais d'un « environnement de surveillance unique » ?

Les quatre principaux obstacles du parcours

Si les experts en sécurité s'accordent généralement sur la nécessité de la microsegmentation dans les centres de données dynamiques d'aujourd'hui, pourquoi est-elle considérée comme si difficile à mettre en œuvre de manière efficace et fructueuse ? Les organisations tentant de mettre en œuvre la microsegmentation à l'aide d'outils conventionnels se heurtent généralement à quatre obstacles majeurs :

1. **Manque de visibilité au niveau des processus**
   C'est probablement le premier obstacle que vous rencontrerez : vous ne pouvez pas sécuriser ce qui n'est pas visible. La microsegmentation consiste à sécuriser des applications individuelles et des groupes d'applications ainsi que des processus de flux de travail. Les équipes de sécurité ont besoin de visibilité sur les flux de trafic est-ouest réels pour les comprendre dans leur contexte. La plupart des outils n'offrent pas cette capacité d'analyse.

2. **Absence de prise en charge du multicloud hybride**
   Les règles de sécurité de microsegmentation doivent pouvoir évoluer facilement dans les environnements sur site et dans le cloud public, et suivre les charges de travail dans leurs déplacements. Les outils conçus pour fonctionner dans un environnement spécifique sont inefficaces dans les environnements hybrides.

3. **Moteurs de règles peu flexibles**
   Comme indiqué précédemment, les centres de données d'aujourd'hui ne sont pas statiques. Les mesures de sécurité ne peuvent pas l'être non plus. L'état d'esprit « configurer puis oublier » n'est plus de mise. Malheureusement, les outils existants des fournisseurs de cloud n'offrent pas la flexibilité nécessaire pour définir, tester et affiner les règles en permanence. Ce défi est d'autant plus important dans les infrastructures hybrides nécessitant plusieurs outils de gestion des règles.

4. **Aucune intégration à des contrôles complémentaires**
   Correctement mise en œuvre, la microsegmentation ne sert pas seulement à protéger les processus, mais aussi à prévenir les attaques. Cependant, les outils de microsegmentation à fonction unique n'incluent généralement pas de fonctionnalités de détection des violations, laissant à l'utilisateur le soin d'intégrer les outils et de les faire fonctionner ensemble de manière efficace. Cette approche disparate comporte un risque élevé d'échec.

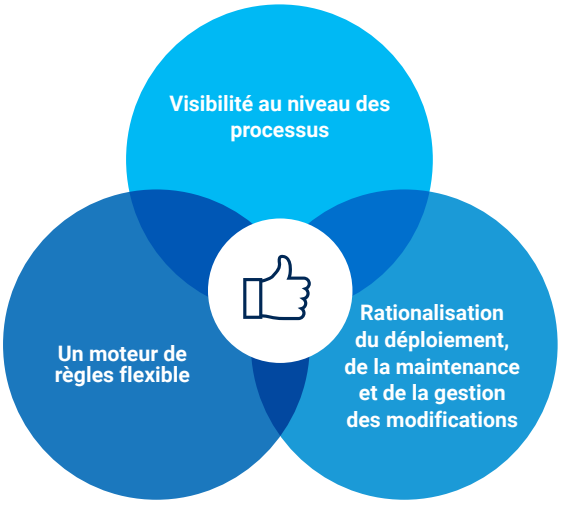
Les projets infructueux sont la norme, pas l'exception

Compte tenu de tous les obstacles, il n'est pas surprenant que la plupart des projets de microsegmentation subissent des cycles de mise en œuvre extrêmement lents, des augmentations des coûts, des ressources fiscales et, en définitive, ne parviennent pas à atteindre leurs objectifs. Les entreprises se heurtent souvent à la difficulté de déterminer ce qui doit être segmenté (en raison d'un manque de visibilité) et de décider de l'ampleur de la segmentation nécessaire. Elles peuvent passer des mois à élaborer des feuilles de calcul contenant des règles complexes pour les communications au niveau des processus, incapables de reconnaître les possibilités de regroupement des applications et de rationalisation des règles. Trop souvent, elles pêchent par excès de segmentation, c'est-à-dire qu'elles définissent trop de règles distinctes, ce qui entraîne une trop grande complexité en matière de sécurité, alors que c'est précisément ce qu'il faut éviter. Comme l'a noté Gartner, « … plus de 70 % des projets de segmentation verront leur conception initiale remaniée en raison d'une segmentation excessive. »[4]

Une segmentation excessive risque de ralentir les applications et, au final, l'activité. Mais le pendule peut se déplacer trop loin dans l'autre sens, vers une segmentation insuffisante, et finir par compromettre votre posture de sécurité.

Stratégie pour une microsegmentation réussie

Le processus de mise en œuvre de la microsegmentation n'est pas linéaire. La route pour identifier, comprendre et contrôler les flux des communications dans votre environnement est semée d'embûches. Les équipes de sécurité ont besoin de flexibilité lors de l'élaboration des règles de sécurité, afin d'intégrer constamment de nouveaux changements ou ajouts sans interrompre les applications. De nombreuses solutions offrent des moteurs de création de règles peu flexibles, ce qui oblige les équipes de sécurité à mettre en œuvre des règles incomplètes ou inefficaces avant qu'elles ne soient prêtes.



Pour simplifier, une mise en œuvre réussie est celle qui surmonte ou contourne les quatre principaux obstacles, en évitant une complexité excessive et en réduisant le risque de segmentation insuffisante ou excessive grâce à une approche progressive. Cela signifie qu'il faut disposer d'une solution répondant aux exigences suivantes :

- **Visibilité au niveau du processus :** Les équipes doivent pouvoir révéler, collecter et normaliser tous les flux est-ouest et nord-sud, disposer d'outils permettant de découvrir automatiquement les applications et de comprendre leurs besoins de communication, et filtrer sur de multiples attributs d'application pour faciliter l'étiquetage et le regroupement des ressources pouvant partager des règles.

- **Un moteur de règles flexible :** Vous devez être en mesure de concevoir simultanément des règles de conformité et de meilleures pratiques de niveau supérieur pour les grands segments et des règles plus granulaires pour les microsegments. La solution doit vous permettre de passer progressivement de l'alerte à leur application. Enfin, elle doit vous permettre d'établir des règles fonctionnant sur toutes les plateformes, tous les terminaux et tous les clouds.

- **Rationalisation du déploiement, de la maintenance et de la gestion des changements :** Le système doit faciliter le déploiement, la maintenance et la modification des règles en fonction des besoins. Il doit intégrer des fonctionnalités intégrées de détection des violations et de réponse aux incidents. Enfin, vos règles doivent être suffisamment bien définies pour que vous puissiez les intégrer dans des outils de déploiement automatisé (CI/CD) pour chaque nouvelle application lancée.

Fonctionnalités idéales de la solution

Bien entendu, il existe de nombreux outils de microsegmentation sur le marché, et tous ne facilitent pas la tâche. Pour garantir une mise en œuvre fluide et fructueuse, veillez à choisir une solution dotée des fonctionnalités suivantes :

- **Découverte automatique des applications**, avec une visibilité complète au niveau des processus pour les serveurs bare-metal, les machines virtuelles et les conteneurs

- La possibilité de définir des **requêtes robustes et étendues** pour créer des étiquettes contextuelles et des groupes d'objets

- Un **moteur de règles flexible** avec une conception intelligente qui vous aide à affiner, renforcer et maintenir les règles

- Une **capacité intégrée de détection des violations multi-méthodes** pour détecter davantage de menaces plus rapidement et limiter leur propagation

- **Prise en charge de l'infrastructure hybride** : une plateforme unique fonctionnant avec n'importe quelle infrastructure, n'importe quels centres de données, clouds publics et privés, etc.

Une solution dotée de ces capacités essentielles vous mettra sur la voie la plus fructueuse pour mettre en œuvre la microsegmentation, vous permettra de surmonter les obstacles et les complexités connus et vous préparera à récolter tous les avantages commerciaux d'une infrastructure de cloud hybride flexible sans sacrifier la sécurité.

Les centres de données hybrides, les plateformes multicloud et l'IaaS offrent aux entreprises plus de flexibilité, d'évolutivité et d'agilité que ne le permettrait un centre de données sur site « fermé ». Mais ils laissent également les applications et les charges de travail (les actifs réels que les cyberattaquants ciblent) plus exposées et vulnérables. Bien que la microsegmentation soit largement considérée comme la meilleure pratique pour protéger les charges de travail dans le cloud, les entreprises ont du mal à la mettre en œuvre correctement. La bonne nouvelle, c'est qu'il n'est pas nécessaire de tout faire en même temps. Les solutions avancées actuelles, associées à une approche progressive, étape par étape, facilitent grandement la mise en œuvre de la microsegmentation. Cela se traduit par une meilleure sécurité pour les actifs les plus importants de votre organisation.

Pour en savoir plus sur la réussite de la mise en œuvre de la microsegmentation, rendez-vous sur akamai.com/guardicore

1 « Selon Gartner, plus de la moitié des dépenses informatiques des entreprises dans les principaux segments du marché seront consacrées au cloud d'ici à 2025. » Gartner, 9 février 2022.

2 Heiser, Jay. « Hype Cycle for Cloud Security, 2017. » Gartner, 17 juillet 2017.

3 MacDonald, Neil. « Market Guide for Cloud Workload Protection Platforms. » Gartner, 22 mars 2017.

4 Young, Greg. « Best Practices in Network Segmentation for Security. » Gartner, 28 juillet 2016.