LIVRE BLANC

Analyse des principaux cas d'usage de la microsegmentation

Par John Grady, Analyste senior chez Enterprise Strategy Group

Janvier 2023

Ce livre blanc d'Enterprise Strategy Group a été commandé par Akamai et est distribué sous licence par TechTarget, Inc.

Sommaire

Résumé

Le Zero Trust s'est généralisé dans le secteur de la cybersécurité. Cependant, l'envergure de l'initiative et les multiples interprétations de son importance stratégique ont semé le doute sur le meilleur point de départ et les outils les plus appropriés pour prendre en charge cette infrastructure. S'il n'y a pas de parcours unique pour adopter le Zero Trust, cette stratégie repose en somme sur l'idée que les ressources et éléments ne peuvent interagir que si une politique spécifique l'y autorise, ce qui souligne le rôle crucial de la microsegmentation.

Aujourd'hui, l'usage des outils de microsegmentation est plutôt restreint, mais l'on peut s'attendre à ce qu'il se développe sensiblement, compte tenu de l'importance de la microsegmentation dans le cadre du Zero Trust et de son applicabilité à divers cas d'usage. Que les entreprises se tournent vers le Zero Trust pour contrer les menaces, stimuler leur efficacité interne ou moderniser leur stratégie globale de sécurité, la microsegmentation peut s'avérer bénéfique. Plus précisément, l'approche de microsegmentation basée sur des logiciels et reposant sur l'intelligence artificielle proposée par Akamai assure une visibilité détaillée, ce qui permet aux entreprises d'entraver les mouvements latéraux, d'intercepter les attaques de ransomwares et d'appliquer les principes du Zero Trust de manière uniforme dans tout l'environnement.

Que les entreprises se tournent vers le Zero Trust pour contrer les menaces, stimuler leur efficacité interne ou moderniser leur stratégie globale de sécurité, la microsegmentation peut s'avérer bénéfique.

Le Zero Trust gagne en popularité, mais il est primordial de définir des priorités bien distinctes

La complexité des environnements d'entreprise s'accroît à mesure que les ressources migrent vers le cloud, que les modèles d'affaires numériques s'imposent et que les utilisateurs sont de plus en plus dispersés. Ces évolutions rendent la tâche de l'équipe de cybersécurité plus ardue, car les pirates exploitent les failles dans les défenses pour lancer des attaques par ransomwares, dérober des informations clients ou exfiltrer de la propriété intellectuelle sensible. Malheureusement, les méthodes de sécurité conventionnelles basées sur des contrôles de périmètre très permissifs ne suffisent plus à faire face à ces réalités, poussant ainsi les équipes de sécurité à repenser leurs stratégies. Par ailleurs, les attaques se font de plus en plus nombreuses et sophistiquées, rendant difficile pour les équipes de sécurité de prendre en compte, traiter et neutraliser toutes les menaces.

Ces défis ont amené de nombreux clients à envisager le concept de Zero Trust. Bien que les stratégies Zero Trust ne soient pas nouvelles, elles ont suscité l'intérêt des entreprises comme un moyen d'adopter une approche de cybersécurité plus dynamique, moins axée sur les privilèges et davantage fondée sur les risques. Un modèle Zero Trust supprime toute confiance implicite dans l'environnement et vérifie constamment chaque interaction numérique. Par conséquent, la stratégie Zero Trust permet aux équipes de sécurité d'avoir plus confiance dans la protection et la disponibilité de leurs ressources, utilisateurs et appareils. Cependant, l'application universelle du Zero Trust, associée à des opinions et à des définitions parfois contradictoires sur ce qu'il représente, a semé la confusion et rend difficile pour les entreprises de déterminer par où commencer.

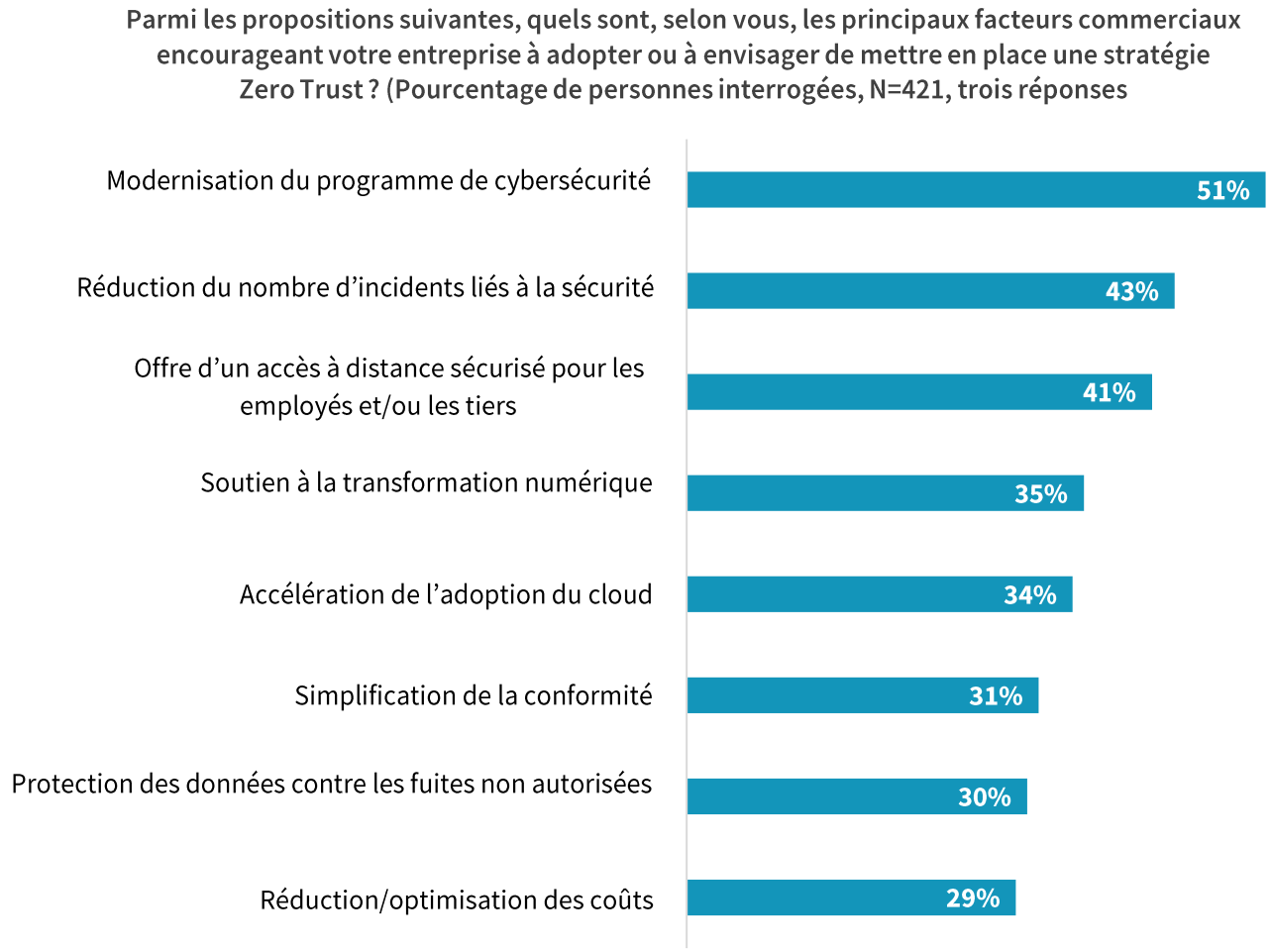
L'évaluation des priorités organisationnelles et des résultats attendus permet de préciser les objectifs et de déterminer par où démarrer une initiative Zero Trust. Plusieurs facteurs incitent les entreprises à se tourner vers le Zero Trust (voir Figure 1)[1]. L'objectif le plus fréquent est la modernisation de la cybersécurité, mentionnée par 51 % des personnes interrogées. Cette préoccupation a été soulignée par le gouvernement fédéral américain via les décrets présidentiels

Le concept du Zero Trust repose sur une idée simple : garantir que les ressources et les éléments en réseau ne peuvent interagir entre eux que si une politique spécifique les y autorise explicitement.

[1]Source : Résultats de l'enquête d'Enterprise Strategy Group, *The State of Zero Trust Security Strategies,* mai 2021.

sur la cybersécurité émis par l'administration Biden, qui a expressément cité l'architecture Zero Trust dans ses exigences relatives à la modernisation. Bien qu'ils ne ciblent pas explicitement le secteur privé, ces décrets peuvent fournir des lignes directrices aux équipes de sécurité en dehors du gouvernement fédéral. Parmi les autres objectifs stratégiques du Zero Trust figurent le soutien à la transformation numérique (35 %) et l'accélération de l'adoption du cloud (34 %). Ces facteurs mettent en évidence l'attente de nombreuses entreprises souhaitant que l'équipe de sécurité contribue à la croissance de l'entreprise, plutôt qu'à simplement protéger les ressources. Des objectifs plus tactiques comme la réduction du nombre d'incidents liés à la sécurité (43 %), la mise en place d'un accès à distance sécurisé (41 %), la simplification de la conformité (31 %) et la prévention de l'exfiltration des données (30 %) sont aussi fréquemment mentionnés.

Figure 1 : les facteurs favorisant le Zero Trust



Source : Enterprise Strategy Group, une division de TechTarget, Inc.

Le fait de limiter l'objectif initial d'un projet Zero Trust peut faciliter la tâche de l'équipe de sécurité pour définir les outils nécessaires à l'appui de la stratégie, du moins dans certains cas. Par exemple, si l'ambition est d'améliorer l'accès sécurisé à distance pour les employés et les tiers, de nombreux choix se porteront sur un accès réseau ZTNA. Dans ce scénario, il est possible d'envisager des instruments d'identification comme l'authentification multifactorielle (MFA). Toutefois, certains facteurs peuvent laisser une marge d'interprétation concernant les exigences technologiques, et bon nombre d'entreprises et d'organismes, même après les avoir affinés, travaillent sur plusieurs objectifs. Dans de tels cas, il est primordial pour les entreprises de définir les outils et méthodes capables de gérer divers scénarios d'utilisation et résultats attendus.

La microsegmentation est actuellement sous-exploitée dans la prise en charge des modèles Zero Trust

Même s'il n'y a pas une seule façon d'adopter le Zero Trust, cette stratégie repose avant tout sur l'assurance que les ressources et entités ne peuvent interagir entre elles que si une politique spécifique les y autorise expressément. L'un des aspects essentiels de la philosophie Zero Trust d'une entreprise doit donc être la capacité à bien segmenter les ressources pour limiter les conséquences des attaques réussies. Cet aspect peut être lié à un objectif général, comme la modernisation de la cybersécurité, ou concerner un but plus spécifique, comme la prévention de l'exfiltration de données.

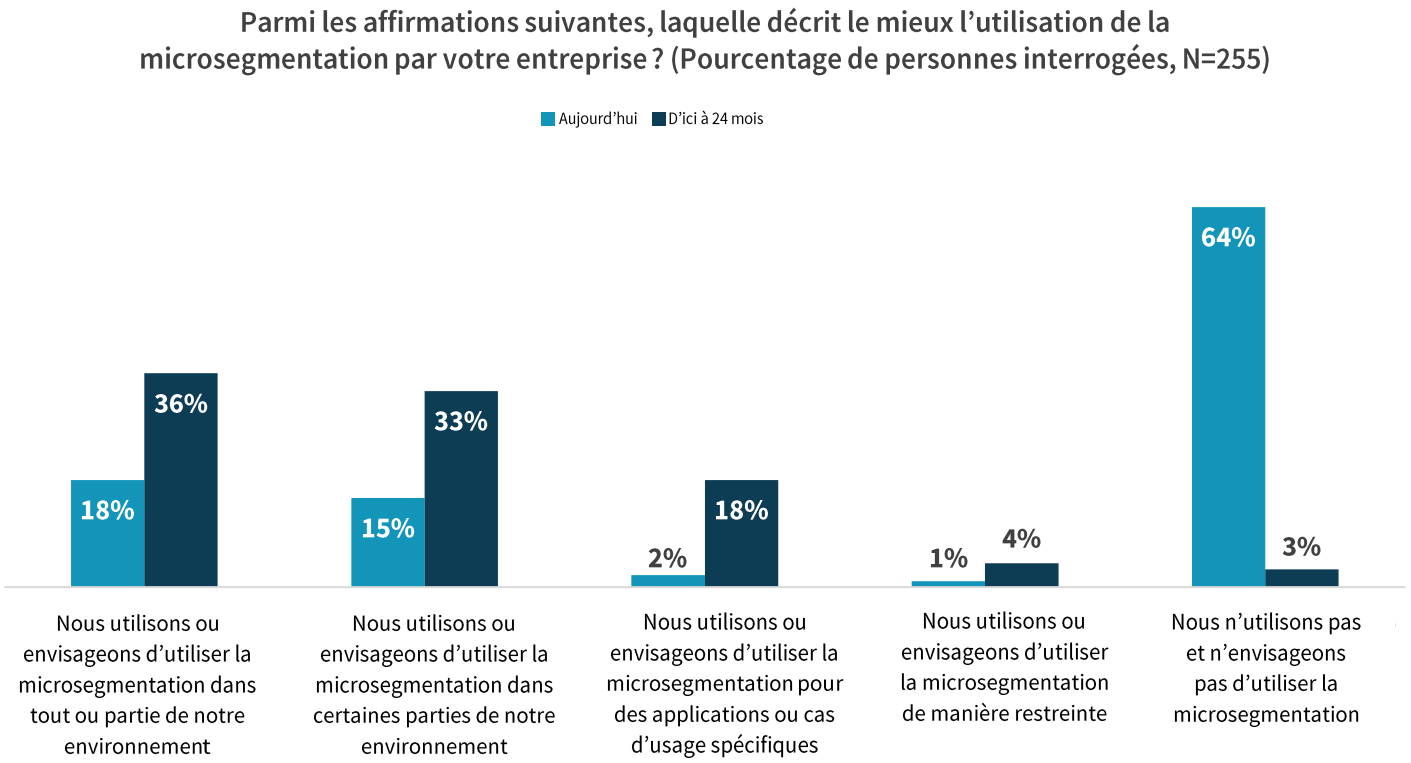
Cependant, dans le contexte actuel, une segmentation à grande échelle s'avère souvent insuffisante. Il est nécessaire d'adopter une microsegmentation plus détaillée pour assurer correctement la protection des ressources de l'entreprise. Les architectures d'applications modernes s'appuient souvent sur des workloads distribuées sur plusieurs instances de serveurs et parfois sur plusieurs environnements cloud. La segmentation des ressources en fonction de leur localisation est une approche dépassée qui ne résout pas les problèmes auxquels les équipes de sécurité sont confrontées aujourd'hui.

Traditionnellement, les entreprises étaient réticentes à l'idée d'adopter des outils de microsegmentation. Une étude menée par l'Enterprise Strategy Group (ESG) de TechTarget a montré que 28 % des entreprises considèrent la microsegmentation comme trop complexe. Cependant, cette réticence est sans doute en grande partie due à l'usage, par les équipes de sécurité, d'outils inadaptés pour la microsegmentation. Plus précisément, les études de l'ESG ont montré que 55 % des entreprises affirment utiliser des outils basés sur l'infrastructure pour la microsegmentation, comme des pare-feu, tandis que seulement 8 % utilisent des outils basés sur l'hôte[2]. Les pare-feu ne sont pas capables d'appliquer les règles détaillées nécessaires à la microsegmentation. De plus, ces outils n'offrent qu'une visibilité limitée sur les workloads applicatives et peinent à gérer tous les aspects de l'environnement, qu'il soit sur site ou dans le cloud.

Cette situation a conduit à une sous-exploitation de la microsegmentation. Malgré l'importance cruciale de la microsegmentation pour le concept de Zero Trust, seulement 36 % des entreprises la mettent en œuvre actuellement, selon une étude ESG (voir Figure 2). Heureusement, nombre d'entreprises reconnaissent qu'il s'agit d'une faille majeure dans leurs défenses. Ainsi, 91 % d'entre elles prévoient de recourir à la microsegmentation dans les 24 prochains mois[3]. Au final, la microsegmentation renforce les principaux avantages du Zero Trust en protégeant les réseaux physiques, virtuels et cloud contre les menaces internes et externes, et devrait constituer un élément clé de toute stratégie Zero Trust.

[2]Source : Enterprise Strategy Group Complete Survey Results, *Network Security Trends in Hybrid Cloud Environments*, décembre 2021.
[3] Ibid.

Figure 2 : adoption de la microsegmentation



Source : Enterprise Strategy Group, une division de TechTarget, Inc.

Principaux cas d'usage de la microsegmentation

La microsegmentation est largement applicable à différents scénarios d'utilisation du Zero Trust, ce qui explique pourquoi elle est plus mise en valeur que jamais. Mais avant tout, la microsegmentation constitue un excellent point de départ pour une démarche Zero Trust, car elle peut sécuriser les ressources les plus sensibles d'une entreprise, notamment si elle offre une visibilité très précise sur la workload et les relations entre les entités. Dans toute démarche Zero Trust, la mise en place d'une base de données des flux de trafic et des dépendances est une étape fondamentale permettant d'éliminer la confiance implicite sans perturber les activités. Cette approche permet aux équipes de sécurité de sécuriser rapidement leurs ressources les plus sensibles afin de minimiser les conséquences en cas d'intrusion durant la mise en place de la stratégie Zero Trust. Une fois ce niveau atteint, les équipes de sécurité peuvent se concentrer sur certains des autres cas d'usage pris en charge par la microsegmentation.

Prévention des menaces

Le Zero Trust est une infrastructure de sécurité, et la finalité de la sécurité est de défendre l'entreprise contre les cybermenaces. C'est pourquoi certains des principaux cas d'usage de la microsegmentation ont pour but de prévenir les menaces et de réduire leur incidence sur les ressources de l'entreprise, notamment :

- Cloisonnement des ressources critiques. Avant de définir les priorités en matière de protection, les équipes de sécurité doivent procéder à l'étude et à l'équilibrage des risques. Un intérêt particulier doit être porté aux applications à forte valeur ajoutée comme celles contenant des données client réglementées, des informations de propriété intellectuelle ou d'autres types de données sensibles. En effet, la compromission de ces systèmes peut avoir de graves conséquences. Pour renforcer les mesures de sécurité, la microsegmentation permet aux équipes de sécurité de séparer ces applications et leurs workloads du reste de l'infrastructure.

- Limitation des mouvements latéraux. Un principe essentiel, mais souvent négligé, du Zero Trust est de considérer comme acquis que les ennemis peuvent accéder au réseau de l'entreprise. La multiplication des points d'accès, qu'il s'agisse de terminaux classiques, de serveurs, de ressources du cloud ou d'appareils intelligents, rend les intrusions presque inévitables. Il est donc crucial de limiter la portée potentielle d'une attaque. C'est là que la microsegmentation intervient : elle bloque les menaces éventuelles en empêchant les pirates de circuler librement sur le réseau.

- Détection et réaction aux menaces. Lorsqu'il s'agit de réagir à des menaces, chaque seconde compte. C'est là que les outils de microsegmentation peuvent faire toute la différence pour les équipes de sécurité. Ils permettent en effet de comprendre rapidement les vecteurs d'attaque potentiels en examinant les liaisons entre les applications. Ils bloquent aussi les ports exploités par les cybercriminels lors d'une intrusion et mettent immédiatement les systèmes concernés en quarantaine pour les isoler du reste du réseau. Plus encore, ils confinent l'attaque à son point d'origine initial.

Protection contre les ransomwares

La recrudescence continue des attaques par ransomwares et leur incidence a propulsé ce problème à un niveau de priorité élevé, voire au niveau du conseil d'administration dans certaines entreprises. Si se préparer aux ransomwares nécessite une sécurité renforcée et de solides capacités en matière de protection des données et de gestion des incidents, la microsegmentation permet aux entreprises de se prémunir efficacement contre une attaque. Lors d'une attaque, les pirates visent souvent des informations et systèmes sensibles une fois qu'ils ont réussi à infiltrer l'environnement et qu'ils ont eu le temps de mener une reconnaissance. Si l'on se sert de la microsegmentation pour protéger les ressources essentielles et limiter les mouvements latéraux, les intrus sont moins libres de se déplacer dans l'environnement. De plus, lorsqu'une attaque par ransomware est détectée, une entreprise ayant recours à la microsegmentation peut rapidement couper les canaux de communication utilisés par les pirates et isoler les serveurs infectés pour empêcher sa propagation.

Efficacité dans toute l'entreprise

La protection de l'environnement est certes la priorité de l'équipe de sécurité. Cependant, à l'ère actuelle, il est également nécessaire qu'elle n'entrave pas l'efficacité de l'entreprise. Il est d'ailleurs avéré que lorsque les équipes de sécurité parviennent à aider leurs collègues, les services informatiques de l'entreprise s'en trouvent améliorés. Cette synergie peut se traduire de différentes manières. Parmi les plus courantes, on peut citer :

- Soutien à l'adoption du cloud La migration vers le cloud n'est pas un concept novateur, mais la sécurité reste une préoccupation majeure pour beaucoup d'entreprises. Ces inquiétudes peuvent découler d'une méconnaissance des contrôles de sécurité natifs sur les plateformes d'infrastructure en tant que service (IaaS), ou bien d'un éventuel manque de cohérence en matière de sécurité dans les environnements de cloud hybride. La microsegmentation rassure les entreprises en offrant des contrôles pouvant s'appliquer à tous les aspects de l'environnement. Elle renforce également la cohérence de la sécurité dans les scénarios de cloud hybride.

- Modernisation des applications. En plus de la migration vers le cloud, l'adoption de nouvelles architectures d'applications comme les conteneurs ne cesse de s'accélérer. Ces modèles permettent aux équipes de conception, de création et de déploiement d'applications de travailler plus rapidement que jamais. L'utilisation d'outils assurant la protection de ces ressources, sans entraver le rythme des développeurs, a des répercussions positives sur l'entreprise. Les outils de microsegmentation offrant une visibilité sur les flux de trafic dans les environnements conteneurisés et appliquant automatiquement des règles de segmentation lorsque les conteneurs sont mis en ligne ou déplacés, apportent un précieux soutien aux équipes de développement pour garantir la sécurité de leurs applications.

- Optimisation de la conformité Les questions de réglementation absorbent de plus en plus de temps, de ressources budgétaires et d'attention. Il peut s'avérer beaucoup moins onéreux d'isoler le plus possible les risques de sécurité de manière à minimiser le risque de problèmes comme la violation de la confidentialité des données ou la perte d'informations personnelles identifiables. La microsegmentation facilite l'isolement des systèmes sujets à des exigences de conformité du reste de l'environnement, allégeant ainsi la charge des équipes de sécurité.

Segmentation Zero Trust

La microsegmentation offre une valeur immédiate aux entreprises lorsqu'elle est axée sur des cas d'usage très ciblés. Il est judicieux de commencer par les opérations les plus accessibles et les moins complexes, comme la mise sur liste bloquée, le cloisonnement des applications stratégiques, ou la segmentation de l'environnement numérique, qui apportent une valeur ajoutée rapide et relativement facile. Il est rare que les entreprises déploient une stratégie de microsegmentation complète, sur tout leur périmètre, en une seule étape. Celle-ci s'effectue généralement progressivement, dans le cadre d'une initiative Zero Trust, et de plus en plus d'entreprises adopteront une segmentation Zero Trust au fur et à mesure de l'expansion de leur microsegmentation. En fusionnant les résultats positifs et les cas d'usage explicités précédemment, la segmentation Zero Trust offre une visibilité complète et détaillée des flux de trafic. Elle assure une protection accrue des ressources les plus sensibles de l'entreprise, entrave les mouvements latéraux possibles, et permet une réactivité optimale face aux menaces, tout en renforçant les capacités globales de l'entreprise. Bien que la plupart des projets de microsegmentation ne débutent pas par cette étape, la segmentation Zero Trust doit être envisagée comme une ligne de progression idéale sur laquelle toutes les entreprises devraient se positionner à terme.

La philosophie d'Akamai en matière de microsegmentation

La solution de microsegmentation logicielle Akamai Guardicore Segmentation a été élaborée avec pour objectif d'entraver la capacité des acteurs de menaces à effectuer des mouvements latéraux dans l'environnement de l'entreprise.

Il convient de rappeler que la microsegmentation, bien qu'elle soit un élément central du concept Zero Trust, doit être complétée par d'autres composantes essentielles comme la détection des menaces, la gestion des identités et la sécurité des données, lesquelles doivent toutes être prises en charge par des technologies appropriées. Le choix des fournisseurs de technologies, et la manière dont vous interagissez avec eux, est une tâche rigoureuse et minutieuse, dont dépend directement l'accomplissement de vos objectifs en matière de cybersécurité. Ce processus, s'il est bien mené, peut vous faire économiser des ressources financières, du temps et des efforts. Par conséquent, l'inclusion d'outils de microsegmentation dotés de fonctionnalités étendues d'intégration et de partage de signaux, peut aider à hisser une stratégie Zero Trust au-delà de la simple microsegmentation, et ce, tout en réduisant la complexité opérationnelle.

Akamai, acteur de longue date du domaine des infrastructures réseau, a su faire de la microsegmentation et du concept Zero Trust, les pierres angulaires de ses solutions. Sa profonde compréhension des exigences des infrastructures de niveau entreprise pour les environnements cloud et sur site lui permet d'identifier et de relever efficacement les défis potentiels en matière de cybersécurité.

Akamai Guardicore Segmentation repose sur une approche logicielle de microsegmentation, essentielle pour contrer les mouvements latéraux des cybermenaces dans l'environnement numérique de l'entreprise. Cette solution bénéficie d'une visibilité détaillée pour instaurer les principes Zero Trust au niveau réseau, permettant ainsi aux entreprises de superviser l'activité et les mouvements au sein de leur environnement numérique, qu'il soit physique ou virtuel. Son infrastructure de segmentation par intelligence artificielle intègre des modèles préétablis pour la détection et la neutralisation de cyberattaques, notamment les ransomwares, les attaques basées sur les terminaux, et celles visant spécifiquement le personnel à distance. Pouvant être déployé sur une multitude de plateformes, notamment les serveurs sans système d'exploitation, les machines virtuelles, les conteneurs, les dispositifs IoT et les instances cloud, cet outil s'avère très polyvalent.

Akamai Guardicore Segmentation génère une collecte de données étendues sur l'infrastructure sous-jacente, en utilisant diverses méthodes comme des capteurs basés sur des agents, une collecte d'informations orientée réseau, des journaux de flux issus de clouds privés virtuels et des intégrations favorisant les fonctionnalités sans agent. Un mappage dynamique procure à vos administrateurs un aperçu complet des activités avec une granularité grossière. Forte de son expérience extensive des environnements réseau de niveau entreprise, la société Akamai a conçu Akamai Guardicore Segmentation en vue d'assurer une évolutivité sans faille pour les grandes entreprises ainsi qu'une performance constante, capable de déceler et contourner les sources potentielles de goulets d'étranglement.

En conclusion

La microsegmentation ne constitue pas une technologie récente, elle s'est peut-être même imposée avant l'heure. Cependant, son rôle prépondérant dans le renforcement de la sécurité des environnements hybrides modernes et multicloud, notamment dans le cadre d'une stratégie Zero Trust, est indéniable. La microsegmentation offre la flexibilité, l'agilité et l'efficacité nécessaires pour instaurer une solution Zero Trust pour divers cas d'usages essentiels et stratégiques. Elle garantit la protection de toutes les structures sensibles, qu'il s'agisse de l'infrastructure cruciale, de la propriété intellectuelle, ou encore des identités et références. Forte de son expérience dans les infrastructures réseau, la segmentation et la microsegmentation, la société Akamai se positionne comme un acteur majeur capable d'accompagner les entreprises dans l'élaboration, le déploiement, et même la gestion d'une infrastructure sécurisée fondée sur les outils et principes de microsegmentation.

Enterprise Strategy Group est un cabinet de conseil, d'analyse, de recherche et de stratégie en matière de technologie qui fournit des informations sur le marché, des informations exploitables et des services de contenu de mise sur le marché à la communauté informatique internationale.

www.esg-global.com contact@esg-global.com 508.482.0188