



Services à impact élevé pour la segmentation

Réduisez la complexité et les risques liés à la sécurité avec Akamai

Introduction

Protéger les ressources stratégiques hébergées dans les centres de données sur site et les environnements de cloud public est plus important que jamais. Pour y parvenir, une expertise spécialisée est de plus en plus nécessaire afin de suivre le rythme des nouveaux modèles de déploiement d'applications alors que l'écosystème des menaces évolue rapidement. L'objectif premier de nos experts en services est de transformer votre investissement dans notre portefeuille de produits de sécurité en résultats commerciaux concrets.

L'équipe des services de microsegmentation d'Akamai est composée d'experts en sécurité disposant d'une formation approfondie et d'une expérience concrète dans le secteur privé et dans les organisations de renseignement militaire. Notre ensemble flexible d'offres de services vous permet d'accéder à cette expertise spécialisée, qui fait office de prolongement de vos équipes informatiques et de sécurité internes, pour mettre en œuvre une sécurité de pointe, du centre de données au cloud.



Parcours client

Un parcours client typique commence par le déploiement et la configuration via notre prestation de services professionnels : nous configurons votre environnement, définissons les ressources et les étiquettes, et mettons en œuvre les règles pour les premiers cas d'utilisation.

Nous offrons ensuite une formation administrative et technique à certains des membres de l'équipe qui utilisent la solution.

En outre, les services d'exploitation du jour 2 peuvent être utilisés pour poursuivre et améliorer le déploiement (définir davantage de ressources et d'étiquettes, mais aussi mettre en œuvre des règles pour d'autres cas d'utilisation), gérer les incidents de sécurité et améliorer la posture de sécurité, fournir les contrôles et les rapports nécessaires pour les audits, et fournir un développement personnalisé pour améliorer l'intégration à l'infrastructure du client.

Tout au long du cycle de vie de la solution, des services d'assistance complets vous aident à résoudre tout problème qui pourrait survenir, et notre équipe Customer Success veille à ce que vous profitiez au maximum de notre produit.

Parcours client avec les services de microsegmentation d'Akamai



Prestation de services professionnels

Une équipe complète composée d'architectes de sécurité, de chefs de projet et de développeurs collabore avec votre équipe pour mettre en œuvre la plateforme Akamai Guardicore Segmentation. En fonction de vos besoins, Akamai propose soit un ensemble de livrables, soit un ingénieur de mise en œuvre à durée déterminée. Quel que soit le forfait que vous choisissiez, nos offres de services sont adaptées pour garantir la protection de vos ressources stratégiques.

Démarrage

L'offre Démarrage est conçue pour les clients qui veulent accélérer leur déploiement d'Akamai Guardicore Segmentation, mais qui préfèrent mettre en œuvre et gérer eux-mêmes les règles suivantes avec les conseils de nos experts. Que vous souhaitiez segmenter votre environnement réseau, cloisonner les applications ou restreindre l'accès aux serveurs, nos ingénieurs conçoivent et mettent en œuvre votre premier objectif de règle, vous forment tout au long du processus et vous guident lorsque vous mettez vous-même en œuvre les règles suivantes.

Notre équipe travaille également avec vous pour planifier l'architecture de sécurité et comprendre toutes les considérations liées à la conception d'applications. Cela inclut la définition et la documentation de la règle d'étiquetage, l'étiquetage de vos ressources sur la plateforme, et la création formelle et l'ajustement précis des règles pour soutenir vos cas d'utilisation.

Une fois qu'Akamai a terminé la mise en œuvre de votre première règle, nos ingénieurs continuent de fournir à votre équipe une assistance directe pour toute future mise en œuvre de règle. Ils restent intégrés à votre équipe étendue jusqu'à ce que vos objectifs de déploiement soient atteints.

Démarrage étendu

Pour les entreprises souhaitant atteindre plusieurs objectifs de segmentation, l'offre Démarrage étendu est idéale. Les experts Akamai collaborent avec vos équipes pour mettre en œuvre plusieurs règles de segmentation, renforçant ainsi la protection de vos ressources stratégiques et de vos autres ressources les plus précieuses.

Notre équipe travaille avec vous pour planifier l'architecture de sécurité et comprendre toutes les considérations liées à la conception d'applications. Cela inclut la définition et la documentation de la règle d'étiquetage, l'étiquetage de vos ressources sur la plateforme, et la création formelle et l'ajustement précis des règles pour soutenir plusieurs initiatives de sécurité.



Objectifs stratégiques types à mettre en œuvre

Que vous souhaitiez segmenter votre environnement réseau, cloisonner les applications ou restreindre l'accès aux serveurs, nos ingénieurs vous accompagnent à chaque étape du processus pour garantir la protection de vos ressources.

Dans le cadre de cette offre, vous pouvez choisir plusieurs objectifs stratégiques ou vous concentrer sur un objectif prioritaire spécifique. Nos ingénieurs mettent alors en œuvre les étiquettes et les règles requises qui forment nos règles jusqu'à ce que vos ressources soient sécurisées conformément à vos objectifs prédéfinis.

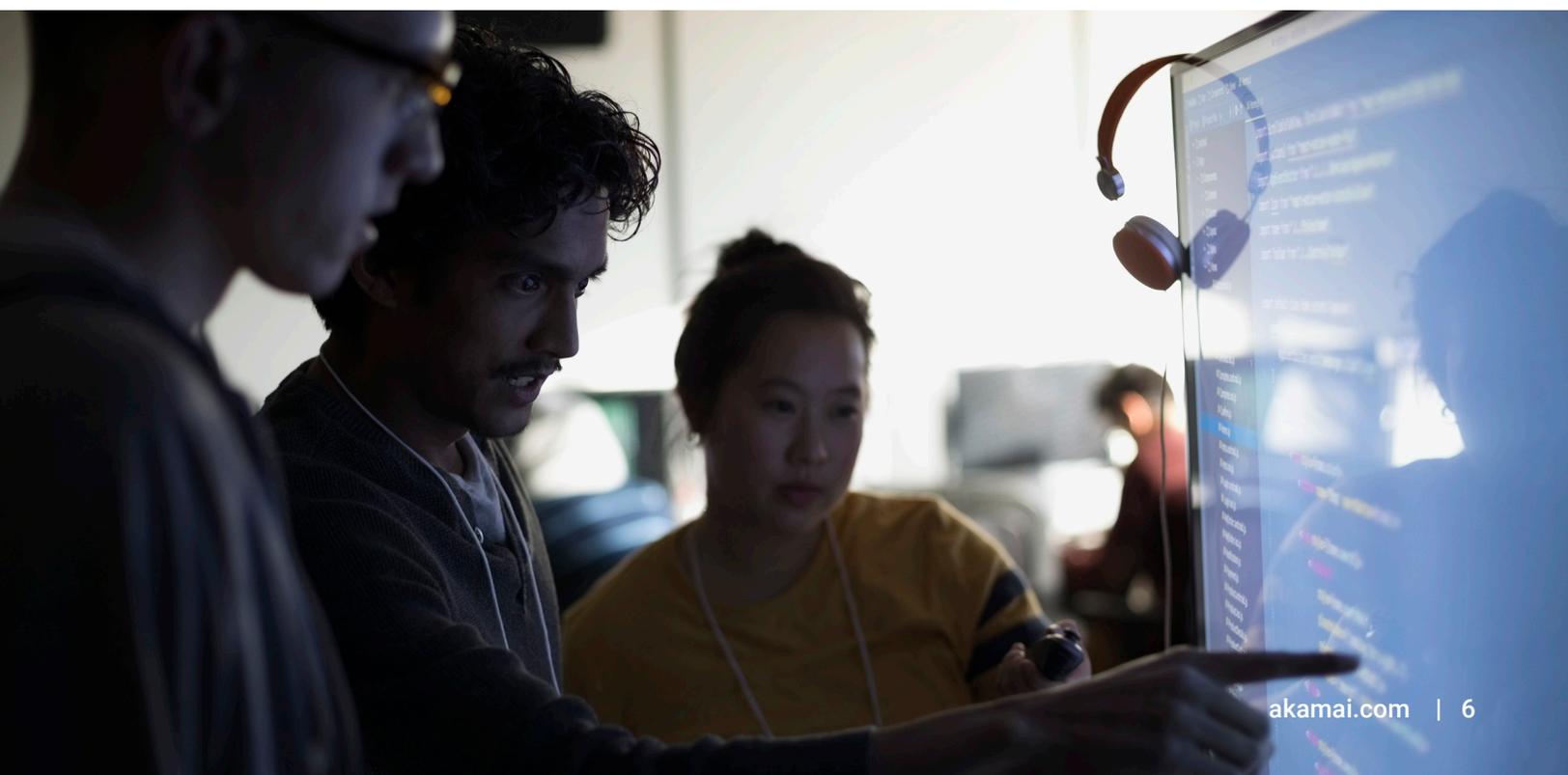
Voici quelques exemples :

- **Segmentation de l'environnement** : les serveurs provenant d'environnements différents ne seront pas autorisés à communiquer, sauf dans le cadre de communications explicitement autorisées.
- **Cloisonnement des applications** : les applications critiques ne doivent communiquer qu'avec les parties explicitement autorisées. Les communications internes des applications seront autorisées.
- **Microsegmentation des applications** : le trafic interne et externe des applications critiques ne sera autorisé que s'il est explicitement approuvé (Zero Trust).
- **Segmentation des points de terminaison « hors entreprise »** : la surface d'attaque d'un point de terminaison en dehors de la protection d'un réseau d'entreprise sera limitée. Akamai Guardicore Segmentation permet d'activer différents ensembles de règles pour le réseau d'entreprise et les réseaux externes.
- **Accès privilégié aux serveurs** : la règle de contrôle des accès au serveur peut être mise en œuvre pour restreindre les ports de gestion aux jump box uniquement, par exemple, ou pour empêcher l'accès à des serveurs spécifiques en fonction de l'identité de l'utilisateur de la source.
- **Application des meilleures pratiques de sécurité** : des règles de liste de blocage seront mises en œuvre pour appliquer les meilleures pratiques de sécurité réseau.

Ingénieur de mise en œuvre

Lorsqu'une entreprise a besoin d'un grand nombre d'objectifs stratégiques, il est souvent préférable de travailler avec un ingénieur désigné pendant une période donnée, sans limiter le nombre de règles que celui-ci peut créer afin d'assurer une mise en œuvre réussie. Permettre à Akamai de fournir l'assistance de mise en œuvre dont vous avez besoin pour atteindre vos objectifs est idéal lorsque votre réseau a besoin d'une segmentation complète de bout en bout.

	Démarrage	Démarrage étendu	Ingénieur de mise en œuvre
Installation	✓	✓	✓
Installation du schéma d'étiquetage	✓ Limité	✓ ✓ ✓	Des ressources de mise en œuvre complètes pour une période définie, sans limitation des cas d'utilisation, pour garantir que vos objectifs de réussite sont atteints.
Conseils sur la posture de sécurité globale	✓ Limité	✓ ✓ ✓	
Conseils sur la création de règles	✓ Limité	✓ ✓ ✓	
Mise en œuvre des cas d'utilisation de règle	Règle unique	Règles multiples	
Formation des utilisateurs finaux	✓	✓	✓
Durée type	6 mois	12 mois	6 à 18 mois
Quelle option pour quelle situation ?	Le client ou le partenaire préfère une mise en œuvre principalement en interne ; Akamai ne met en œuvre que le premier cas d'utilisation.	Akamai met en œuvre plusieurs cas d'utilisation et plusieurs règles, et fournit des conseils détaillés.	Le client ou le partenaire souhaite une mise en œuvre complète (plusieurs cas d'utilisation), préfère explorer et définir exactement les éléments et la manière de faire tout au long de la période.



Formation Akamai

La formation de certification à la microsegmentation d'Akamai permet aux administrateurs (GCSA) et aux ingénieurs opérationnels (GCSE) d'acquérir les compétences et les connaissances nécessaires pour assurer leurs tâches administratives et de maintenance.

Pour mieux répondre aux besoins des clients et des partenaires, les méthodes de formation sont polyvalentes, allant de la formation en ligne de base à la formation de certification animée par un instructeur, en passant par la formation privée et dédiée (virtuelle ou en personne).



Guardicore Certified Segmentation Administrator (GCSA)

Notre programme de cinq demi-journées permet aux utilisateurs d'Akamai Guardicore Segmentation d'acquérir l'expertise nécessaire pour tirer avantage de tous les aspects de la plateforme. Les administrateurs GCSA certifiés utiliseront la plateforme avec beaucoup plus de confiance pour mettre en œuvre et assurer la sécurité de leur organisation.

La formation couvre l'ensemble des fonctionnalités principales d'Akamai Guardicore Segmentation : visibilité, étiquetage, microsegmentation et détection des violations. L'accent est mis en majorité sur le comportement et l'utilisation des fonctionnalités, et les participants seront guidés de la configuration initiale d'Akamai Guardicore Segmentation jusqu'aux opérations quotidiennes courantes.



Guardicore Certified Segmentation Engineer (GCSE)

Notre programme de trois demi-journées apporte aux propriétaires opérationnels du système les compétences et connaissances nécessaires pour effectuer les tâches administratives et de maintenance liées à la plateforme.

Les ingénieurs GCSE certifiés seront en mesure de gérer l'ensemble du fonctionnement de l'environnement d'Akamai Guardicore Segmentation. La formation couvre les sujets suivants : configuration de la plateforme et des composants, intégration à des outils tiers, vérification de l'intégrité de la plateforme, dépannage et tâches de maintenance courantes.

Les deux formations s'accompagnent d'un laboratoire pratique en ligne, disponible pour tous les participants pendant toute la durée des formations. Un examen de certification a lieu à la fin de chaque formation.

Assistance aux entreprises et Customer Success

Notre programme d'assistance aux entreprises est conçu pour prendre en charge toutes les conséquences possibles de l'utilisation d'Akamai Guardicore Segmentation dans votre entreprise. Notre équipe d'assistance est à votre disposition 24 h/24, 7 j/7, 365 jours par an pour traiter tous les problèmes que vous rencontrez, mais aussi pour vous aider avec les mises à niveau et les correctifs.

Notre programme Customer Success vous aide à atteindre les objectifs de sécurité à court et à long terme de votre organisation, tout en maximisant la valeur que vous avez investie dans notre plateforme.

Assistance Elite

L'assistance Elite d'Akamai offre à votre entreprise un accès prioritaire à des experts désignés, expérimentés et de haut niveau pour résoudre les problèmes complexes. Un spécialiste hautement qualifié, familiarisé avec votre centre de données et vos processus internes, est votre point de contact unique et vous aide à accélérer la réponse et la résolution de tout problème, tout en maximisant votre investissement dans la segmentation basée sur logiciel.

	Premium	Elite
Disponibilité de l'assistance	24 h/24, 7 j/7, 365 jours par an	24 h/24, 7 j/7, 365 jours par an
Nombre illimité de cas	✓	✓
Mises à niveau et correctifs	✓	✓
Téléphone, e-mail, Slack et portail	✓	✓
Analyse des causes premières (sur demande)	Gravité 1	Gravité 1 et gravité 2
Traitement prioritaire des cas par un ingénieur dédié expérimenté		✓ Ingénieur désigné disponible pendant les heures d'ouverture
Surveillance proactive et continue de l'intégrité du système		✓
Optimisation personnalisée		✓ Session d'optimisation trimestrielle
Examen périodique des problèmes et rapport d'assistance		✓ Examen hebdomadaire des problèmes ; rapport d'assistance mensuel
Journées de consultation		✓ 2, 4 ou 6 jours de consultation par an selon la taille (SKU)
Quelle option pour quelle situation ?	Petit déploiement ; nécessite principalement une assistance	Déploiement à grande échelle ; nécessite un meilleur contrôle sur les problèmes en cours

Services d'exploitation du jour 2

Après avoir déployé les premiers cas d'utilisation, les clients tirent profit du produit Akamai Guardicore Segmentation. Cependant, il est nécessaire de procéder à une maintenance et à des mises à jour continues afin de maximiser la valeur ajoutée tirée de notre produit :

- Mise à jour du déploiement (ressources, étiquettes, règles) pour refléter les changements apportés à l'organisation au fur et à mesure qu'ils se produisent.
- Mise en œuvre des cas d'utilisation supplémentaires qui n'ont pas été traités lors de la phase initiale de déploiement (nouveaux cas d'utilisation que vous avez identifiés depuis que vous utilisez notre produit, services et/ou applications supplémentaires à gérer, etc.).
- Mise en œuvre d'Akamai Guardicore Segmentation dans d'autres services de votre entreprise, par exemple les réseaux et applications basés sur le cloud (qu'ils soient nouveaux ou qu'ils aient été prévus pour la phase 2 dès le départ).
- Déploiement sur des points de terminaison supplémentaires, des terminaux Internet des objets, des environnements d'infrastructure de postes de travail virtuels, etc.
- Utilisation d'Akamai Guardicore Segmentation pour identifier et atténuer les événements de sécurité (par exemple, arrêter les mouvements latéraux sur votre réseau). Vous pouvez connecter votre environnement à Akamai Security Operations Command Center et bénéficier d'une surveillance 24 h/24, 7 j/7, 365 jours par an, ainsi que d'alertes et d'atténuation en temps réel.
- Sécurité renforcée et proactive via Akamai Hunt, Akamai Edge DNS (pour un DNS sécurisé et une protection contre le déni de service distribué) et Akamai Enterprise Application Access (pour la gestion des accès et des identités).
- Utilisation d'Akamai Guardicore Segmentation pour vous assister dans vos audits de certification.

Ces services devraient être fournis par des partenaires GCSP certifiés.



Responsables de compte technique et ingénieurs résidents

Les responsables de compte technique et les ingénieurs résidents d'Akamai sont des conseillers techniques expérimentés pour les entreprises ayant des besoins de segmentation étendus et potentiellement complexes. Une fois intégrés à votre entreprise, nos ingénieurs deviennent rapidement des experts de votre environnement, ce qui vous permet d'obtenir des résultats encore plus positifs avec Akamai Guardicore Segmentation.

L'ingénieur résident* affecté à votre compte sera intégré à vos équipes et prendra en charge toutes vos opérations de manière proactive afin que vous puissiez tirer le meilleur parti d'Akamai Guardicore Segmentation à tout moment.

Cet ingénieur peut assurer votre réussite en vous guidant lors de la prise de décisions stratégiques, en vous informant des dernières fonctionnalités à venir de notre produit, en planifiant (et en aidant à exécuter) une mise à niveau et en effectuant des évaluations de niveau exécutif.

Votre responsable de compte technique ou votre ingénieur résident peut également superviser et exécuter vos services d'exploitation du jour 2.

**L'ingénieur résident peut travailler à distance*

Akamai Hunt : un service géré de recherche des menaces

Akamai Hunt, une extension d'Akamai Guardicore Segmentation, est un service géré de recherche des menaces qui peut vous aider à garder une longueur d'avance sur les menaces les plus fuyantes et à mieux protéger votre entreprise.

L'équipe d'Akamai Hunt recherche en permanence les comportements d'attaque anormaux et les menaces avancées qui contournent systématiquement les solutions de sécurité les plus avancées. Grâce à Hunt, vous recevez des notifications instantanées pour chaque incident critique détecté sur votre réseau. Nos experts travaillent en étroite collaboration avec votre équipe afin de corriger toute ressource compromise et d'obtenir une résolution rapide.

Que vous soyez concentré sur la détection et la prévention des ransomwares, la lutte contre les menaces persistantes avancées, la protection contre les vulnérabilités Zero Day ou l'amélioration de l'intégrité générale de votre sécurité informatique, Akamai Hunt vous permet de tirer le meilleur parti de votre déploiement Akamai Guardicore Segmentation sans aucun logiciel, déploiement d'agents ou mise à niveau supplémentaire.



Akamai Hunt comprend les avantages suivants :

Analyses 24 h/24, 7 j/7 effectuées par des experts humains : nos professionnels de la cybersécurité travaillent dans des secteurs très diversifiés, parmi lesquels la recherche sur la sécurité, la sécurité offensive, les informations militaires, la red team, la réponse aux incidents et la science des données.

Alertes pour les menaces réelles : pour éviter la lassitude liée aux alertes, l'équipe Hunt avertit uniquement ses clients des menaces réelles. Ainsi, ils n'ont plus à traiter de faux positifs.

Outils de détection propriétaires : les experts d'Akamai Hunt développent systématiquement des algorithmes avancés de détection des menaces, comme les anomalies d'activité de réseau et d'utilisateur, l'analyse des exécutables, l'analyse des journaux, etc., afin de former un ensemble d'outils puissants pour accélérer la détection et la réponse. Puissant outil basé sur l'osquery, Akamai Guardicore Insight permet d'interroger les serveurs et les points de terminaison en temps réel. Il est inclus dans le service sans coût supplémentaire.

Informations sur les menaces enrichies par le contexte : grâce à la solution Akamai Guardicore Segmentation et les informations mondiales étendues sur les menaces d'Akamai, notre équipe de chasseurs recueille de nombreuses données sur les indicateurs d'infection, des adresses IP aux domaines en passant par les processus, les utilisateurs et les services.

Visibilité sur le réseau, le cloud et les points de terminaison : notre équipe bénéficie de la visibilité la plus complète sur votre environnement grâce à cette combinaison de données générées par les déploiements de la solution Akamai Guardicore Segmentation et les capteurs mondiaux d'Akamai, qui comprennent notamment plus de sept mille milliards de requêtes DNS envoyées dans le cloud DNS d'Akamai.

Notification instantanée et informations proactives :

- Les notifications de menaces par e-mail sont envoyées immédiatement après leur détection.
- Grâce aux rapports périodiques sur les menaces de niveau exécutif qui incluent des analyses, des statistiques et des indicateurs, vos dirigeants ou votre conseil d'administration sont informés des campagnes d'attaque de grande envergure.
- Avec l'intégration de la console d'Akamai Guardicore Segmentation, la gestion des incidents devient un jeu d'enfant.

Pour en savoir plus sur Akamai Guardicore Segmentation, rendez-vous sur akamai.com



Akamai soutient et protège la vie en ligne. Les entreprises leaders du monde entier choisissent Akamai pour concevoir, diffuser et sécuriser leurs expériences digitales, et aident des milliards de personnes à vivre, travailler et jouer chaque jour. Akamai Connected Cloud, plateforme cloud massivement distribuée en bordure de l'Internet, rapproche les expériences et les applications des utilisateurs tout en éloignant les menaces. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu d'Akamai, rendez-vous sur akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur [X](#) (anciennement Twitter) et [LinkedIn](#). Publication : 09/23.