Témoignage client d'Akamai

Une entreprise américaine de soins de santé a déjoué 4 000 cyberattaques en une journée

Les ingénieurs réseau ont utilisé la visibilité de couche 7 et des stratégies intelligentes via la microsegmentation pour réduire les cyberrisques

Contrecarrer les ransomwares

Visibilité approfondie

Stratégies améliorées

Connecter les patients aux soins de santé essentiels

Imaginez que vous essayez de protéger un réseau qui a un impact direct sur la vie des patients, tout en gardant une longueur d'avance sur des cyberattaques de plus en plus sophistiquées. Telle était la réalité d'une entreprise de soins de santé de taille moyenne. Son équipe d'ingénierie réseau était confrontée à des menaces de ransomwares croissantes et à un besoin de visibilité accrue. L'équipe s'est donc tournée vers Akamai Guardicore Segmentation pour améliorer la posture de sécurité de l'entreprise.

Étendre l'architecture Zero Trust

L'entreprise avait une vision audacieuse : renforcer son environnement informatique en appliquant des principes Zero Trust tout en répondant aux exigences de conformité HIPAA et SOC 2. Les enjeux étant élevés, l'équipe d'ingénierie réseau s'est fixé les objectifs suivants :

- Maintenir les applications critiques en ligne, même en cas d'incident de sécurité
- Réduire l'impact des attaques par ransomware en limitant leur propagation
- Obtenir une visibilité détaillée du réseau bien au-delà des pare-feux traditionnels

L'entreprise avait besoin d'une solution de microsegmentation rentable et évolutive qui ne nécessitait pas le remplacement de l'infrastructure informatique existante. De plus, elle devait être suffisamment simple pour être gérée par une équipe réduite, et adaptable pour évoluer avec l'entreprise.

Comme l'explique un ingénieur réseau, « Les ransomwares ciblent le secteur de la santé. Plus vite nous parvenons à isoler et éliminer ces menaces, mieux c'est. »

Healthcare Company

Localisation géographique

États-Unis

Secteur

Santé et sciences de la vie

Solution

Akamai Guardicore Segmentation

Akamai

Trouver la bonne solution de microsegmentation

Après avoir rapidement écarté l'option d'une approche conteneurisée, l'entreprise a évalué les solutions de microsegmentation. « Nous voulions les mêmes fonctionnalités que celles des pare-feux de nouvelle génération, à savoir la visibilité au niveau de la couche applicative », explique l'ingénieur réseau.

Après avoir évalué de nombreuses solutions, l'entreprise a trouvé Akamai Guardicore Segmentation. Une démonstration positive associée à une assistance pratique de la part des ingénieurs d'Akamai a permis de conclure l'affaire. La solution répondait à toutes les attentes, notamment :

- **Visibilité approfondie :** inspection de couche 7 et informations complètes sur le réseau
- **Facilité de déploiement :** agents logiciels sans matériel supplémentaire
- **Résilience :** pas de point de défaillance unique dans le réseau central
- **Flexibilité :** prise en charge de divers systèmes d'exploitation

Selon le vice-président de l'infrastructure informatique et de la sécurité de l'information, Akamai Guardicore Segmentation offre un avantage considérable aux équipes réduites. « Dès le début du déploiement, nous avons constaté des avantages en termes de visibilité et de contrôle. »

« Nous n'avons pas besoin d'acheter et de gérer plusieurs pare-feux est-ouest, ce qui nous permet de réaliser des économies considérables et d'obtenir un niveau de visibilité impossible à atteindre avec les pare-feux », ajoute le responsable de l'infrastructure informatique.

Arrêter les ransomwares dans leur élan

Les résultats ont été immédiats et impressionnants. En améliorant le cloisonnement de ses applications et en utilisant des stratégies prêtes à l'emploi de prévention des ransomwares d'Akamai Guardicore Segmentation, l'équipe a neutralisé 4 000 cyberattaques dès le premier jour. La solution a même adapté les stratégies aux besoins spécifiques de l'entreprise.

« Pour les politiques de terrain intermédiaire, nous avons utilisé le mode alerte pour signaler les incidents sans provoquer de temps d'arrêt. C'est un excellent moyen d'affiner les stratégies sans interruption », affirme l'ingénieur réseau.

> Akamai Guardicore Segmentation nous a aidés à faire plus que répondre à nos préoccupations en matière de ransomware : il a amélioré notre approche de la cybersécurité.
>
> – Ingénieur réseau

> « L'ascension de la « montagne Zero Trust » est un vétritable défi. Akamai Guardicore Segmentation nous a permis de gravir rapidement cette montagne tout en réduisant les défis liés aux dépenses et à la complexité. »
>
> — Vice-président de l'infrastructure informatique et de la sécurité de l'information

Obtenir des informations de couche 7 inégalées

Selon le responsable de l'infrastructure informatique, Akamai Guardicore Segmentation fournit des informations précieuses sur les flux de trafic entre différentes applications. Cela a débloqué une mine de données pour l'équipe. L'équipe peut désormais inspecter des détails granulaires au-delà des journaux de couche 4 : identifiants utilisateur, entrées de ligne de commande et même corrélations de service.

« Notre équipe réseau peut examiner le flux de trafic pour résoudre les problèmes et fournir à notre équipe de sécurité les informations nécessaires pour enquêter de manière approfondie sur les incidents », note l'ingénieur réseau.

Cette visibilité s'est avérée utile en cas de violation inattendue de la politique. Un nouvel employé a connecté un PC directement à l'équipement des locaux du client (CPE) de son opérateur au lieu de le connecter à un port LAN protégé par un routeur domestique. Cela était strictement interdit, puisque l'infrastructure client a attribué au PC une adresse IP publique, ce qui le rend vulnérable aux analyses publiques d'Internet.

Comme l'explique l'ingénieur réseau de l'organisation, « Akamai Guardicore Segmentation a détecté le problème instantanément, ce qui nous a permis d'isoler le PC et de résoudre la situation avant qu'elle ne s'aggrave. En outre, cela nous a incités à créer une stratégie visant à empêcher ce type d'incident de se produire à l'avenir. »

Un étiquetage plus intelligent, de meilleures stratégies

Grâce à l'étiquetage intuitif et à la création de règles, l'équipe d'ingénierie réseau a pu facilement cartographier le trafic et appliquer les règles de sécurité. Selon l'ingénieur réseau, « nous avons pu décider de ce qui fonctionne le mieux pour notre environnement. Cette capacité nous a beaucoup plus impressionnés que ce à quoi nous nous attendions, et nous a aidés à créer des règles de manière efficace. »

Par exemple, l'équipe a limité l'accès aux serveurs d'impression, en n'autorisant que les zones de confiance, un gain rapide qui a amélioré la posture de sécurité globale de l'entreprise. « Ainsi, nous avons pu résoudre les plus grandes failles dès le départ », poursuit l'ingénieur.

Une visibilité qui inspire confiance

Un avantage inattendu ? Une vision claire du flux de trafic interne et du comportement des applications. Cette nouvelle visibilité a permis d'améliorer la collaboration avec les propriétaires d'applications et de rationaliser les fenêtres de maintenance. Par exemple, l'équipe est habilitée à montrer aux propriétaires d'applications si leur trafic est bloqué.

« Par le passé, le dépannage et la pérennisation posaient problème. Désormais, lors des transitions, nous pouvons confirmer en toute confiance le moment où le trafic passe d'un ancien serveur à un nouveau. Cela nous a permis de retirer les systèmes existants avec certitude », explique l'ingénieur réseau.

Le vice-président de l'infrastructure informatique et de la sécurité de l'information de l'organisation conclut : « Akamai Guardicore Segmentation a déjà eu un impact et est devenu un produit essentiel dans nos pratiques de sécurité. J'ai hâte d'étendre son déploiement à l'ensemble de l'organisation. »