Témoignage client d'Akamai

Un district scolaire des États-Unis a évité les menaces internes

Un grand district scolaire du Texas a déployé la microsegmentation d'Akamai pour protéger le trafic est-ouest

Applications sécurisées

Attaques internes empêchées

Vue du trafic

Un leader de l'excellence éducative

En 2022, un grand district scolaire public du Texas comptant plus de 75 000 étudiants a reçu la note « A » de la Texas Education Agency. Leader en matière d'excellence pédagogique, ce district offre des expériences d'apprentissage inégalées, conçues pour préparer et inspirer chaque étudiant à mener une vie honorable et épanouissante. Dans cette optique, le service des opérations technologiques du district s'efforce de créer et de maintenir une infrastructure de pointe pour s'adapter, en toute sécurité, aux générations actuelles et futures de contenu et d'outils numériques pour toutes les parties prenantes. Lorsque le nouveau responsable de la cybersécurité du département a identifié une faiblesse dans l'approche de sécurité du district, Akamai Guardicore Segmentation a permis de combler cette lacune.

Nécessité d'éliminer les menaces internes

Traditionnellement, ce district scolaire du Texas s'appuyait sur les pare-feux et le géorepérage pour protéger son environnement informatique contre les menaces externes. Il lui manquait toutefois un moyen de prévenir les menaces internes, provenant plus particulièrement des membres ayant des intentions malveillantes. « S'ils avaient pu accéder à un système, ils auraient pu facilement accéder à tous les autres systèmes », explique le responsable de l'ingénierie des systèmes du district.

Texas School District

Localisation géographique

Texas, États-Unis

Secteur

Secteur public

Solution

Akamai Guardicore Segmentation

Akamai

En l'absence de visibilité sur les communications légitimes entre les systèmes internes, le district scolaire n'était pas en mesure de bloquer le trafic est-ouest illégitime et malveillant. Conscient de la menace que cela représentait, le service des opérations technologiques, qui comprend l'ingénierie réseau, l'ingénierie des systèmes et la cybersécurité, a compris la nécessité d'une solution complète d'atténuation des risques. « Nous aurions été négligents si nous n'avions pas mis en place de solution pour garantir la sécurité totale des informations associées à nos étudiants et à notre personnel », poursuit le responsable.

Déploiement graduel et facile de la microsegmentation

Après avoir évalué ses options, le district scolaire a choisi la technologie Akamai Guardicore Segmentation. « C'était l'une des meilleures solutions sur le marché », assure le responsable.

Le département des opérations technologiques a audité son environnement afin d'identifier les applications et les systèmes à faire protéger par Akamai Guardicore Segmentation. « Nous avons commencé par nos applications de premier niveau, mais notre mission consistait à toutes les protéger à l'aide de la solution », poursuit le responsable.

Guidé par Akamai, le district a facilement et rapidement intégré des applications prioritaires, notamment Active Directory et SQL Server, avec des règles de segmentation précises pour éliminer les flux de données indésirables entre les systèmes. Le processus d'audit et de déploiement a favorisé la collaboration interfonctionnelle. « Il y a eu un véritable effort collectif pour déterminer comment étiqueter les appareils, procéder au cloisonnement, etc. Ainsi, Akamai Guardicore Segmentation a constitué un terrain d'entente pour collaborer étroitement ».

Dès qu'un cloisonnement était en place, le district scolaire était alerté des problèmes potentiels. « Aucun trafic ne pouvait passer à moins que nous ne l'ayons autorisé », explique le responsable de l'ingénierie système du district scolaire. Le district a ainsi eu l'assurance que la solution d'Akamai protégeait immédiatement ces applications.

« Une fois que nous avions une idée du trafic avec une application, nous passions, si nécessaire, au mode de blocage. Akamai Guardicore Segmentation fournit une feuille de route claire du déploiement progressif de la sécurité dans notre environnement », explique-t-il.

> Akamai Guardicore Segmentation offre une vue inestimable sur notre environnement et garantit la protection de nos systèmes critiques contre le trafic est-ouest non autorisé.
>
> — Responsable de l'ingénierie système, district scolaire texan

> « Nous adorons Akamai Guardicore Segmentation. C'est une solution facile à configurer et à gérer, indispensable à tout district scolaire cherchant à se protéger contre les menaces internes. »
>
> — Responsable de l'ingénierie système, district scolaire texan

Amélioration de la visibilité sur l'environnement

Bien que certaines applications ne puissent pas bénéficier du cloisonnement, le district scolaire a tout de même gagné en visibilité sur les communications entre ces applications et les autres, comme Active Directory. Tous les groupes au sein du service des opérations technologiques peuvent voir les flux de données depuis et vers les applications cloisonnées, ce qui permet d'obtenir une visibilité sur ce qui se passe au sein de tous les systèmes de l'environnement. « Akamai Guardicore Segmentation fournit une vue à jour du fonctionnement de l'infrastructure et un moyen simple d'identifier le trafic indésirable. De plus, nous pouvons facilement configurer la solution pour autoriser ou bloquer le trafic selon les besoins », explique le responsable.

Cette visibilité permet aux équipes d'ingénierie réseau, d'ingénierie système et de cybersécurité de travailler ensemble, selon les besoins, pour résoudre les problèmes au fur et à mesure qu'ils se présentent. « Lorsque nous sommes alertés d'un trafic suspect, la solution d'Akamai fournit le contexte nécessaire pour bloquer le trafic indésirable, tout en garantissant le fonctionnement de notre environnement selon les besoins », explique le responsable.

Empêchement des accès à distance non autorisés

Selon le responsable de l'ingénierie système du district scolaire, Akamai Guardicore Segmentation contribue en permanence à lutter contre les cyberattaques : « Des adresses IP malveillantes frappent régulièrement nos systèmes. La solution d'Akamai offre une vue d'ensemble sur les activités inhabituelles, telles que celles des ports sur un serveur Web, ce qui nous permet de bloquer les accès et les attaques potentielles. »

De plus, en travaillant en toute transparence avec d'autres outils de sécurité, Akamai Guardicore Segmentation renforce la posture de sécurité du district. Par exemple, le district scolaire utilise une solution de gestion des accès privilégiés (PAM) pour fournir aux fournisseurs externes l'accès dont ils ont besoin à certains systèmes. Plutôt que d'autoriser l'accès RDP (Remote Desktop Protocol) à ces serveurs, le district exige que son service d'ingénierie utilise la solution PAM pour gérer les serveurs à distance. De plus, Akamai Guardicore Segmentation contribue à empêcher cet accès RDP.

Comme l'a expliqué le responsable de l'ingénierie système du district scolaire, cette mesure de sécurité combinée empêche les équipes d'accéder à distance aux serveurs, comme cela était possible auparavant : « En utilisant la solution Akamai pour bloquer l'accès RDP, nous pouvons nous assurer que personne ne se connecte à distance à notre environnement de serveurs. »

Déploiement des applications en toute confiance

À ce jour, le district scolaire a mis en œuvre Akamai Guardicore Segmentation sur 375 de ses 500 serveurs existants, et il prévoit de protéger toutes les applications possibles avec la solution de microsegmentation. « Nous déployons constamment de nouvelles applications, parfois une par semaine, et dès le départ, nous les sécurisons avec la solution d'Akamai. Cela nous donne plus de confiance dans le déploiement de nouvelles applications, car Akamai Guardicore Segmentation nous permet de visualiser la façon dont nos applications fonctionnent et communiquent », conclut le responsable de l'ingénierie système du district.

| Publication 11/24