TÉMOIGNAGE CLIENT AKAMAI

Une société de fabrication cotée en bourse normalise ses contrôles de sécurité et gagne du temps avec Akamai Guardicore Segmentation

La société de fabrication avait besoin d'une solution mondiale sécurisée

Visibilité complète du réseau

Segmentation des infrastructures informatiques

Réponse aux menaces de ransomware

Le client

Cette société de fabrication de premier plan est cotée à la Bourse de New York et dessert les marchés du monde entier.

L'enjeu

Protection d'une entreprise mondiale

Le groupe de sécurité informatique est responsable de plusieurs sites dans le monde, dont la plupart sont des sites de production et des bureaux à usage mixte. Pour assurer une sécurité renforcée, l'équipe avait pour mission de normaliser les contrôles de sécurité dans l'ensemble de l'entreprise et de fournir une protection cohérente entre les différentes zones géographiques.

« Nous voulions passer d'un réseau ouvert et plat à une architecture segmentée basée sur des meilleures pratiques », explique l'architecte d'infrastructure à la tête du projet de segmentation.

Comme bon nombre avant elle, cette entreprise de fabrication s'est d'abord tournée vers des pare-feu pour ce projet.

Cependant, la gestion d'une multitude de règles basées sur l'infrastructure et de modifications et mises à niveau à l'échelle des postes de travail sur l'ensemble du réseau est rapidement devenue chronophage, même sur un seul site. En outre, bien que la visibilité ait été améliorée, elle restait limitée à des zones spécifiques, ce qui ne permettait pas d'obtenir facilement une vision complète et centralisée de l'activité du réseau et des dépendances entre les ressources.

Bloquer les mouvements latéraux non autorisés

Les pare-feu offraient des contrôles de segmentation approximatifs, mais ne permettaient pas de répondre à une autre préoccupation majeure de l'équipe de sécurité : les communications P2P non gérées. Il était donc essentiel d'étendre la protection et la visibilité à ce domaine spécifique. Ne pas s'atteler à ce problème risquait de rendre l'entreprise vulnérable aux attaques de type « pass-the-hash », aux ransomwares et aux autres menaces recourant à des mouvements latéraux entre les points de terminaison pour se propager.

Manufacturing Company

Localisation
États-Unis

Secteur
Fabrication

Solution
Akamai Guardicore Segmentation

Impacts majeurs

- Empêche les logiciels malveillants de se propager via des mouvements latéraux
- Offre une visibilité granulaire
- Sécurise les points de terminaison à l'aide de la segmentation
- Facilite la réponse aux incidents

Akamai

Choix d'une solution

Après plusieurs déploiements de contrôle de pare-feu complexes, l'équipe a appris l'existence d'Akamai Guardicore Segmentation et a entamé des discussions internes sur les avantages et les possibilités de la segmentation nouvelle génération.

Des recherches approfondies doivent être effectuées pour toutes les nouvelles solutions mises en œuvre par l'entreprise, de sorte que l'équipe a également évalué plusieurs alternatives. Après un processus de vérification minutieux, l'équipe a finalement adopté Akamai Guardicore Segmentation. « Aucun autre fournisseur ne nous a proposé une solution aussi complète que celle d'[Akamai], avec une surveillance du trafic, un étiquetage flexible et une riche visibilité au niveau des applications à travers l'empreinte d'un seul agent sur un client », explique l'architecte d'infrastructure.

Akamai Guardicore Segmentation

Pour la première phase du projet, la société a déployé Akamai Guardicore Segmentation sur environ 2 000 postes de travail. L'équipe de sécurité informatique a immédiatement découvert un nouveau niveau de visibilité sur le réseau et ses flux de communication une fois la solution mise en place.

Nouvelle visibilité et segmentation en action

« Les cartes de trafic [d'Akamai] ont prodigieusement amélioré notre visibilité, y compris sur les communications entre les ordinateurs individuels », raconte l'architecte d'infrastructure.

La possibilité d'affiner la visibilité jusqu'au niveau des activités des ordinateurs individuels tout en ayant une compréhension des activités globales au niveau des applications a aidé l'entreprise à prendre des décisions de sécurité plus éclairées. Par exemple, certains utilisateurs avaient installé des applications pour leur imprimante domestique sur leur ordinateur portable professionnel. Il a été découvert que bon nombre de ces applications balayaient en permanence le réseau de l'entreprise pour détecter les terminaux pris en charge. Sur la base de ces nouvelles informations issues de la visibilité d'Akamai, l'équipe a pu arrêter les analyses.

Akamai Hunt : exploitation d'Akamai Guardicore Segmentation pour la détection des menaces

Cette nouvelle compréhension de l'activité du réseau a également aidé l'entreprise à arrêter les acteurs de menaces externes. Par exemple, peu après le déploiement de la plateforme, le service Akamai Hunt a détecté une ressource en communication avec un fichier présentant les caractéristiques d'un programme malveillant connu appelé GoldenSpy. Le service Hunt a informé l'équipe de sécurité informatique de l'entreprise de la menace détectée. Le client a également reçu une analyse de l'étendue de l'infection, des informations sur les risques potentiels (en faisant correspondre les résultats avec les informations de MITRE sur GoldenSpy), une analyse post-attaque (en tirant parti d'Insight) et des recommandations pour les enquêtes internes et les mesures d'atténuation. La société a ensuite utilisé les contrôles de règle d'Akamai pour mettre en quarantaine le système infecté et empêcher le programme malveillant de se déplacer latéralement vers de nouvelles machines.

Normaliser et gagner du temps

Cette entreprise peut désormais également créer et gérer des règles de manière centralisée, y compris une règle de poste de travail mondiale centralisée, et bénéficie de la flexibilité de définir des exceptions uniques lorsqu'un cas d'utilisation l'exige. Cela garantit une application cohérente partout où il existe un agent Akamai, et réduit le risque d'erreurs et de retards de configuration.

En outre, le délai de mise en œuvre des politiques s'est également considérablement amélioré au sein de l'entreprise. Par exemple, la modification des contrôles de pare-feu avant la nouvelle plateforme était un processus qui pouvait prendre des jours. En utilisant les nouveaux modèles de règle d'Akamai comme guide initial, l'équipe de sécurité informatique peut créer des contrôles de sécurité même pour les cas d'utilisation les plus complexes en moins d'une heure, et les appliquer à l'ensemble de la base installée en quelques secondes.

> Avec un seul agent sur une machine, nous avons résolu pour de bon le problème d'une attaque sur un point de terminaison par mouvement latéral.
>
> Architecte d'infrastructure, société de fabrication

L'avenir avec Akamai

Alors que l'objectif initial du projet consistait à normaliser les contrôles de sécurité pour l'accès et la segmentation des points de terminaison, il est prévu de traiter d'autres cas d'utilisation avec Akamai. Les parties prenantes discutent d'une extension de la protection pour inclure les serveurs et les applications critiques, comme le système ERP de l'organisation.

Quels que soient les plans pour demain, le projet d'origine est déjà considéré comme un succès chez la société de fabrication et a considérablement réduit la surface d'attaque et les risques pour les postes de travail de l'entreprise. L'équipe est désormais beaucoup plus confiante dans la sécurité de l'entreprise face aux attaques qui se déplacent latéralement d'un point de terminaison à l'autre. Comme l'a expliqué le chef de projet : « Dorénavant avec un seul agent sur une machine, nous avons résolu ce problème pour de bon et pouvons passer d'un poste de travail sans règle à la mise en œuvre totale des contrôles de sécurité en 30 secondes. »

Pour plus d'informations, consultez le site akamai.com/guardicore.

> Les cartes de trafic [d'Akamai] ont prodigieusement amélioré notre visibilité, y compris sur les communications entre les ordinateurs individuels.
>
> Architecte d'infrastructure, société de fabrication

©2023 Akamai Technologies | Assistance | Publication : 06/23