Témoignage de client d'Akamai

Protection des clients avec Akamai API Security

Un leader de la sécurité assure la conformité de milliers de clients et la sécurité de dizaines de milliers d'API

Netskope est un leader mondial de la cybersécurité qui redéfinit la sécurité du cloud, des données et des réseaux. Des milliers de clients, dont plus de 25 des entreprises du classement Fortune 100, font confiance à Netskope pour répondre aux menaces en constante évolution, faciliter les changements technologiques et les aider à respecter les réglementations.

Parmi les nombreux domaines technologiques stratégiques qu'elle protège, Netskope est responsable de la sécurisation de dizaines de milliers d'API dans le monde entier – un exploit que l'entreprise ne pouvait réaliser qu'en adoptant une nouvelle approche qui aille au-delà de la sécurité traditionnelle des applications. Après avoir découvert des lacunes dans la posture de sécurité des API de l'un de ses clients, Netskope s'est tourné vers Noname Security (désormais une entreprise Akamai) pour obtenir les outils de nouvelle génération nécessaires à la protection de ses clients contre les attaques d'API malveillantes.

Voir au-delà du pare-feu

Que les clients déploient des applications de petite taille ou de grande taille avec une myriade de microservices, la réalité est qu'ils utilisent tous des API, qui font toutes partie de la surface d'attaque. Par exemple, Netskope a découvert qu'il existait des abus au sein du parc d'API d'un client, qui n'avaient pas été détectées et que Netskope ne pouvait pas voir. C'est pour cette raison que l'équipe AppSec de Netskope a commencé à rechercher une solution qui sécuriserait aussi bien ses propres API que celles de ses clients, ainsi que d'autres actifs digitaux publics.

Netskope savait qu'il ne s'agissait pas d'un problème traditionnel – ce qui l'empêcherait d'utiliser des solutions héritées telles qu'un pare-feu d'application Web ou de mener des tests de sécurité des applications conventionnels. Le volume de journaux, les types d'attaques observés et les types d'abus d'API nécessitaient une approche différente.

netskope

Localisation

Santa Clara, Californie
netskope.com

Secteur

Hautes technologies

Solution

Akamai API Security

Impacts majeurs

- Sécurisation complète du cycle de vie des API
- Blocage des attaques d'API en temps réel
- Création automatique de spécifications d'API

Akamai

James Robinson, RSSI adjoint de Netskope, a également compris que pour avoir une visibilité totale du parc d'API au niveau de l'entreprise, son équipe devait tirer parti de l'apprentissage automatique et des outils avancés. Mais pour intégrer un nouvel outil, l'équipe de sécurité était bien consciente qu'elle aurait besoin de l'assistance de développeurs.

Une victoire pour l'équipe de sécurité

Netskope a décidé d'utiliser la plateforme Noname de sécurité des API (désormais intégrée à Akamai API Security) pour protéger ses API en pré-production et en production. Pour sécuriser les API en production, elle a utilisé le module Discovery d'Akamai API Security afin d'obtenir un inventaire précis des API internes, externes et tierces de ses clients, et pour classer les données sensibles qui avaient transité sur ces API. Une fois en possession de cet inventaire précis, elle a utilisé le module Runtime Protection pour détecter les anomalies et bloquer les attaques d'API en temps réel.

Pour la pré-production, Netskope a utilisé la solution de test de la sécurité des API d'Akamai, qui aide les entreprises à tester les API en vue de détecter les vulnérabilités et les erreurs de configuration avant leur déploiement. Cette solution est capable d'exécuter automatiquement plus de 100 tests dynamiques qui simulent le trafic malveillant, ce qui aide les développeurs d'une entreprise à sécuriser leur code tout en garantissant la sécurité de l'API qu'ils sont sur le point de publier pour les clients.

Pendant la phase d'évaluation, les développeurs ont immédiatement identifié les fonctionnalités qui leur faciliteraient la vie. Ils se sont rendu compte qu'Akamai pouvait être utile lorsque le développeur ne disposait pas d'une spécification d'API en raison de son ancienneté, car ils étaient désormais en mesure d'en créer une rapidement. Ils n'ont pas besoin d'examiner le code pour comprendre l'API, car la spécification est créée automatiquement pour eux. Il en va de même pour les journaux et les transactions. Les développeurs peuvent effectuer des requêtes dans différents systèmes et consulter les lignes de journal.

Sans surprise, la plateforme a également été une réussite pour l'équipe de sécurité, qui a non seulement commencé à détecter les attaques traditionnelles, mais a également découvert des menaces plus sophistiquées.

> “Lorsque nous avons commencé à examiner la solution en interne, nous nous sommes rendu compte que nous avions absolument besoin de la collaboration des développeurs. Il est impossible de pénétrer dans leurs systèmes critiques — le cœur de leurs applications — sans leur assistance.
>
> – **James Robinson**
> **RSSI adjoint, Netskope**

Regard vers l'avenir : assurer la conformité des clients

À l'avenir, Netskope prévoit d'utiliser Akamai pour gérer la gouvernance des API, en veillant à ce que ses clients et elle-même restent conformes aux lois et obligations en matière de confidentialité des données, de plus en plus nombreuses à l'échelle mondiale. L'entreprise de sécurité prévoit également de continuer à explorer différents cas d'utilisation, car Akamai API Security a été déployé dans le cloud et sur site. Le déploiement sur site a changé la donne pour elle et pour ses clients du secteur public et d'autres secteurs fortement réglementés.

> Non seulement Noname a tenu sa promesse, mais en plus de cela, elle a rendu possible un déploiement plus efficace et plus rapide, ce qui nous a permis de nous lancer plus rapidement sur le marché.
>
> – **James Robinson**
> **RSSI adjoint, Netskope**

Les entreprises adoptent rapidement une architecture SASE (Secure Access Service Edge) pour protéger les données où qu'elles se trouvent, soutenir les efforts de transformation digitale et améliorer l'efficacité et le retour sur investissement (ROI) de leur technologie. Netskope est une société experte et innovatrice largement reconnue dans les domaines CASB, SWG, ZTNA, FWaaS et d'autres composants de service de sécurité en bordure de l'Internet (SSE), qui décrit les services de sécurité nécessaires à une architecture SASE réussie.

Malgré la popularité du SASE, il existe des ensembles de produits fragmentés, souvent accompagnés de messages prêtant à confusion, qui se font appeler « SASE » et sont souvent accompagnés de messages. La plupart de ces produits ne sont ni intégrés de manière native ni capables de simplifier les environnements technologiques, et ne disposent pas des capacités cruciales de transformation du réseau et de l'infrastructure, ce qui entraîne des risques plus élevés d'incidents de sécurité, d'interruptions de réseau et de faible retour sur investissement.

Pour relever ces défis, Netskope Borderless SD-WAN a été associé à Netskope Intelligent SSE dans une plateforme SASE unique et entièrement convergée.

| Publication 09/24