Historia de cliente de Akamai

# Protección de los clientes con Akamai API Security

Una empresa líder en seguridad ayuda a miles de clientes a cumplir la normativa y garantizar la seguridad de decenas de miles de API

Netskope es un líder mundial en ciberseguridad que está redefiniendo la seguridad de la nube, los datos y la red. Miles de clientes, incluidas más de 25 empresas de la lista Fortune 100, confían en Netskope para hacer frente a las amenazas emergentes, facilitar los procesos de transición tecnológica y cumplir la normativa.

En Netskope garantizan la protección de numerosas áreas tecnológicas fundamentales, entre ellas decenas de miles de API en todo el mundo. Por eso, la empresa decidió que era necesario adoptar un nuevo enfoque que fuera más allá de la seguridad tradicional de las aplicaciones. Tras detectar ciertas brechas en la estrategia de seguridad de API de uno de sus clientes, Netskope recurrió a Noname Security (ahora una empresa de Akamai) para adquirir las herramientas de nueva generación necesarias para protegerlos de ataques maliciosos a sus API.

## Los firewalls no son suficiente

Los clientes utilizan API para implementar todas las aplicaciones, indistintamente de si son pequeñas o de si cuentan con una infinidad de microservicios, lo que implica que cada una de esas API expuestas forma parte de la superficie de ataque. Veámoslo en contexto. Netskope descubrió que se estaba explotando el entorno de API de un cliente, pero, hasta ese momento, estos abusos habían pasado completamente desapercibidos. Por ese motivo, su equipo de seguridad de las aplicaciones comenzó a buscar una solución para garantizar la protección de sus propias API y las de sus clientes, así como de otros recursos digitales públicos.

En Netskope sabían que no se enfrentaban a un problema convencional, por lo que no podían utilizar soluciones tradicionales como un firewall de aplicaciones web (WAF) o realizar las pruebas de seguridad de aplicaciones habituales. Dado el volumen de registros y los tipos de ataque y de explotación de las API, era necesario adoptar un enfoque diferente.

netskope

**Ubicación**

Santa Clara, California
netskope.com

**Sector**

Alta tecnología

**Solución**

Akamai API Security

**Resultados clave**

- Ciclo de vida de las API totalmente protegido
- Ataques a las API mitigados en tiempo real
- Especificaciones de API creadas automáticamente

Akamai

James Robinson, subdirector de seguridad de la información de Netskope, llegó a la conclusión de que, al intentar crecer como empresa, su equipo necesitaría recurrir al aprendizaje automático (ML) y a herramientas avanzadas para obtener una visibilidad completa de su entorno de API. Por otro lado, el equipo de seguridad era consciente de que necesitaría la ayuda de los desarrolladores para incorporar una nueva herramienta.

## Un triunfo para el equipo de seguridad

Netskope decidió utilizar la plataforma de seguridad de API de Noname (ahora parte de Akamai API Security) para proteger sus API tanto en la fase previa a la producción como durante la producción propiamente dicha. Con el fin de proteger las API en fase de producción, utilizaron el módulo de detección de Akamai API Security para conseguir un inventario preciso de las API de sus clientes, tanto internas como externas y de terceros, y clasificaron los datos confidenciales que contenían. Una vez creado el inventario, usaron el módulo de protección del tiempo de ejecución para detectar anomalías y bloquear los ataques a las API en tiempo real.

En la fase previa a la producción, recurrieron a la utilísima solución de Akamai para pruebas de seguridad de API, capaz de detectar vulnerabilidades y errores de configuración antes de implementar nada. Con ella, las empresas pueden ejecutar automáticamente más de 100 pruebas dinámicas que simulan tráfico malicioso para así proteger su código y las API que están a punto de publicarse.

Al evaluarlo todo, los desarrolladores detectaron al instante las funciones que necesitaban y tuvieron claro que Akamai podría ayudarles cuando les faltara una especificación de API antigua, ya que con la herramienta se puede desarrollar rápidamente. Además, ya no tendrían que consultar el código para entenderla, porque la especificación se crea automáticamente. Lo mismo ocurre con los registros y las transacciones. Los desarrolladores podrían realizar consultas en diferentes sistemas y analizar las líneas de registro.

Con tantas ventajas, no es de extrañar que la plataforma fuese todo un éxito para el equipo de seguridad también. El equipo no solo empezó a detectar ataques convencionales, sino que también identificó amenazas más sofisticadas.

> “Nos dimos cuenta de que necesitábamos trabajar con los desarrolladores cuando empezamos a examinar la solución. Sin su ayuda, no podríamos haber accedido a sus sistemas críticos que, básicamente, son el núcleo de las aplicaciones.
>
> – **James Robinson**
> Subdirector de seguridad de la información de Netskope

## Una mirada hacia el futuro: cumplimiento garantizado

En lo que respecta al futuro, en Netskope planean seguir utilizando Akamai para controlar las API. De esta forma, se aseguran de que tanto ellos como sus clientes sigan cumpliendo las leyes y normativas globales en materia de privacidad de datos. También tienen previsto seguir explorando diferentes casos de uso, ya que Akamai API Security se ha implementado tanto en la nube como en entornos locales. La implementación en entornos locales ha supuesto un cambio radical para ellos y sus clientes del sector público, así como de otros sectores altamente regulados.

> Noname fue la empresa elegida. Eso nos ha permitido mejorar y acelerar nuestros procesos para comercializar nuestros productos más rápido.
>
> – **James Robinson**
> **Subdirector de seguridad de la información de Netskope**

Las empresas están adoptando rápidamente una arquitectura de acceso seguro a los servicios en el Edge (SASE) para proteger los datos independientemente de donde se encuentren, facilitar los procesos de transformación digital y mejorar la eficiencia y el retorno de la inversión (ROI) de su tecnología. Netskope es una empresa innovadora y ampliamente reconocida experta en CASB, SWG, ZTNA, firewall como servicio y otros componentes del perímetro de servicio de seguridad (SSE) que describe los servicios de seguridad necesarios para contar con una buena arquitectura SASE.

A pesar de la popularidad de dicha arquitectura, los proveedores a menudo utilizan mensajes confusos para acompañar grupos fragmentados de productos que se comercializan cuestionablemente bajo la etiqueta "SASE". La mayoría de estos productos no están integrados de forma nativa ni son capaces de simplificar los entornos tecnológicos. Además, carecen de las funciones esenciales para transformar la red y la infraestructura, lo que supone un mayor riesgo de incidentes de seguridad, tiempo de inactividad de la red y un ROI bajo.

Los servicios no delimitados SD-WAN de Netskope, combinados con sus servicios SSE inteligentes en una plataforma SASE totalmente convergente, hacen frente a estos desafíos.


| Publicado en septiembre de 2024