INFORME SOBRE LA SOLUCIÓN DE AKAMAI

API Security para el sector sanitario

Descubra cómo ayuda Akamai API Security a los proveedores de atención sanitaria a identificar las amenazas que se dirigen a las API y defenderse de manera eficaz.

Gracias a las API, estos proveedores pueden ofrecer una mejor y más rápida atención al paciente, pues permiten un intercambio de datos sencillo entre los diferentes sistemas, dispositivos y personas. Sin embargo, estos datos suelen ser sensibles (puede tratarse tanto de registros de pacientes como de pólizas de seguros), lo que convierte a las API en un objetivo de gran valor para los atacantes.

¿Están sus API a salvo? Tenga en cuenta las siguientes conclusiones sacadas del Estudio sobre el impacto de la seguridad de API de 2024:

- Casi el 85 % de las organizaciones sanitarias experimentaron incidentes de seguridad de API en 2024, frente al 79 % de 2023.
- Tan solo el 24 % de las organizaciones con inventarios de API completos conocen cuáles transfieren datos sensibles, en comparación con el 40 % de 2023.

Por otro lado, los responsables de TI y seguridad de varios sectores aseguran que están gastando más de 943 000 dólares en promedio para solucionar los incidentes de seguridad de API y recuperarse de sus consecuencias.

Las API facilitan el intercambio fluido de datos entre sistemas, lo que ofrece a las instituciones sanitarias una mayor interoperabilidad y eficiencia. Sin embargo, las API también amplían la superficie de ataque y el riesgo aumenta a medida que se integran en las aplicaciones, entornos en la nube y modelos de IA. Las instituciones sanitarias están implementando sin darse cuenta API mal configuradas, cuya calidad no se ha comprobado, y creadas sin controles de acceso, lo que facilita que los atacantes roben los datos e interrumpan las actividades.

Akamai API Security ayuda a los proveedores a identificar cuántas API tienen y qué tipos de datos circulan por ellas, y les proporciona los medios necesarios para proteger estos datos en todo momento. Por desgracia, muchos profesionales sanitarios creen que la protección de API forma parte de la seguridad de las aplicaciones tradicionales. Por este motivo, es necesario que el personal de AppSec y DevOps piense individualmente en las implicaciones de seguridad que tienen las API para ellos. Las API son una tecnología básica que permite la asistencia sanitaria moderna y presentan riesgos novedosos para los que las herramientas heredadas no están preparadas.

Para implementar un programa de protección y control de las API robusto, las organizaciones deben trabajar con el proveedor de seguridad de API adecuado. En el sector sanitario, los flujos de datos no supervisados plantean riesgos importantes, y aun así, muchas organizaciones siguen sin contar con un inventario completo de sus API. Akamai API Security proporciona a las instituciones una visibilidad completa de su entorno de API porque analiza todas las API activas y los tipos de datos que gestionan. Nuestra solución ofrece una protección continua con gestión de recursos, análisis de datos sensibles, detección de anomalías, pruebas de seguridad de API, integración e implementación continuas (CI/CD), y corrección manual y automatizada. Además, se integra a la perfección en flujos de trabajo de terceros.

Desafíos

Las API amplían la superficie de ataque

Casi el 85 % de las organizaciones sanitarias experimentaron incidentes de seguridad de API en 2024

Cómo gestiona Akamai API Security las amenazas de API

La solución de Akamai se ha diseñado específicamente para ayudar a las instituciones sanitarias a proteger las infraestructuras de API.

Detección completa de las API

Identifique y haga un inventario de las API de su entorno, incluidas RESTful, GraphQL, SOAP, XML-RPC y gRPC. Detecte las API no gestionadas u obsoletas que no estén cubiertas por las puertas de enlace de API y tenga control total sobre los atributos y metadatos.

Entienda cómo se comportan las API y detecte las amenazas

Aproveche el análisis realizado por la IA para identificar automáticamente posibles riesgos de seguridad, como filtraciones de datos, accesos no autorizados, configuraciones erróneas o actividades sospechosas. Vaya un paso por delante de las posibles amenazas gracias a la supervisión continua y la detección de anomalías.

Proteja las API y corrija las brechas de seguridad

Bloquee los ataques en tiempo real, corrija los errores de configuración de la seguridad y actualice automáticamente las reglas del firewall para detener el tráfico malicioso. Integre perfectamente la solución en los ecosistemas de seguridad existentes, como WAF, sistemas de seguimiento de incidencias, y plataformas de gestión de información y eventos de seguridad (SIEM), para mejorar su capacidad de respuesta.

Pruebe las API proactivamente antes de implementarlas

Asegúrese de que las API se prueban de principio a fin como parte del ciclo de vida de desarrollo, para así detectar fallos en la lógica empresarial, configuraciones erróneas y otras vulnerabilidades antes de que lleguen a la fase de producción. Mediante una integración temprana de las pruebas de seguridad, las organizaciones pueden prever riesgos y fortalecer sus defensas de API.

Akamai API Security

Desde detección de API y análisis de riesgos hasta pruebas y conformidad de API

Para más información, visite nuestra página de API Security o póngase en contacto con el equipo de ventas de Akamai.