INFORMACIÓN SOBRE EL PRODUCTO DE AKAMAI

API Security

Akamai API Security es la manera inteligente de proteger sus API frente al uso indebido de la lógica empresarial y al robo de datos.

Las amenazas a las API están evolucionando

Si bien las API hacen que su empresa avance cada día al conectarla con partners, proveedores y clientes, también amplían la superficie de ataque, y los atacantes son conscientes de ello. Los ataques a las API crecen y evolucionan rápidamente, tanto que, a veces, su protección de aplicaciones web y API no los detectan. El hecho de que su equipo no disponga de un inventario completo de las API dará lugar a un punto ciego y las API de su empresa no estarán protegidas.

Motivos para elegir Akamai API Security

Nuestra plataforma protege las API durante todo su ciclo de vida, desde el desarrollo hasta la producción. API Security, que se ha diseñado para organizaciones que muestran las API a partners, proveedores y usuarios, detecta sus API, conoce sus estrategias de riesgo, analiza sus comportamientos y evita que las amenazas se oculten dentro.

Principales prestaciones de API Security

Detección

Es habitual tener API que nadie conoce. Sin embargo, sin un inventario preciso, su empresa se expone a muchos riesgos de seguridad. Olvídese de las conjeturas y déjenos ayudarle a:

- Localizar y realizar inventario de todas sus API independientemente de la configuración o el tipo, incluidas RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC y gRPC.
- Detectar las API inactivas, heredadas y zombis.
- Identificar dominios ocultos olvidados, descuidados o desconocidos.
- Eliminar los puntos ciegos y descubrir posibles rutas de ataque.

Pruebas

El desarrollo de aplicaciones ha adquirido un ritmo vertiginoso, por lo que es más fácil que una vulnerabilidad de seguridad o un defecto de diseño pasen desapercibidos. Aproveche nuestro paquete de pruebas de seguridad de API para:

- Realizar automáticamente más de 150 pruebas que simulan tráfico malicioso, incluidos los 10 principales riesgos de seguridad de API OWASP.
- Descubrir las vulnerabilidades antes de poner las API en funcionamiento para reducir el riesgo de que se produzca un ataque.
- Analizar las especificaciones de sus API con respecto a las políticas y normativas de control establecidas.
- Realizar pruebas de seguridad bajo demanda dirigidas a las API o como parte de un proceso de integración e implementación continuas (CI/CD).

VENTAJAS PARA SU EMPRESA

Descubrimiento
Conocer la superficie de ataque de sus API. Reducir los costes de los inventarios de API y las actualizaciones de documentación. Mejorar el cumplimiento de los requisitos normativos y las políticas internas.

Pruebas
Reducir los costes de reparación al detectar los problemas con antelación. Mejorar la calidad del código sin que esto afecte a la velocidad. Aumentar los ingresos al acelerar la comercialización.

Detección
Conocer el contexto empresarial al saber lo que ha ocurrido exactamente. Deducir por qué es un problema y descubrir su impacto potencial. Determinar la forma de solucionar el problema.

Respuesta
Mitigar el riesgo al detener los ataques de inmediato. Reducir los costes al solucionar las vulnerabilidades antes de que se produzcan los ataques. Reducir la pérdida de ingresos por el tiempo de inactividad.

Akamai

Detección

Hasta los más simples errores de configuración de las API pueden dejar desprotegida a su empresa frente a los ciberdelincuentes. Una vez dentro, los hackers accederán y exfiltrarán rápidamente sus datos confidenciales. Utilice nuestra plataforma para:

- Analizar automáticamente la infraestructura para detectar errores de configuración y riesgos ocultos.
- Crear flujos de trabajo personalizados para informar acerca de las vulnerabilidades a las principales personas afectadas.
- Identificar qué API y usuarios internos pueden acceder a los datos confidenciales.
- Clasificar los problemas detectados en función de la gravedad para priorizar la reparación de los más críticos.

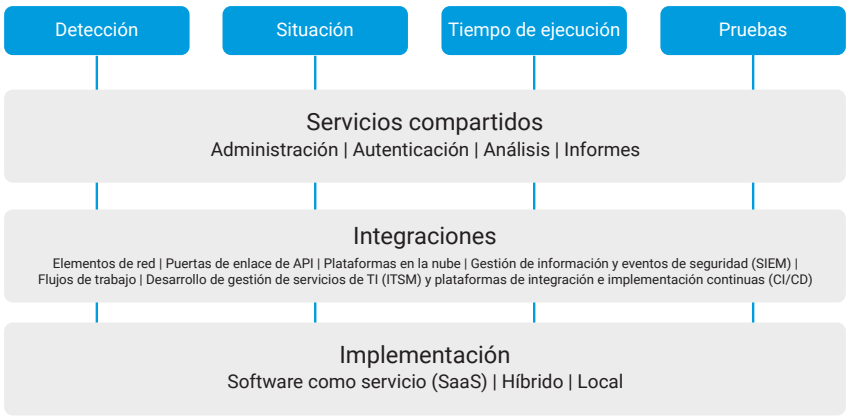
Respuesta

Ya no se trata de si su empresa sufrirá ataques, sino de cuándo, por eso es fundamental que pueda detectarlos y detenerlos en tiempo real. Utilice nuestro sistema de detección de anomalías con inteligencia artificial/aprendizaje automático para:

- Supervisar la manipulación y filtración de datos, las infracciones de políticas, el comportamiento sospechoso y los ataques a las API.
- Analizar el tráfico de las API sin necesidad de realizar cambios adicionales en la red ni implementar agentes difíciles de instalar.
- Integrar los flujos de trabajo existentes (incidencias, gestión de información y eventos de seguridad [SIEM], etc.) para alertar a los equipos de seguridad y operaciones.
- Evitar los ataques y el uso indebido de los datos en tiempo real con el proceso de reparación parcial o completamente automatizado.

Akamai marca la diferencia: Bloquea en el Edge

App & API Protector detecta y mitiga las amenazas dirigidas a aplicaciones y API que se ejecutan a través de Akamai Connected Cloud, así como bloquea cualquier tráfico que contenga posibles amenazas desenmascaradas por API Security. Si se implementan juntas, las protecciones de API de Akamai ofrecen una visibilidad completa y continua de las API, lo que le permite detectar, auditar y responder a los problemas de seguridad de las API en todo el entorno de aplicaciones.



¿Le interesa saber cómo funciona API Security? Visite akamai.com/apisecurity y reserve una cita con nuestro equipo.

| Publicado en junio de 2024