Guía definitiva de la protección de API en tiempo de ejecución

Tabla de contenido

Introducción

Por qué la seguridad de las API es imprescindible

En la carrera por satisfacer las necesidades de los clientes, las empresas afrontan la presión por desarrollar, producir y mejorar rápidamente aplicaciones, servicios y herramientas de IA generativa. Con este ritmo tan vertiginoso, se corren riesgos que no son tan evidentes: las API que son el motor de todas estas innovaciones suelen crearse con fallos de configuración, errores de codificación y controles de seguridad incompletos. Cuando estas API llegan a la fase de producción, no solo interactúan con ellas los usuarios: los atacantes prueban constantemente nuevas maneras de explotarlas y acceder a los datos que intercambian.

Unas API mal configuradas y en peligro son cada vez más las causantes de importantes filtraciones de datos y, sin embargo, son pocas las organizaciones que vigilan los miles de llamadas de API que se producen en sus ecosistemas digitales. Son aún menos las empresas que cuentan con protección total contra amenazas de API en tiempo de ejecución.

Por ejemplo, en 2021, una compañía de retail de fitness encontró un error en una API con datos de las cuentas de los usuarios que permitía que cualquiera sin autenticarse solicitara datos como la edad, el sexo, la ciudad, el peso o la fecha de nacimiento. Si bien hubo suerte y un investigador de seguridad detectó y notificó esta vulnerabilidad a la empresa, los errores como este pueden pasar inadvertidos y seguir explotándose durante semanas o meses.

Cuando se trata de proteger las API, las herramientas que las organizaciones utilizan tradicionalmente, como las puertas de enlace de API y los firewalls de aplicaciones web, pueden proporcionar una protección básica. Sin embargo, los equipos de seguridad de hoy necesitan más capas de seguridad, ya que los ataques a las API crecen tanto en número como en sofisticación. La clave es complementar los controles existentes con información más detallada sobre las vulnerabilidades, las posibles rutas de ataque, la actividad maliciosa y el comportamiento de las API.

Las organizaciones pueden disfrutar de estas capacidades con una completa solución de seguridad para las API que abarque cuatro áreas:

1. Detección de las API
2. Gestión de la estrategia de las API
3. Protección del tiempo de ejecución de las API
4. Pruebas de seguridad de las API

Contenido de esta guía

La protección de las API en tiempo de ejecución es el proceso de protegerlas durante su funcionamiento habitual de gestión de solicitudes. Esta guía incluye los requisitos principales de la protección de API en tiempo de ejecución, como la supervisión de API para evitar los fallos de configuración, la explotación y los ataques. Analiza los conceptos básicos de prevención en tiempo de ejecución e introduce las funciones que ofrece Akamai API Security.

¿Por qué usar la protección de tiempo de ejecución?

La protección de las API en tiempo de ejecución salvaguarda las API durante la fase de producción, cuando están operativas y los usuarios finales (y los atacantes) pueden interactuar con ellas. Con funciones que ayuden a las organizaciones a identificar y hacer frente con rapidez a las solicitudes de API maliciosas, una protección en tiempo de ejecución eficaz puede proteger las API de una amplia variedad de amenazas posteriores a la implementación, por ejemplo:

- Atacantes que extraen grandes volúmenes de datos confidenciales de una API
- Ataques de derivación de privilegios que explotan errores de seguridad
- Implementación de API no autorizadas fuera de los procesos habituales

Para bloquear las amenazas de API en tiempo de ejecución es necesario comprender el contexto de las operaciones de cada una de estas API en términos de acceso, uso y comportamiento. Lo primero que necesita conocer es el alcance de su infraestructura de API. Nuestra Guía definitiva para la detección de API explica la importancia de contar con un inventario de API. Con un inventario completo puede supervisar todo el tráfico de API y comprender a un nivel básico el comportamiento "típico" de cada una de ellas para reconocer anomalías. La protección de API en tiempo de ejecución debe detectar:

- Filtraciones de datos
- Infracciones de la política de datos
- Ataques contra la seguridad de las API
- Manipulación de datos
- Comportamiento sospechoso

Además, esta protección en tiempo de ejecución debe registrar el tráfico de las API, supervisar el acceso a datos confidenciales, detectar amenazas y bloquear o corregir ataques.

Supervisión del tráfico de API para detectar ataques

Observar el comportamiento del tráfico de API es esencial para identificar los riesgos. Si se implementa una solución de supervisión sin tener un panorama claro de la infraestructura de API, la visibilidad va a ser limitada. Tras haber hecho un inventario de su presencia de API, la protección en tiempo de ejecución debe supervisar continuamente el tráfico y el consumo, y buscar vulnerabilidades y errores de configuración.

Detección de anomalías

Al contar con una referencia del comportamiento habitual de las API, se puede identificar cualquier cosa fuera de lo normal. Reproducir los datos históricos ayuda a detectar anomalías que, asimismo, pueden revelar un intento de ataque.

Cualquier comportamiento no habitual se debe examinar a fondo en contexto con otras acciones que se produzcan en la aplicación o la red. Por ejemplo, si las solicitudes de datos suelen tener un cierto tamaño, y una llamada de API solicita datos fuera del rango de las solicitudes corrientes, debería señalizarse. Puede que no sea una acción maliciosa, pero esta anomalía se debe investigar a fondo.

Detección de la exposición de datos

Posiblemente, algunas de las API de su infraestructura envíen y reciban datos confidenciales. Esta información que se expone cuando hay una vulnerabilidad de seguridad permite que los atacantes deriven privilegios o accedan de manera indebida a otros ajustes de control. La IA y el aprendizaje automático pueden ser esenciales para analizar el tráfico en tiempo real y detectar anomalías, ya que ofrecen información contextual sobre las filtraciones, la manipulación y las infracciones de la política de datos, el comportamiento sospechoso y los ataques contra la seguridad de las API.

Un tipo de ataque que es cada vez más común es que los ciberdelincuentes tengan claves de API válidas. Una vez que el atacante posee claves válidas, la única manera de protegerse del uso indebido de las API y de las posibles filtraciones de datos es poder detectar y bloquear el comportamiento anómalo y la exposición de los datos.

Auditorías de seguridad de las API

Las herramientas para auditar la seguridad de las API deben supervisar el tráfico en tiempo real y avisarle de los ataques y de otros intentos maliciosos. Como mínimo, en estas auditorías se debe hacer lo siguiente:

- Supervisar continuamente para identificar atacantes y solicitudes maliciosas
- Escanear las API de forma pasiva, tanto interna como externamente, para ver si hay errores de configuración y otros aspectos que se hayan pasado por alto y que puedan propiciar o empeorar una filtración, o debilitar las defensas
- Aplicar políticas sobre qué datos deben y no deben enviar o recibir las API

La protección en tiempo de ejecución también debe complementarse con la gestión de la estrategia de las API, que permite identificar errores de configuración y vulnerabilidades conocidas. Eche un vistazo a nuestra Guía definitiva para la gestión de la estrategia de las API para más información.

Funciones imprescindibles para la protección en tiempo de ejecución

Si su organización desarrolla e implementa API activamente, una protección en tiempo de ejecución sólida debe formar parte de su programa de seguridad. A continuación, le presentamos las funciones imprescindibles que deberían incluir sus herramientas de gestión.

Supervisión fuera de banda en tiempo real

La supervisión de seguridad no debería afectar, ralentizar ni incrementar la latencia del tráfico de API. Debe funcionar completamente fuera de banda sin necesitar cambios en la red ni implementar complejos agentes difíciles de instalar. Las herramientas de protección en tiempo de ejecución deben reflejar el tráfico de las fuentes de datos identificadas y realizar un análisis de esos datos de tráfico en segundo plano, con alertas en tiempo real de cualquier problema detectado.

Akamai funciona fuera de banda y sin agente de manera predeterminada, pero ofrecemos opciones de detección con agentes y bloqueo en línea si es necesario.

Detección de anomalías y explotación de API

La recopilación pasiva de datos no es suficiente, especialmente teniendo en cuenta que el número de API y el volumen total de tráfico de las API siguen aumentando. La actividad de las API se debe analizar continuamente para detectar eventos anómalos y alertar a los equipos de seguridad y operaciones. Las herramientas de plataforma de última generación incorporan IA y aprendizaje automático para analizar el tráfico en tiempo real y aprovechar la información contextual sobre filtraciones, manipulación e infracciones de la política de datos, comportamientos sospechosos y ataques contra la seguridad de las API.

Prevención de ataques a las API y corrección de riesgos

Cuando se identifica una anomalía u otro problema y se genera una alerta, el tiempo es esencial. Se debe detectar y corregir el movimiento no autorizado de datos confidenciales a través de API u otro uso indebido sospechoso de estas. La protección en tiempo de ejecución no solo debe evitar el uso indebido de las API integrándose con sus firewalls y puertas de enlace existentes. Además, debe ofrecer opciones de corrección que estén automatizadas si es posible. Busque funciones con puntuaciones de confianza para los atacantes que le ayuden a determinar si las señales de abusos, ataques o filtraciones son legítimas y hay que derivarlas.

Integraciones para la respuesta ante incidentes

Como norma general, las herramientas de protección en tiempo de ejecución deben integrarse fácilmente con el resto de herramientas de seguridad, supervisión y gestión que utiliza su organización. Por ejemplo, cuando se produce un incidente, estas herramientas de protección en tiempo de ejecución deben incluir las integraciones necesarias para garantizar que las tareas de corrección se asignan a los equipos adecuados. Si se detectan errores de configuración, infracciones de políticas de datos o comportamientos sospechosos, se debe informar de ellos a la puerta de enlace de API, el sistema de gestión de información y eventos de seguridad (SIEM) y otros motores de seguridad de la información para garantizar el nivel adecuado de difusión. Contar con la puntuación de confianza para los atacantes permite a los equipos filtrar el ruido y centrarse en las verdaderas prioridades de seguridad de las API.

Rapyd

Rapyd, una empresa de tecnología financiera y procesamiento de pagos a nivel mundial, gestiona sistemas de pago en más de 100 países. Como la empresa no tenía una visibilidad detallada sobre el uso y el comportamiento de sus API, necesitaba una estrategia mejor para proteger las API tanto públicas como internas en un sistema global muy complejo que funciona en la nube de AWS. Rapyd necesitaba un inventario detallado de todas ellas, visibilidad de los errores de configuración y vulnerabilidades, y alertas priorizadas de forma inteligente para adoptar un enfoque de corrección más lógico.

Akamai API Security cumplía las necesidades de Rapyd gracias a su completa visibilidad y su protección en tiempo de ejecución que se sirve del aprendizaje automático para crear una referencia del tráfico para cada API, con detección y corrección automatizadas de anomalías.

Leer la historia de cliente completa

> Ahora podemos evaluar nuestro riesgo de la manera más científica posible y controlar hacia dónde vamos.

– Nir Rothenberg
Director de Seguridad de la Información, Rapyd

Protección en tiempo de ejecución de Akamai API Security

Poder identificar y neutralizar los ataques a las API conforme ocurren debería estar integrado en su programa de cumplimiento y evaluación de riesgos. Puede considerarlo su última línea de defensa si los demás controles de seguridad se quedan cortos.

El módulo de protección en tiempo de ejecución de Akamai API Security incluye todas las funciones que hemos descrito en la sección anterior. Su función principal es detectar y bloquear los ataques a las API en tiempo real. La supervisión automatizada basada en el aprendizaje automático se utiliza para realizar análisis del tráfico y proporcionar información contextual sobre filtraciones, manipulación, infracciones de políticas de datos, comportamientos sospechosos y ataques a la seguridad de las API. La protección en tiempo de ejecución detecta anomalías y posibles amenazas en su tráfico de API, y facilita la corrección en función de políticas preseleccionadas de respuesta a incidentes.

La protección en tiempo de ejecución se integra con los firewalls de aplicaciones web (WAF), las puertas de enlace de API, la gestión de servicios de TI (ITSM), los sistemas SIEM y otras herramientas de flujo de trabajo con el objetivo de ofrecer una defensa completa ante los ataques. Puede optar por automatizar totalmente la corrección de amenazas o requerir diferentes niveles de intervención manual para obtener una mayor visibilidad y control. La solución Akamai API Security también se integra de forma nativa con la plataforma de Akamai, lo que nos permite bloquear las IP de los atacantes directamente en el Edge.

Generación de casos

Gracias al aprendizaje automático, Akamai crea un modelo para cada API. Este comportamiento habitual de referencia se utiliza para detectar ataques a la lógica empresarial de las API, como la autorización a nivel de objeto comprometida (BOLA), en la que se obtiene acceso a datos a los que no se debería acceder. Akamai generará un caso en tiempo real siempre que el tráfico de API se desvíe del comportamiento habitual.

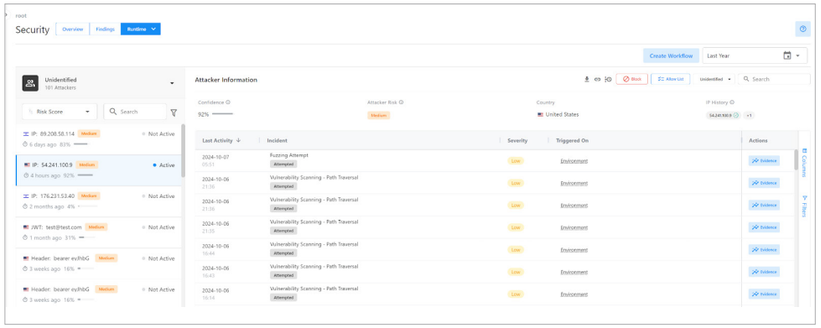
Estos casos son como alertas y se generan siempre que se detecta un comportamiento de API anómalo o un error de configuración. A medida que se generan los casos, se envían alertas automáticamente a un sistema SIEM, como Splunk o QRadar. Estas alertas también se pueden enviar automáticamente a un sistema de seguimiento de incidencias, como ServiceNow o Jira.

Detalles del caso

Cada caso generado por la protección en tiempo de ejecución de Akamai API Security incluye la gravedad, el estado, una asignación a los 10 principales riesgos de las API según OWASP y detalles del atacante, cuando corresponda.

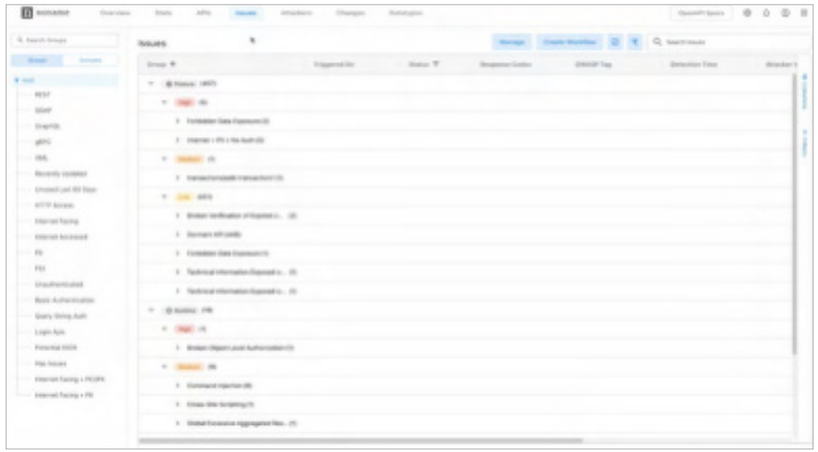
Las páginas de detalles incluyen una descripción del caso y la repercusión que puede tener para su empresa, así como recomendaciones de corrección. Akamai API Security también permite a las organizaciones ver qué tipos de acciones han llevado a cabo los atacantes en un periodo de tiempo específico, con un registro histórico de cada ataque y la posibilidad de actuar contra los agentes maliciosos.

Ejemplo: Visibilidad de las acciones de los atacantes

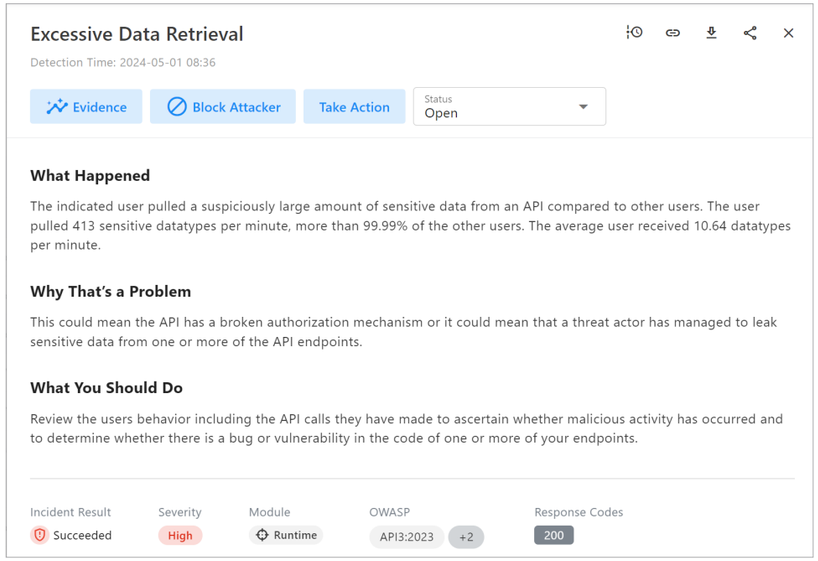


En cada caso se incluyen pruebas, que son los detalles de la sesión del atacante que llevaron a la generación del caso y una copia de la solicitud de API y la respuesta, tanto los encabezados como los cuerpos del mensaje, para ayudar a diagnosticar y corregir el problema rápidamente. Con paneles intuitivos, funciones de filtrado, alertas e informes, el módulo de protección en tiempo de ejecución de la solución Akamai API Security puede ayudar a las organizaciones a determinar qué ha ocurrido, por qué y qué hay que hacer exactamente.

Ejemplo: Notificación de problemas de API con pruebas



Ejemplo: Información sobre extracción de datos excesiva



Acciones de políticas

Con Akamai API Security, se pueden poner en marcha acciones de políticas semiautomatizadas por cada caso que se genere, entre otras, abrir un ticket, enviar información a un sistema SIEM o un webhook a un sistema de terceros, o bloquear a un atacante. El tipo de acciones disponibles se determina según el tipo de integraciones configuradas en la plataforma de Akamai.

La solución contiene muchas políticas predefinidas y listas para usar con el objetivo de detectar ataques a las API y errores de configuración. Akamai API Security también incluye más de 20 tipos de datos preconfigurados a fin de ayudarle a crear las políticas de datos que necesita para detectar cuándo los tipos de datos confidenciales pasan por las API y actuar en consecuencia.

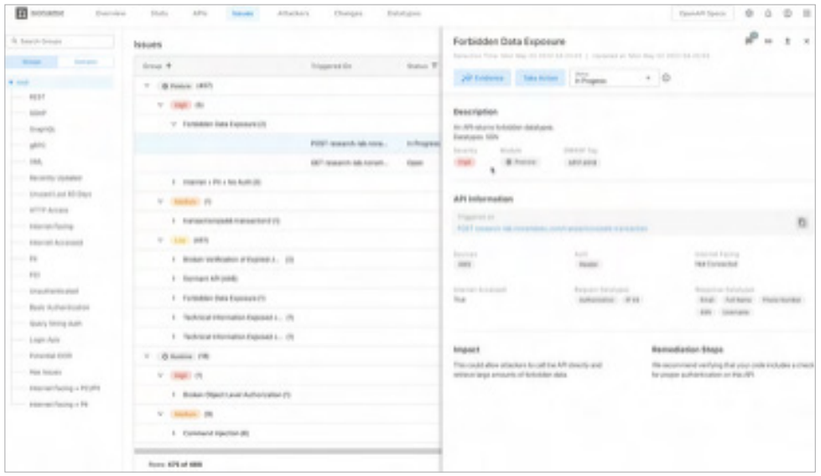
En resumen, el módulo de protección en tiempo de ejecución de la solución Akamai API Security ofrece detección y prevención en tiempo real de ataques de API junto con detección continua de errores de configuración, además de muchas integraciones de flujos de trabajo populares que simplifican las operaciones y la corrección.

Anatomía de un incidente de seguridad de API

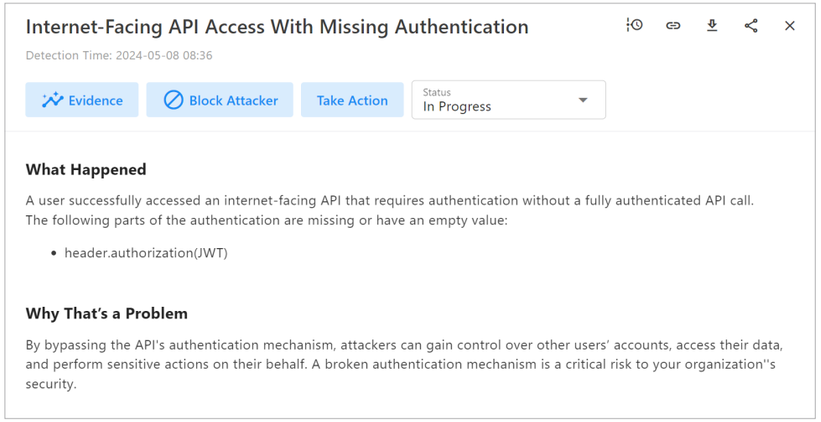
Miremos más en detalle un ejemplo de exposición de datos no autorizados. En este ejemplo se muestra un problema de estrategia interno de una API. La plataforma de Akamai conoce por contexto los tipos de datos y valores asociados con cada API.

En la figura de abajo vemos que hay datos no autorizados que una API está exponiendo. La plataforma de Akamai ha detectado el tipo de datos que se están transmitiendo (en este caso, un número de la Seguridad Social) y ha comprendido que ese tipo de datos se había marcado previamente como no autorizado. Asimismo, Akamai puede detectar errores de configuración externos a las API, como aquellas que son accesibles a través de Internet pero no están registradas en una puerta de enlace de API.

Ejemplo: Notificación de exposición de datos no autorizados



Ejemplo: Identificación de API sin autenticación



Siguientes pasos para una protección de API en tiempo de ejecución eficaz

Cada vez que un cliente, partner o proveedor interactúa digitalmente con su empresa, hay una API en segundo plano que facilita un intercambio de datos que, a menudo, son confidenciales. Implementar funciones de protección de API en tiempo de ejecución, como la supervisión para defenderse ante la explotación y los errores de configuración, así como prevenir los ataques, puede ayudarle a proteger su organización de los vectores de ataque que crecen rápidamente.

Aprenda a **evaluar a los proveedores de seguridad de API** para asegurarse de que ofrecen funciones esenciales de protección en tiempo de ejecución.

Descubra cómo podemos ayudarle con esta **demostración de Akamai API Security personalizada**.

La seguridad de Akamai protege las aplicaciones que impulsan su negocio en cada punto de interacción sin comprometer el rendimiento ni la experiencia del cliente. Gracias a la escala de nuestra plataforma global y su visibilidad de las amenazas, colaboramos con usted para prevenirlas, detectarlas y mitigarlas, de forma que pueda generar confianza en la marca y cumplir su visión. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite **akamai.com** y **akamai.com/blog**, o siga a Akamai Technologies en **X**, antes conocido como Twitter, y **LinkedIn**. Publicado en diciembre de 2024

Akamai