

# Akamai API Security para la gestión de recursos de API

Las organizaciones tienen cada vez más presencia digital y en la nube, por lo que el alcance, la escala y el valor de las API aumentan sin cesar. Este rápido crecimiento también conlleva riesgos.

Es frecuente encontrar API expuestas o mal configuradas, fáciles de atacar. No solo están desprotegidas, a veces no se gestionan o no se tiene visibilidad de ellas, como sucede con las llamadas "API en la sombra", altamente vulnerables. Además, su proliferación dificulta la localización y el inventariado de todas las API de la empresa.

Para ayudar a las organizaciones a obtener la visibilidad que necesitan, Akamai API Security proporciona clasificación e inventariado de API automatizados para usuarios internos y externos.

A la hora de crear un inventario completo, Akamai API Security utiliza varias fuentes, como puertas de enlace de API, firewalls de aplicaciones web (WAF), servicios en la nube pública, tráfico de red o documentación de API, entre otras. Así se garantiza el control sobre cualquier cambio en las API y que aparezca la última versión en la biblioteca de API.

## Solución Akamai API Security

Akamai API Security consta de cuatro módulos integrados que ofrecen gestión de recursos de API y una seguridad integral.

### Detección

Localice sus API y los riesgos relacionados y lleve un inventario, tanto interno como externo.

### Estrategia

Descubra vulnerabilidades y configuraciones erróneas para acelerar la corrección y garantizar el cumplimiento.

### Tiempo de ejecución

Detecte y bloquee los ataques a API gracias al análisis de tráfico en tiempo real basado en el aprendizaje automático.

### Pruebas

Detecte y corrija vulnerabilidades durante el ciclo de vida de desarrollo.

## Ventajas



### Catálogo de API

Identifique sistemas, servicios y aplicaciones que exponen sus API, con una taxonomía detallada.



### Catálogo de consultas

Explore y gestione su inventario de API según casos de uso o marcos regulatorios.



### Estándares de API

Cargue, vea y analice sus archivos de especificación OpenAPI y de reglas de validación.



### Reutilización de API

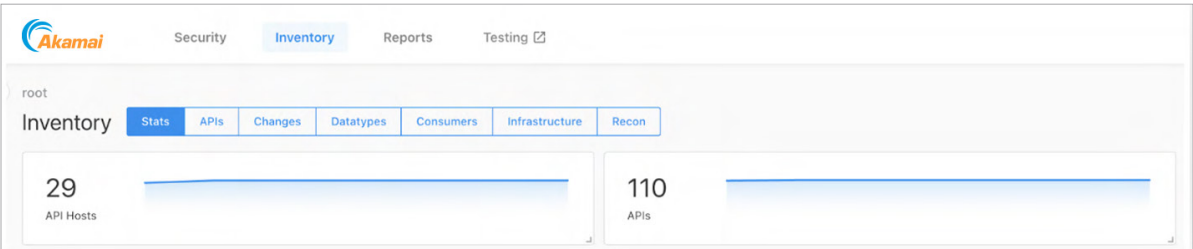
Localice las API existentes que realizan las tareas necesarias en lugar de codificar otras API nuevas.



El punto de partida para la gestión de recursos es el módulo de detección. Al analizar las fuentes de tráfico de su entorno, la solución determina cuántas API tiene y las clasifica automáticamente en función de varios marcos de trabajo.

## Catálogo de API

Akamai API Security presenta un catálogo completo de sus API existentes. Este catálogo identifica los sistemas, servicios y aplicaciones que exponen estas API y proporciona una taxonomía detallada de cada API individual.

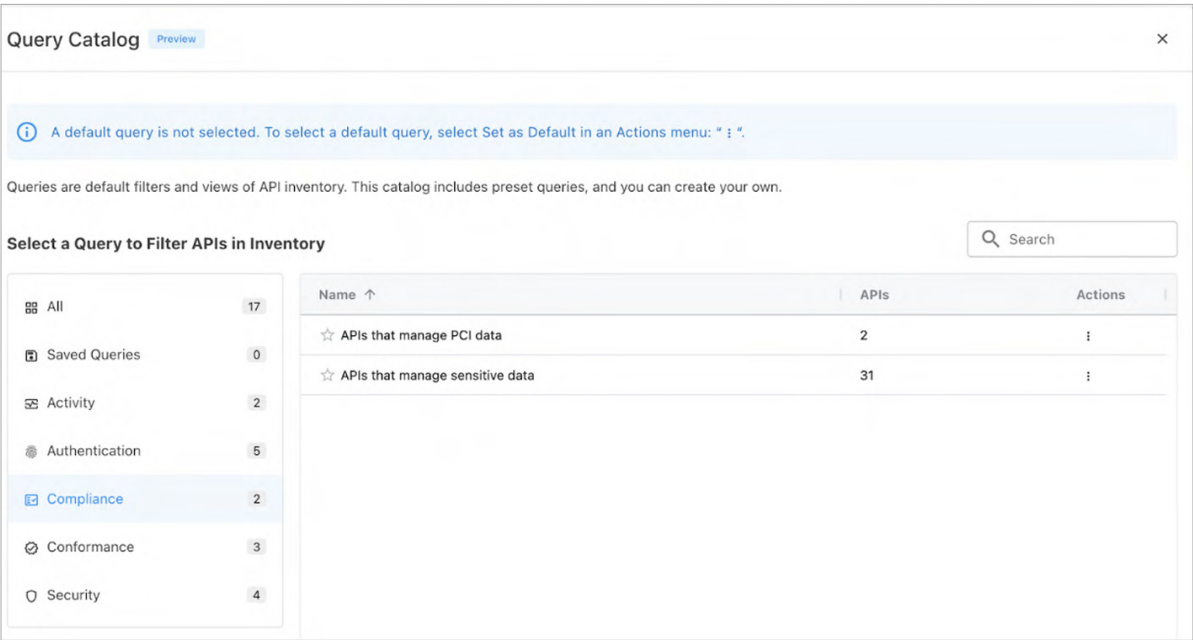


Además, realiza un seguimiento de todos los cambios realizados en las API, lo que permite a los usuarios exportar documentación actualizada como un archivo de especificación OpenAPI basado en estos cambios. El sistema también puede notificar a los usuarios si se agregan nuevas API a su entorno.

Por otro lado, puede utilizar la API de gestión integrada en Akamai API Security para extraer información de la biblioteca de API y crear una base de datos de gestión de configuraciones (CMDB) de API centralizada.

## Catálogo de consultas

Akamai API Security proporciona un catálogo de consultas integrado que le permite explorar y gestionar fácilmente su inventario según sus casos de uso o marcos normativos específicos.



Para cada API, el sistema proporcionará la siguiente información:

- Propietario, tipo y flujos de llamada de API
- Tipos de datos procesados
- Métodos de autenticación admitidos
- Origen y ubicación de la API
- Validación si la API detectada coincide con la especificación/documentación de la API
- Infraestructura que hay detrás de la API
- Gráfico de red completo con las dependencias de API

## Estándares de API

La solución también le permite cargar, ver y analizar sus propios archivos de especificación OpenAPI o de reglas de validación. Crear reglas de validación permite asegurarse de que las API sean técnicamente correctas y cumplan con un conjunto de restricciones adicionales que a menudo se documentan en forma de directrices de API. Akamai incluye un conjunto predeterminado de reglas de validación para Spectral, una herramienta de código abierto que permite a los desarrolladores crear, documentar y mantener API. Además, puede cargar tres formatos de archivos de especificaciones:

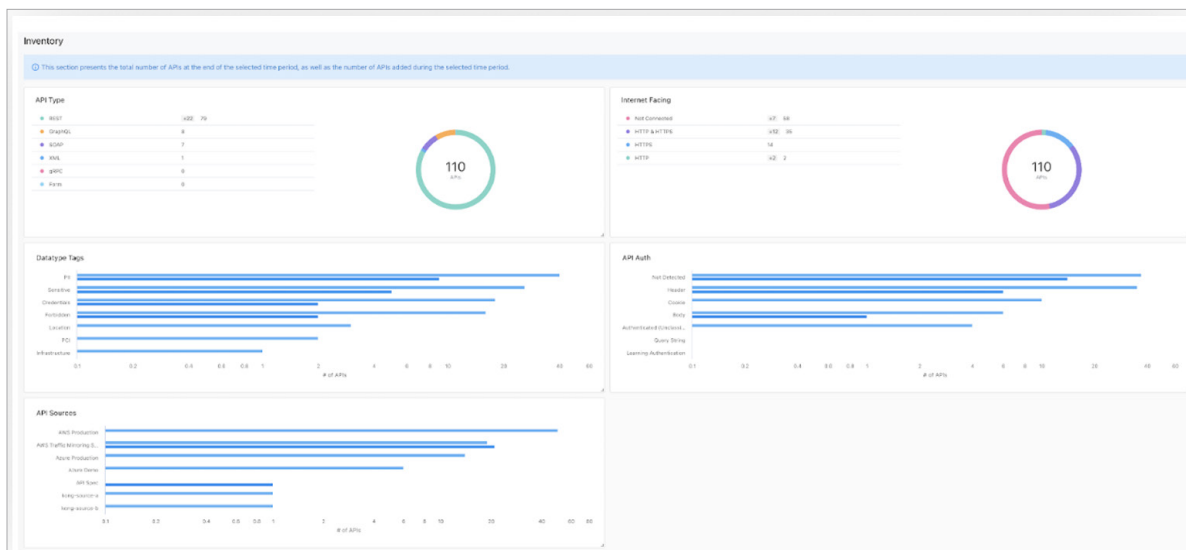
- Lenguaje de modelado de API RESTful (RAML)
- Lenguaje de descripción de servicios web (WSDL)
- Lenguaje de descripción de aplicaciones web (WADL)

De este modo, puede aprovechar los estándares de API existentes o definir los suyos propios y aplicarlos en su entorno. Estos estándares pueden ser específicos de cada sector, por ejemplo, API estándar de banca abierta para el sector de los servicios financieros, basadas en la Red de Arquitectura de la Industria Bancaria (BIAN).

Además, nuestra solución API Security también detectará la desviación del estándar y le permitirá definir políticas de corrección para abordar estos tipos de detecciones. El sistema también detectará e importará las API de sus archivos de especificaciones y las comparará con el tráfico de red real. Con Akamai API Security Recon, también podemos detectar e importar API externas basándonos simplemente en información de nombres de dominio.

## Reutilización de API

Con una completa biblioteca de API en la que es fácil buscar y navegar, los desarrolladores pueden localizar las API existentes que ya realizan la tarea necesaria en lugar de codificar las nuevas desde cero. Gracias a nuestro inventario y catálogo de API, puede fomentar fácilmente una mejor reutilización de sus API, a la vez que limita cualquier brecha de visibilidad en su entorno, tanto para desarrolladores como para profesionales de la seguridad.



## Más información

Las API son un componente clave para las organizaciones a la hora de atender a los clientes, generar ingresos y operar de forma eficiente. Sin embargo, su crecimiento continuo, su proximidad a los datos confidenciales y la falta de controles de seguridad hacen que las API sean un objetivo atractivo para los atacantes de hoy en día. Las organizaciones pueden reducir el riesgo y protegerse contra los ataques de API con una solución de seguridad completa que proporciona funciones de detección, gestión de la estrategia, protección del tiempo de ejecución y pruebas de seguridad.

Descubra cómo puede [Akamai API Security](#) ayudar a su organización.