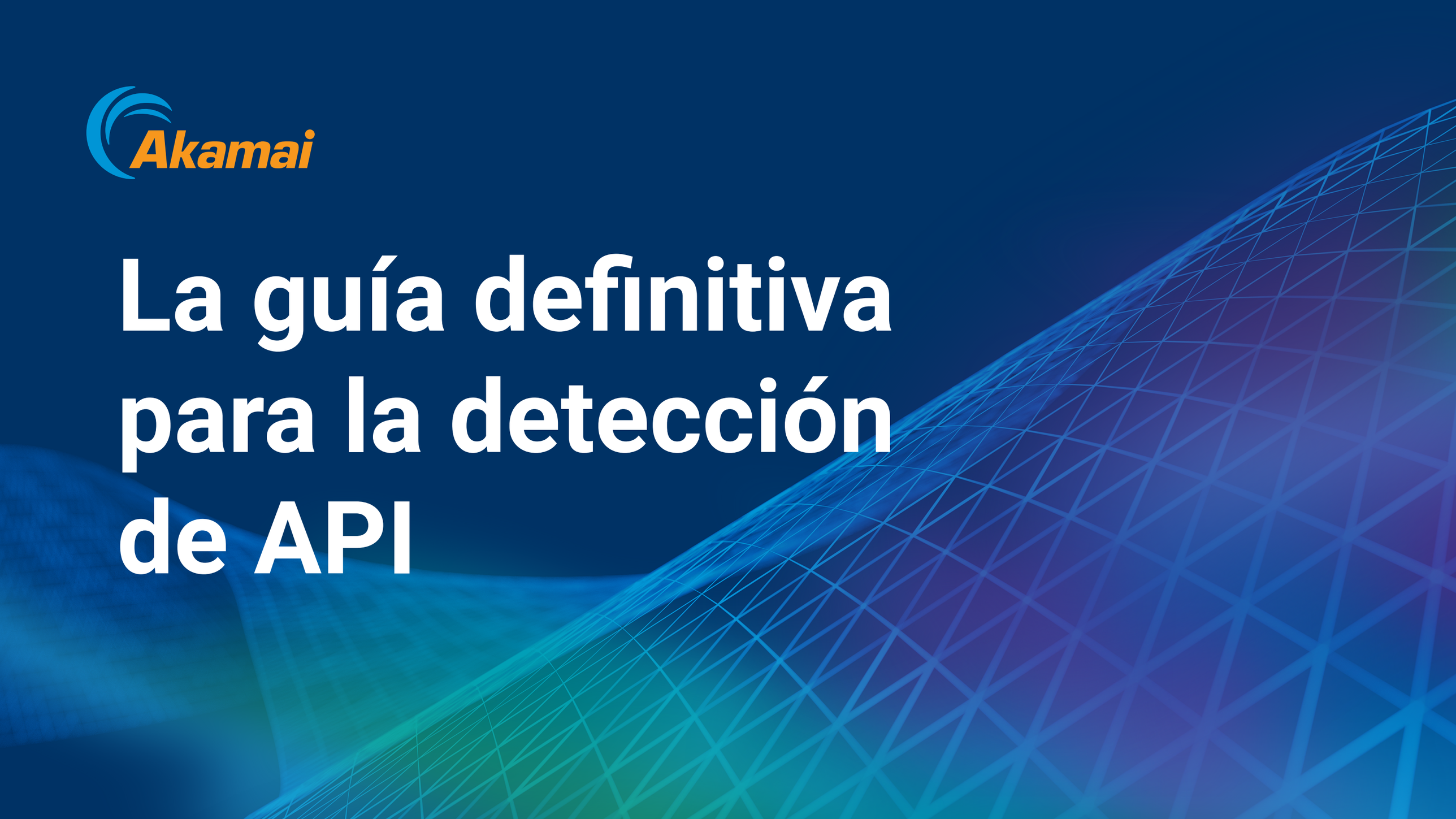

La guía definitiva para la detección de API

Índice

La importancia de la detección de API

Tanto si está familiarizándose con el concepto de seguridad de API como si busca perfeccionar su estrategia actual, detectar todas las API de su organización y llevar un inventario es un paso fundamental. ¿Por qué? Para cada aplicación que cree, cada carga de trabajo que migre a la nube y cada herramienta de colaboración que utilicen sus empleados, existen API que intercambian datos en segundo plano, que a menudo son confidenciales. El riesgo radica en que muchas organizaciones, incluso aquellas conscientes de la importancia de contar con un inventario completo de API, son incapaces de visualizar un porcentaje sustancial de estas.

Y si no puede verlas, no puede protegerlas.

Las organizaciones tienen cada vez más presencia digital y en la nube, por lo que el alcance, la escala y la complejidad de su infraestructura de API aumenta sin cesar. Las API suelen estar repartidas por varios entornos, que pueden ser desde locales hasta de nube híbrida. Y, por si la situación no fuese lo bastante compleja, es probable que su ecosistema de API vaya más allá de su propia red y presencia en la nube. Piense en la infinidad de conexiones que han establecido sus API con aplicaciones y servicios, así como con sistemas de terceros y ecosistemas de desarrolladores.

A medida que sus API crecen en alcance, escalabilidad y complejidad, se vuelve más difícil obtener información en tiempo real sobre:

- Dónde se ubican las API en las diferentes unidades de negocio que, en muchos casos, cuentan con sus propios equipos de desarrolladores
- Cómo están configuradas, a dónde transfieren los datos y si disponen de los controles de autenticación y autorización adecuados
- Si devuelven datos confidenciales cuando reciben una llamada y quién puede acceder a ellos

Para complicar aún más la situación, a menudo las organizaciones no gestionan, visualizan ni protegen una gran parte de las API que acumulan. Hablamos de API inactivas, en la sombra y zombis que, en muchos casos, burlan las herramientas de protección más comunes, como las puertas de enlace de API y los firewalls de aplicaciones web (WAF). Por supuesto, estas herramientas ofrecen ventajas y protección básica, pero el panorama actual de amenazas de API requiere un mayor grado de visibilidad, protección en tiempo real y pruebas continuas que solo las soluciones de seguridad de API más especializadas pueden garantizar.

Una vez que haya detectado todas sus API, podrá llevar a cabo los siguientes pasos con unos cimientos sólidos, como evaluar los riesgos de cada API, entender el nivel de seguridad de las API de su organización y usar la información obtenida para implementar una protección en tiempo real con el fin de evitar los ataques. En este white paper, trataremos los siguientes temas:

- Razones por las que algunas API resultan tan escurridizas para los equipos de seguridad
- Detalles sobre las capacidades de detección de API que pueden ayudarle a obtener visibilidad y evitar ataques

¿Por qué son tan difíciles de detectar las API?

No es raro encontrarse con API no gestionadas en el entorno de producción de las que nadie de los equipos de operaciones y seguridad está al tanto, lo que expone a la empresa a todo tipo de riesgos de ciberseguridad y problemas operativos. Las API expuestas o mal configuradas prevalecen, están desprotegidas y son un blanco fácil para los agentes maliciosos. Hay mucho en juego. Los ataques a las API pueden poner en peligro los ingresos, la resiliencia y el cumplimiento normativo de una empresa.

A continuación, le mostramos cuatro razones por las que pueden surgir API no autorizadas:

1. Atajos y procesos que no se siguen

Algunas API no autorizadas son el resultado de no informar a las personas adecuadas. Por ejemplo, es posible que el equipo de una línea de negocio (LOB) cree API para dar respuesta a sus propias necesidades sin informar al departamento de TI, o que a los desarrolladores les preocupe más la ejecución que los procedimientos. También es habitual pasar por alto API que se han "heredado" como parte de una adquisición. Estos tipos de API no autorizadas se conocen comúnmente como API en la sombra.

2. Versiones anteriores de API

En muchas ocasiones, no se elimina la versión anterior de una API, a menudo con una seguridad más débil o una vulnerabilidad detectada. Esta versión coexiste con la más nueva durante un tiempo mientras se actualiza el software. Pero ¿y si la persona responsable de desactivar la API abandona la empresa, cambia de puesto o simplemente se olvida de desactivarla? También es posible que una API se haya retirado oficialmente, pero permanezca en funcionamiento debido a descuidos operativos. En cualquier caso, el resultado final es lo que conocemos como API zombi.

3. API heredadas

Las API que se han “heredado” como parte de fusiones o adquisiciones también suelen pasar inadvertidas y se convierten en API en la sombra. Los inventarios (si existen) a menudo se pierden en el complicado proceso de integración de sistemas. Las empresas más grandes que adquieren pequeñas firmas con frecuencia están especialmente expuestas, ya que estas últimas no suelen organizar ni documentar su infraestructura de API.

4. API comerciales

Algunos paquetes de software comercial incluyen API para crear conexiones con otras aplicaciones y fuentes de datos externas. A veces, estas API se activan sin que nadie se dé cuenta.

¿Qué es la detección de API?

La detección de API es un proceso y un conjunto de funciones que ayudan a las organizaciones a identificar, catalogar, gestionar y evaluar el riesgo de sus API. Si se lleva a cabo correctamente, la detección de API ofrece a las organizaciones las siguientes ventajas:

- Reduce la proliferación de API (la rápida acumulación de API sin una documentación o supervisión adecuadas) y fortalece la estrategia de seguridad
- Ayuda a las empresas a comprender mejor el panorama actual de API y a tomar decisiones fundamentadas sobre futuros cambios
- Facilita la supervisión y el control del acceso a las API, lo que garantiza que solo los usuarios autorizados tengan acceso a ellas

Funciones clave de detección de API para aumentar la visibilidad y mitigar el riesgo

Es habitual tener API que nadie conoce. Sin embargo, sin un inventario preciso, su empresa se expone a muchos riesgos. Para crear un inventario adecuado de sus API, debe poder:

Localizar
sus API y llevar un inventario, independientemente de su configuración o tipo

Detectar
las API no gestionadas, como las API inactivas y zombis

Identificar
dominios en la sombra olvidados, descuidados o desconocidos

Eliminar
las brechas de visibilidad y descubrir posibles rutas de ataque

Cuando valore nuevas soluciones para la detección de API, tenga en cuenta las siguientes capacidades; una herramienta de detección debe incorporarlas todas.

Detección de todos los tipos de API

Una herramienta de detección de API debe poder identificar las API, independientemente de su tipo o configuración, lo que abarca RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC y gRPC.

Inventario detallado de API

También debe crear un inventario que se actualice automáticamente para evitar que quede obsoleto, así como proporcionar la capacidad de buscar, etiquetar, filtrar, asignar y exportar API en función de cualquier atributo.

Detección de las API más escurridizas

Es posible que sus API empezasen a proliferar mientras trabajaba un equipo de desarrolladores que ya no figura en su organización, por lo que algunas de sus API no gestionadas pueden ser anteriores a la implementación de iniciativas de seguridad de API. Lo normal es que estas API no tengan dueño, no haya visibilidad de ellas y no se les apliquen controles de seguridad. Es fundamental que una herramienta de detección de API pueda localizarlas.

Detección de dominios de API en la sombra

Además de API en la sombra, es posible que tenga dominios enteros en la sombra; es decir, nombres de dominio de API totalmente desconocidos. Las herramientas de detección de API deben poder identificar dominios en la sombra olvidados, descuidados o desconocidos que puedan suponer un riesgo para la seguridad.

Análisis automático de API

Los análisis son esenciales para eliminar los puntos ciegos e identificar problemas críticos, como:

- Claves y credenciales de API filtradas
- Exposición de esquemas y código de API
- Errores de configuración de la infraestructura
- Vulnerabilidades en páginas de documentación, repositorios de GitHub, espacios de trabajo Postman, etc.

Identificar estas y otras fuentes de inteligencia explotable también puede ayudar a los equipos a conocer las posibles rutas de ataque que podrían utilizar los ciberdelincuentes.

Sin integraciones

Una herramienta de detección de API debe ser capaz de aportar visibilidad completa del entorno de API, así como de encontrar API vulnerables y dominios en la sombra, sin necesidad de integraciones especiales ni instalación de software. De lo contrario, no se podrán evitar las brechas de visibilidad que se producen simplemente porque no se han instalado los agentes adecuados o no se ha configurado la herramienta correctamente.

Desarrollo personalizado limitado

Por último, una herramienta de detección de API debe contar con un diseño que no requiera un desarrollo personalizado para las fuentes de tráfico. Estas herramientas deben incluir integraciones predefinidas para los principales componentes de la infraestructura. El desarrollo personalizado suele llevar mucho tiempo y, si se producen cambios en el origen de la fuente, es probable que sea necesario modificar una integración, una tarea que los desbordados equipos de seguridad de TI no pueden escalar.

Descubra cómo la seguridad de Akamai puede ayudarle a detectar todas las API

Con nuestras capacidades de detección de API completas y continuas, su organización experimentará las siguientes mejoras:

- Conocerá toda la superficie de ataque de API
- Reducirá los costes de los inventarios de API y las actualizaciones de documentación
- Mejorará el cumplimiento de los requisitos normativos y las políticas internas

Las amenazas actuales exigen una solución completa de seguridad de las API que abarque cuatro áreas críticas: detección, gestión de la estrategia, detección y corrección de amenazas y pruebas de seguridad de API. Akamai API Security proporciona estos cuatro módulos esenciales para proteger 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, evalúa su nivel de riesgo, analiza sus comportamientos y evita que las amenazas se infiltren en su empresa.

Obtenga más información sobre los métodos de ataque a las API, las vulnerabilidades comunes de las API y las formas de proteger su organización.

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

Acerca de la seguridad de Akamai

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 el 24 de octubre.