Akamai

WHITE PAPER

10 capacidades fundamentales de detección y respuesta de API

Desarrollando su estrategia de seguridad de API

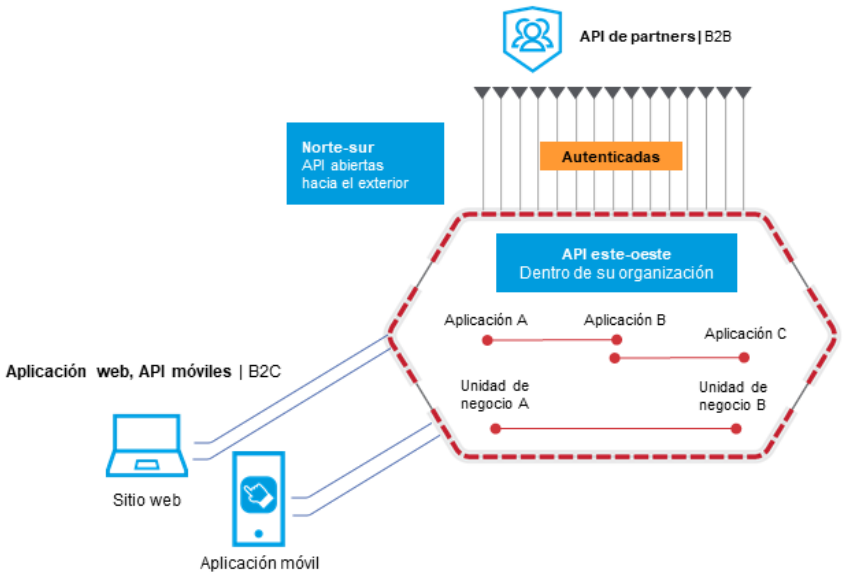
Introducción

Las interfaces de programación de aplicaciones (API) son los componentes básicos clave que impulsan la innovación, y las aplicaciones de empresa a empresa (B2B) y de empresa a cliente (B2C) son el eje de esta transformación. Esto significa que es fundamental proteger las comunicaciones esenciales, que suelen ser confidenciales, internamente (del resto de los microservicios) y externamente (del resto de los clientes y partners). Hoy en día, la mayoría de las organizaciones reconocen que el éxito empresarial a largo plazo requiere una estrategia de seguridad de aplicaciones sólida, y utilizan tecnologías de seguridad como plataformas de protección de API y aplicaciones web (WAAP), funciones y productos de seguridad en la nube, y herramientas de pruebas de seguridad para reducir el riesgo al que se enfrentan las aplicaciones. Es importante reconocer cómo han evolucionado los ataques para eludir las WAAP y acceder a las API que se usan en las organizaciones. Es hora de analizar cómo ajustar su estrategia de seguridad de API antes de que se materialicen estas amenazas.

¿Dónde encaja la detección y respuesta de API en una estrategia de seguridad de API?

En los últimos años, las organizaciones han creado muchos más canales de API que interfaces de aplicaciones web, y estas API incluyen volúmenes cada vez mayores de datos empresariales y lógica empresarial esenciales. Las API han modificado la forma de operar de las empresas, ya que posibilitan más casos de uso, aceleran el cambio, transportan más datos confidenciales y están abiertas a más usuarios.

¿Cómo es su panorama de API?



Aunque la mayoría de las categorías de productos de seguridad admiten API de alguna manera debido a su creciente prevalencia, las API son una clase de activos diferente e incluso aparecen como tal en ciertos marcos de cumplimiento. La incorporación de capacidades de protección contra amenazas de API a un producto de seguridad heredado, como una plataforma de WAAP, no aborda los nuevos desafíos que plantean estas API. Los responsables de la seguridad deben tratar las API como una clase de activo independiente y reconocer las capacidades fundamentales que protegen las API completamente y a gran escala.

Comencemos con los fundamentos en torno a cómo han cambiado las protecciones de las API para hacer frente a las amenazas emergentes. En el pasado, si una organización tenía un inventario completo de sus API y una WAAP sólida, las amenazas contra las API se podían evitar por lo general. En la actualidad, los ataques se dirigen contra las API de las organizaciones y de sus partners de formas diseñadas para eludir la WAAP.

Por ejemplo, algunos tipos de abuso de API proceden de clientes y partners a los que se les han otorgado credenciales de API y deciden utilizarlas de formas no autorizadas. También hay maneras de piratear credenciales de API o tokens de seguridad aparentemente legítimos. Las vulnerabilidades ocultas en las implementaciones de cliente de API son otro vector de ataque que los atacantes pueden aprovechar para abusar de las API de formas que las herramientas de seguridad tradicionales no pueden detectar.

Lo bueno es que las organizaciones ya tienen a su disposición las capacidades fundamentales a gran escala que se necesitan para proteger las API de tendencias emergentes, específicamente en términos de detección y respuesta. En las páginas siguientes se analizan detenidamente las capacidades fundamentales que hacen de estas plataformas una protección eficaz frente a un panorama de amenazas de API que cambia sin cesar.

Capacidad fundamental n.º 1
Protección independiente de la plataforma

Por lo general, los servicios de API los implementan diferentes grupos de una organización, que suelen utilizar un conjunto diverso de plataformas y tecnologías. Por ejemplo, algunas API se pueden implementar localmente, mientras que otras se pueden ejecutar en la nube pública. También puede haber tecnologías intermedias en uso, como proxies inversos, puertas de enlace de API, firewalls de aplicaciones web (WAF) y redes de distribución de contenido (CDN), lo que genera complejidad respecto a la visibilidad de las API.

La capacidad de acceder a los datos de actividad de API de cada una de estas tecnologías diferentes es imprescindible. Un enfoque de protección frente a las amenazas contra las API que no dependa de la plataforma garantiza que su organización siempre tenga una visión completa de toda la actividad de las API, independientemente de las particularidades de implementación o de la infraestructura en uso. Esto ofrecerá:

- protección para todos los departamentos, empresas adquiridas y entornos;
- protección para todas las API, tanto las autorizadas como las que se usen en la sombra, independientemente de si utilizan la puerta de enlace de API; y
- visibilidad ampliada más allá de las API que manejan tráfico norte-sur, incluidas las API públicas, las de partners y las internas que manejan tráfico este-oeste.

Garantizar que la visibilidad de su plataforma de protección contra amenazas de API sea lo más amplia posible protegerá su organización contra las amenazas internas y el abuso de API por parte de organizaciones de partners, así como contra los riesgos de atacantes externos.

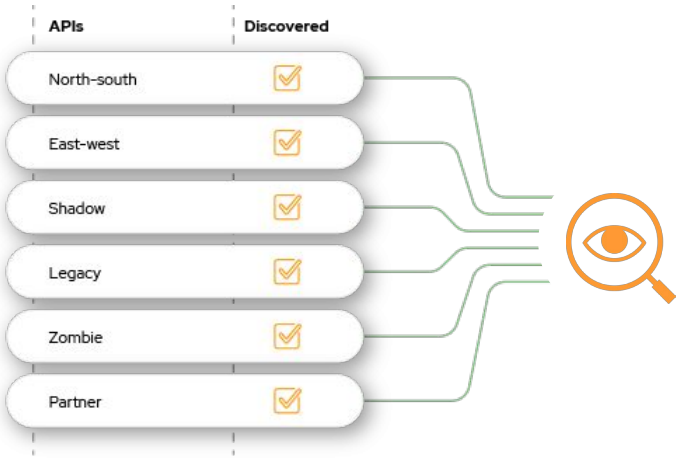
Capacidad fundamental n.º 2
Gestión de la estrategia y detección continua de API

Un inventario completo y continuamente actualizado de todas las API en uso en toda la organización es la base esencial de cualquier estrategia de seguridad de API. Esto se debe a la sencilla razón de que una organización no puede proteger lo que no sabe que tiene en su entorno. Muchos productos de seguridad de API afirman contar con cierto nivel de detección de API, pero su funcionamiento se limita a una vez al día o a petición. Es importante asegurarse de que las capacidades de detección de API de la plataforma incluyan:

- detección automatizada y continua de API en todo momento, incluida la detección de API que solo se utilizan una vez (la detección una vez al día o a petición no es suficiente);
- detección de todas las API de diferentes tecnologías e infraestructuras;
- detección de API recién implementadas y comparación con el conjunto de API bien documentadas para identificar las API en la sombra;
- puntuación de riesgo de todos los terminales y servicios de API; y
- detección de instancias de vulnerabilidades conocidas de API, como las descritas en la lista de las 10 principales vulnerabilidades según OWASP.

Mejora de la visibilidad

No pierda nunca de vista su inventario de API

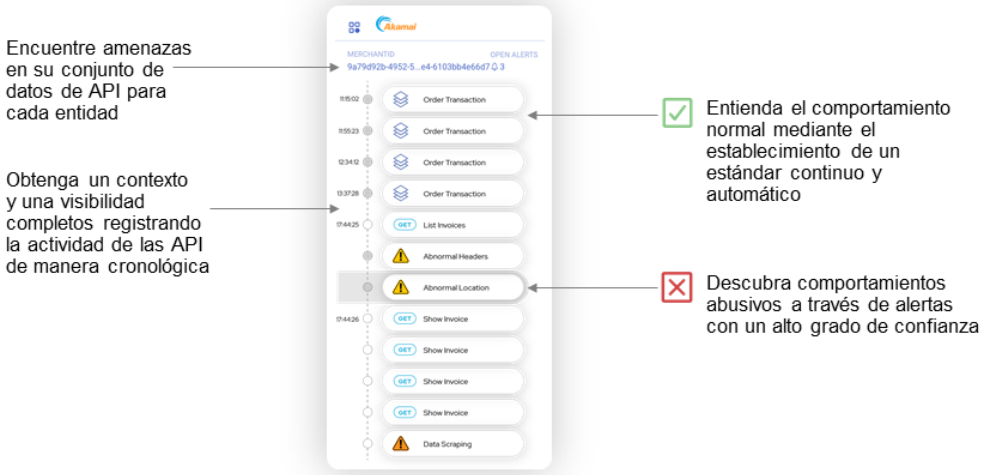


Capacidad fundamental n.º 3
Visualización del comportamiento de las API

La capacidad de mostrar y visualizar el comportamiento real de las API (llamadas a las API) es una capacidad fundamental en las plataformas de seguridad de API. Esta capacidad es necesaria para que las partes interesadas clave de los departamentos de seguridad, desarrollo y operaciones puedan ver y comprender cómo se están utilizando las API o si se están explotando, de modo que puedan comunicarse con los equipos e investigar los casos. Las funciones de visualización específicas que deben tener son:

- **Investigación:** cualquier alerta debe ofrecer la capacidad de inspeccionar la actividad original de la API, llamada por llamada, para identificar qué elemento específico ha activado la alerta.
- **Búsqueda de amenazas:** el historial de datos debe abarcar un periodo de al menos 30 días consecutivos, así como ofrecer la posibilidad de ver todas las actividades de las API y de consultar periodos y llamadas que no se limiten a alertas específicas. Esta capacidad también ayuda a cumplir con los reglamentos.
- **Fidelidad y enriquecimiento de datos:** respecto a cada llamada a la API, debe ser posible identificar qué usuario la ha realizado, qué operación ha utilizado, a qué registros ha accedido o cuáles ha manipulado, qué encabezados y parámetros se han utilizado, etc.
- **Privacidad de datos:** aunque la fidelidad de los datos es importante, los datos confidenciales no se pueden almacenar en reposo. La tokenización es necesaria para conservar la riqueza de los datos sin almacenar información confidencial.
- **Visualización de cronología:** se debe proporcionar a los usuarios una vista que permita ver fácilmente las secuencias de actividad anteriores y posteriores.

Detección de amenazas mediante análisis de comportamiento



Capacidad fundamental n.º 4
Seguimiento de varias entidades de usuario

La identificación de la entidad y la visualización de la actividad de API relacionada ofrecen contexto de cualquier tipo de uso o abuso, por lo que es fundamental que su plataforma de protección de API sea lo suficientemente sofisticada para realizar un seguimiento individual de cada una de estas entidades. Esto proporciona un contexto esencial, ya que la actividad normal para una categoría de usuarios puede ser una señal de advertencia de abuso para otro usuario. La capacidad de ver la cronología de las actividades de cada entidad proporciona una visibilidad vital y comprensión contextual. Por ejemplo:

Actividad de API	Participantes	Entidades	Entidades de procesos empresariales
Ejemplos	Usuarios internos, partners B2B, usuarios externos	Dirección IP, token de API, ID de comercio, ID de sesión, ID de inquilino	ID de pago, ID de factura

Capacidad fundamental n.º 5
Seguridad de API B2B y este-oeste

El área en la que más aumenta el uso de API son los casos de uso B2B, tanto internos como externos. La seguridad debe abarcar las API B2B de máquina a máquina, incluidas las instancias norte-sur (orientadas al exterior) y este-oeste (orientadas al interior).

Aunque las plataformas WAAP y WAF ofrecen protección a las aplicaciones web B2C, algunos de los tipos más sensibles de actividad de API, como la de las API este-oeste internas o la funcionalidad de aplicaciones de propiedad expuestas a los partners a través de API B2B, pueden estar en peligro incluso al pasar por WAAP.

A menudo, una vez que un usuario se autentica en una API de partner B2B, se supone que es seguro y no se aplica ningún otro método de supervisión. Esto constituye una carencia crítica de la estrategia de seguridad de API de muchas organizaciones. Para proporcionar una imagen completa de la actividad de las API y del panorama de amenazas general, las organizaciones deben aplicar un enfoque que proporcione visibilidad, capacidad de observación y supervisión eficaces de todos los casos de uso.

Capacidad fundamental n.º 6
Análisis y detección de comportamiento

La detección de amenazas sofisticadas contra las API no es posible mediante el análisis de llamadas a API individuales (ni siquiera de sesiones individuales). La detección y respuesta de API requiere un conocimiento profundo y un aprendizaje basado en contextos de comportamiento. Para saber si el comportamiento de una API es anómalo, lo que podría indicar que su seguridad se ha visto comprometida, es necesario analizar el uso de la API durante periodos más largos. La técnica de análisis de comportamiento fija como referencia el comportamiento normal del usuario y lo supervisa continuamente para detectar anomalías.

Debido a los recursos informáticos y de almacenamiento necesarios para analizar a este nivel la actividad de API de una empresa estándar, es poco práctico realizar la tarea usando herramientas de seguridad de API locales con limitaciones de escala. Las soluciones de detección y respuesta en los terminales (EDR) y detección y respuesta extendidas (XDR) fueron pioneras al demostrar que se necesita una arquitectura basada en software como servicio (SaaS) para realizar análisis de comportamiento útiles. La potencia y la escala de la nube permiten almacenar datos a lo largo del tiempo y analizarlos para determinar el comportamiento normal del usuario a lo largo del tiempo y detectar la aguja en el pajar que revela el abuso. Un enfoque SaaS tiene otras ventajas, como una implementación más rápida y sencilla, y una escalabilidad y elasticidad mejoradas a medida que aumenta el uso de API.

Capacidad fundamental n.º 7
Alertas útiles con contexto

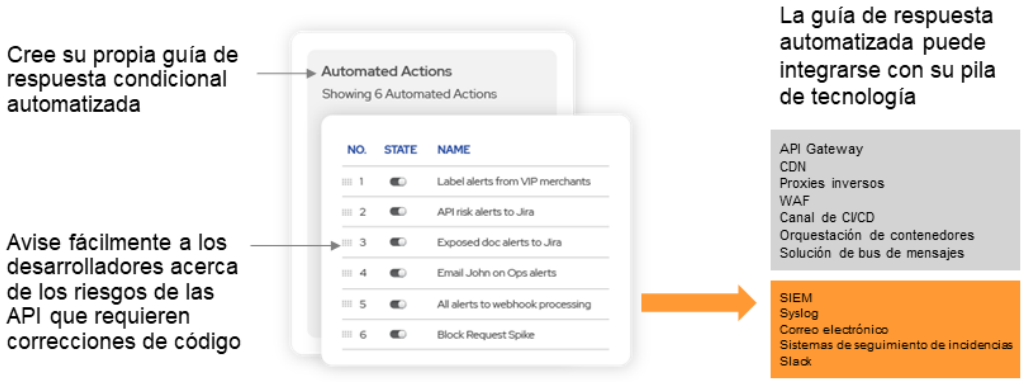
Una vez que una organización tiene visibilidad de toda la actividad de las API y análisis de comportamiento a gran escala, las alertas sobre la actividad de las API son mucho más útiles. Por tanto, las organizaciones ya no necesitan anticiparse a todos los métodos de ataque posibles haciendo que el enfoque de supervisión de la seguridad sea más abstracto. Establecer los valores de referencia del comportamiento normal y detectar anomalías también permite detectar el abuso de API, que a menudo no se puede detectar mediante ningún patrón o firma. Además, poder "rebobinar" el ataque y ver lo que ocurrió antes de una alerta proporciona información valiosa sobre el uso y el abuso de un entorno de API.

Capacidad fundamental n.º 8
Respuestas personalizadas y automatizadas

Los enfoques tradicionales de API en línea pueden automatizar acciones para bloquear posibles ataques contra las API, con la salvedad de que las organizaciones deben ser capaces de identificar los ataques. Dado que el análisis de comportamiento y la detección de anomalías de las API se realizan a lo largo del tiempo con un contexto empresarial mucho mayor, la profundidad de la detección permite identificar anomalías. Esto posibilita una amplia gama de respuestas automatizadas y personalizadas, que se pueden aplicar con gran precisión. Veamos algunos ejemplos:

- Bloquear o limitar el tráfico en las puertas de enlace de API y los filtros en el borde de Internet de CDN compatibles.
- Enviar notificaciones por correo electrónico a las partes interesadas de la empresa y el departamento de seguridad.
- Crear incidencias para los desarrolladores.
- Activar webhooks.

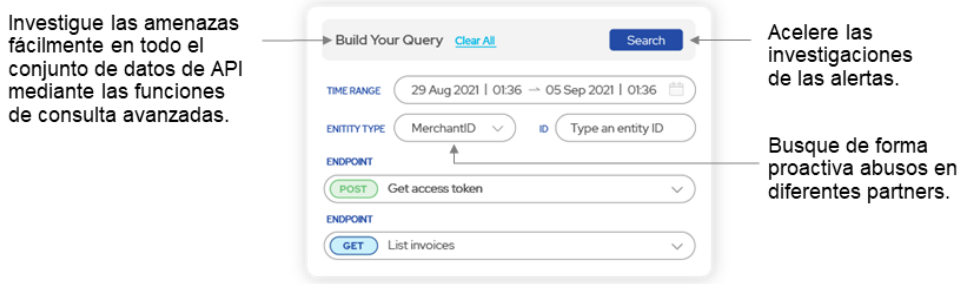
Las respuestas se pueden adaptar a sus procesos empresariales



Capacidad fundamental n.º 9
Investigación y búsqueda proactivas de amenazas

Muchas organizaciones no pueden permitirse el lujo de esperar a que se produzca un incidente de seguridad para actuar. Un enfoque más eficaz consiste en identificar situaciones no deseadas y buscarlas activamente. Por ejemplo, si una alerta detecta un abuso en una API podría identificarse el mismo comportamiento en otra API a través de la búsqueda proactiva de amenazas. Por lo tanto, una plataforma de protección contra amenazas de API debe incluir la capacidad de buscar tipos específicos de comportamiento más allá de las alertas generadas en respuesta a incidentes activos. Las funciones de búsqueda de amenazas requieren acceso a historiales de datos para encontrar los abusos que se ocultan entre la información de actividad de las API. Las soluciones de solicitud única que no enriquecen los datos para proporcionar contexto no pueden elaborar una historia completa. La búsqueda y la investigación de amenazas se basan en datos históricos.

El poder de investigar y buscar amenazas, a su alcance



Capacidad fundamental n.º 10
Lago de datos observable

En todas las capacidades que conforman una estrategia de seguridad de API sólida, el contexto es clave para proteger cualquier API a largo plazo. La mejor forma de acumular un contexto suficiente para vigilar la aparición de amenazas, identificar posibles vulnerabilidades y solucionar problemas en caso de ataque es registrar todo el comportamiento de las API y mantener un registro de esta actividad. Esto se puede lograr si se tiene un lago de datos asociado a la solución de seguridad de API. Busque un lago de datos que proporcione la mayor cantidad de detalles históricos posible en los que basar su estrategia. Si bien puede resultar útil introducir datos de solicitud básicos en los modelos de aprendizaje automático, disponer de detalles como los parámetros de solicitud permite a las organizaciones actuar en función de sus datos históricos para protegerse frente a amenazas y ataques futuros.

N.º 1: Protección independiente de la plataforma	Garantizar que la visibilidad de su plataforma de protección contra amenazas de API sea lo más amplia posible protegerá su organización contra las amenazas y el abuso.
N.º 2: Gestión de la estrategia y detección continua de API	Un inventario completo y continuamente actualizado de todas las API en uso en toda la organización es esencial porque las organizaciones no pueden proteger lo que no saben que tienen en su entorno.
N.º 3: Visualización del comportamiento de las API	La visibilidad es necesaria para que las partes interesadas clave de los departamentos de seguridad, desarrollo y operaciones puedan ver y comprender cómo se están utilizando las API o si se están explotando, y puedan comunicarse con los equipos e investigar los casos.
N.º 4: Seguimiento de varias entidades de usuario	La identificación de la entidad y la visualización de la actividad de API relacionada ofrecen contexto de cualquier tipo de uso o abuso, por lo que es fundamental que su plataforma de protección de API sea lo suficientemente sofisticada para realizar un seguimiento individual de cada entidad.
N.º 5: Seguridad de API B2B y este-oeste	Para proporcionar una imagen completa de la actividad de las API y del panorama de amenazas general, las organizaciones deben aplicar un enfoque que proporcione visibilidad, capacidad de observación y supervisión eficaces de todos los casos de uso.
N.º 6: Análisis y detección de comportamiento	Para saber si el comportamiento de una API es anómalo, lo que podría indicar que su seguridad se ha visto comprometida, es necesario analizar el uso de la API durante periodos más largos. La técnica de análisis de comportamiento fija como referencia el comportamiento normal del usuario y lo supervisa continuamente para detectar anomalías.
N.º 7: Alertas útiles con contexto	Una vez que una organización tiene visibilidad de toda la actividad de las API y análisis de comportamiento a gran escala, las alertas sobre la actividad de las API son mucho más útiles. Por tanto, las organizaciones ya no necesitan anticiparse a todos los métodos de ataque posibles haciendo que el enfoque de supervisión de la seguridad sea más abstracto.

N.º 8: Respuestas personalizadas y automatizadas	Dado que el análisis de comportamiento y la detección de anomalías de las API se realizan a lo largo del tiempo con un contexto empresarial mucho mayor, la profundidad de la detección permite identificar anomalías. Esto posibilita una amplia gama de respuestas automatizadas y personalizadas, que se pueden aplicar con gran precisión.
N.º 9: Investigación y búsqueda proactivas de amenazas	Muchas organizaciones no pueden permitirse el lujo de esperar a que se produzca un incidente de seguridad para actuar. Un enfoque más eficaz consiste en identificar situaciones no deseadas y buscarlas activamente.
N.º 10: Lago de datos observable	La mejor forma de acumular un contexto suficiente para vigilar la aparición de amenazas, identificar posibles vulnerabilidades y solucionar problemas en caso de ataque es registrar todo el comportamiento de las API y mantener un registro de esta actividad. Esto se puede lograr si se tiene un lago de datos asociado a la plataforma de seguridad de API.

Si esta información le ha resultado útil, el siguiente paso es explorar la solución API Security de Akamai para asegurarse de contar con la estrategia de seguridad de API más sólida posible.

Akamai protege la experiencia de sus clientes, su personal, sus sistemas y sus datos, ayudándole a integrar la seguridad en todo lo que crea, dondequiera que lo cree o distribuya. La visibilidad de las amenazas globales que ofrece nuestra plataforma nos permite adaptar y desarrollar su estrategia de seguridad para integrar el enfoque Zero Trust, detener el ransomware, proteger las aplicaciones y las API o combatir los ataques DDoS, y le proporciona la confianza necesaria para innovar, crecer y transformar todo su entorno. 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, anteriormente conocido como Twitter, y en LinkedIn. Publicado en diciembre de 2023.