Akamai

WHITE PAPER

13 preguntas que debe hacer a su proveedor de seguridad de API

Introducción

La red de API de empresa a empresa crece exponencialmente, y un universo en expansión de dispositivos del Internet de las cosas está ofreciendo nuevas oportunidades para que los desarrolladores introduzcan datos del mundo real en las aplicaciones a través de las API.

Sin embargo, aunque las API dan pie a muchas oportunidades nuevas de innovación y crecimiento, también presentan toda una serie de nuevos desafíos de seguridad, entre los que se incluyen:

- Robo de las credenciales de API
- Reconocimiento de API no detectado
- Autenticación y autorización configuradas de forma incorrecta
- API en la sombra y API zombis
- Ejecución remota de código, inyección, inclusión de archivos locales y otras técnicas de ataque
- Filtración o exfiltración de datos
- Scraping de API
- Abuso de la lógica empresarial

Los proveedores de seguridad ofrecen muchas opciones para detectar y mitigar estas y otras amenazas de API, pero no todas son igual de eficaces o fáciles de usar.

Las 13 preguntas siguientes le ayudarán a dirigir sus conversaciones con los proveedores de seguridad de API y a evaluar la eficacia con la que sus productos satisfarán las necesidades de su organización.

1 ¿Su solución de seguridad de API es capaz de detectar las API en toda la empresa?

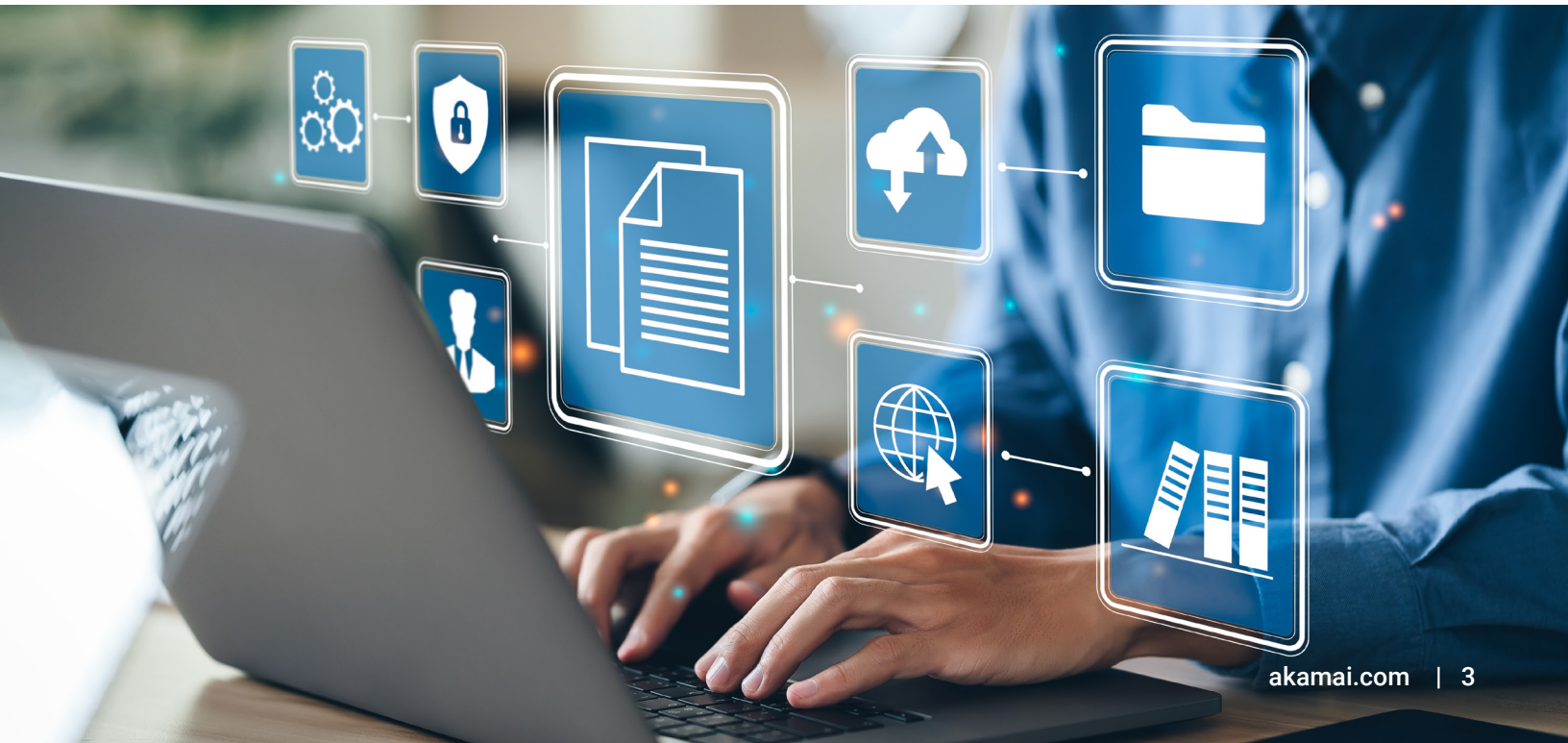
Uno de los mayores problemas a los que se enfrentan los equipos de seguridad es que no tienen un inventario completo y preciso de todas las API que tiene expuestas su organización. Muchas de las API en la sombra no documentadas que los equipos de seguridad no saben que existen no forman parte del marco formal de seguridad y gestión de API. También es habitual que las API zombis, aquellas que la organización pensaba que se habían retirado, sigan siendo accesibles. E incluso entre las API sancionadas y documentadas, puede haber parámetros de API no documentados que es posible explotar. La detección de todas las API norte-sur, este-oeste y salientes es imprescindible. La única forma de garantizar una visibilidad completa de las API en toda la empresa es examinando los datos de actividad de las API existentes, recogidos de una amplia gama de tecnologías y plataformas de nube.

2 ¿Su producto detecta las API de forma continua y, en caso afirmativo, en qué medida es manual este proceso?

Las API aparecen y desaparecen periódicamente debido a los procesos de DevOps en constante cambio. Por lo tanto, los inventarios puntuales de API son insuficientes. Su producto de seguridad de API debe realizar una detección continua para garantizar que las nuevas API documentadas se incluyan en el inventario, se analicen y se protejan. También debe ser capaz de detectar cualquier instancia futura de API en la sombra o zombis. Además, los productos que suponen una carga continua para su equipo porque obligan a interpretar los resultados y actuar en función de ellos no serán sostenibles a largo plazo. Por el contrario, los productos que aplican la automatización y el aprendizaje automático tanto a la detección como a la evaluación de las API mantendrán su empresa en perfecto funcionamiento, en lugar de añadir más tareas manuales a la lista de tareas diarias de su equipo.

3 ¿Cómo ayuda su producto a mis procesos y herramientas de documentación de API?

La integración de su enfoque de documentación con su plataforma de seguridad de API tiene muchas ventajas, por lo que debe verificar que su proveedor cuenta con esta capacidad. Por ejemplo, la carga automática de la documentación de Swagger existente en su plataforma de seguridad de API como parte de su proceso de integración y entrega continua (CI/CD) mejora la precisión de la detección de API en la sombra y la identificación de parámetros en la sombra (si el proveedor tiene la capacidad de comparar los parámetros de API detectados con los parámetros ya documentados). Su plataforma de seguridad también debe tener la capacidad de crear archivos Swagger personalizados simplemente haciendo clic en un botón para cualquier API que carezca de documentación, lo que ayudará a sus desarrolladores a poner en marcha y mejorar sus procesos de documentación.



4 ¿Cuánto tiempo y esfuerzo hará falta para implementar el producto en mi entorno?

La forma más rápida y eficaz de empezar es utilizar un producto de seguridad de API de tipo “seguridad como servicio (SaaS)" capaz de procesar de forma no intrusiva la ingesta y el análisis de los datos de actividad de las API de sus sistemas existentes. Una arquitectura SaaS bien diseñada para la seguridad de API se puede integrar en su entorno en cuestión de minutos, lo que puede acelerar vertiginosamente el tiempo de amortización y eliminar los costes y riesgos continuos asociados a las actualizaciones del sistema. Para lograr una mayor agilidad, busque un proveedor que ofrezca tanto protección de API y aplicaciones web (WAAP) como detección y respuesta de API, de manera que los datos del tráfico de API fluyan sin problemas entre la solución que protege el tráfico entrante y la solución que protege todo el tráfico de API de su organización.

5 ¿Cómo ayuda su producto a identificar y priorizar las API detectadas que son peligrosas?

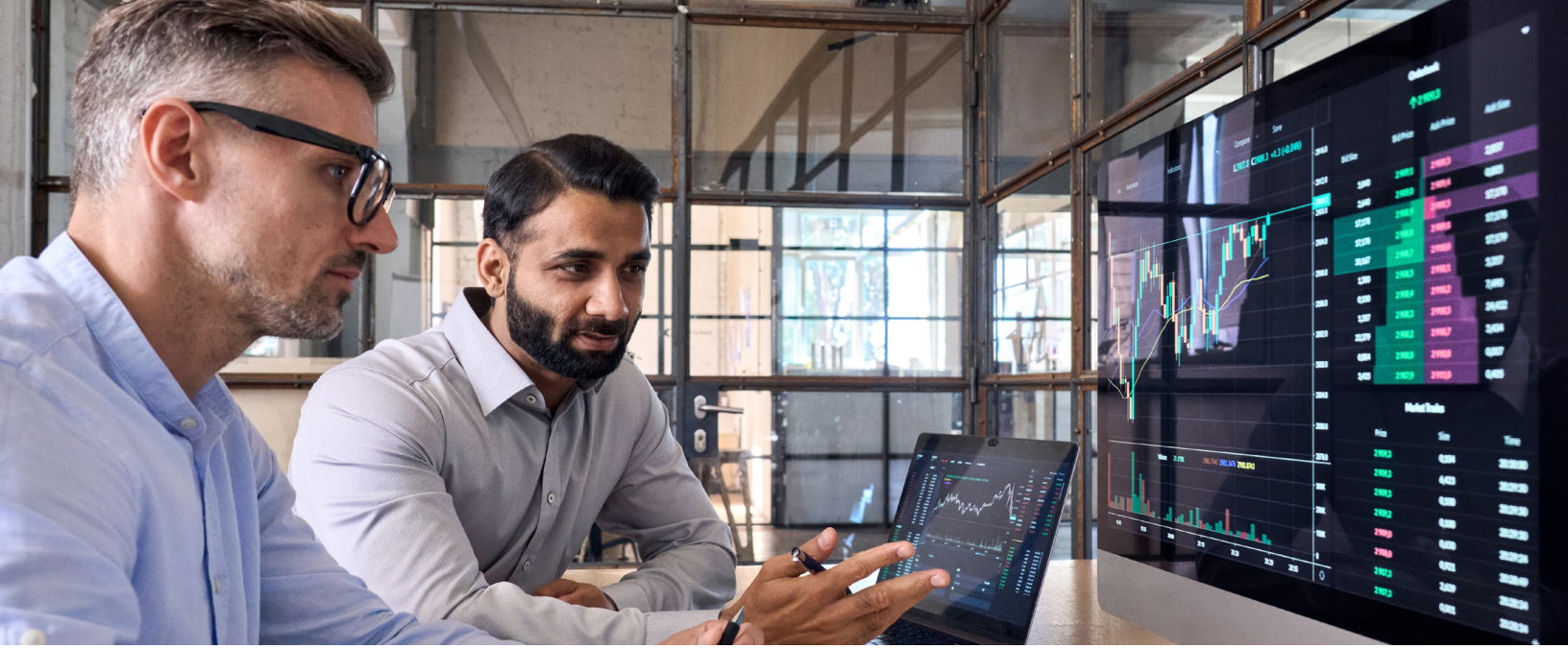
Ver un inventario completo de las API por primera vez puede resultar a la vez estimulante y abrumador. Muchos equipos de seguridad sufren una sobrecarga de información y tienen dificultades para identificar las áreas en las que tienen que centrarse en cuanto respecta a la seguridad de las API. La mejor manera de evitar este problema es seleccionando un producto de seguridad de API que realice gran parte de estas tareas por usted, entre las que se incluyen:

- Destacar la presencia de API que permiten acceder a datos confidenciales
- Etiquetar automáticamente los datos confidenciales por tipo (por ejemplo, información de identificación personal, direcciones de correo electrónico, datos de tarjetas de crédito, etc.)

Su plataforma de seguridad de API también debe permitirle crear categorías de etiquetado personalizadas para que los equipos encargados de las API y la seguridad hablen un lenguaje común que se adapte a sus objetivos empresariales y a sus preocupaciones en materia de seguridad.

6 ¿Su producto utiliza análisis de comportamiento para establecer un estándar previsto y detectar posibles anomalías?

Se pueden detectar muchos tipos de ataques mediante el uso de firmas de ataque para bloquearlos en el nivel WAAP. Sin embargo, muchos tipos de ataques incluidos en la lista 10 principales vulnerabilidades de seguridad de API del Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP) de 2023, como la autorización a nivel de objeto comprometida, no se pueden detectar de esa manera. Estos tipos de ataques son más pasivos y se centran en el abuso de la lógica empresarial, por lo que son más difíciles de detectar. La única forma de defenderse eficazmente contra todos los vectores de amenaza de API es mediante el análisis de comportamiento y el aprendizaje automático. El verdadero análisis de comportamiento requiere grandes conjuntos de datos, algoritmos de aprendizaje automático que aprendan las características específicas de su entorno y la flexibilidad y agilidad necesarias para actualizarse y adaptarse automáticamente a partir de la información global. Un modelo SaaS es la única forma práctica de realizar estas actividades a escala.



7 ¿Puede capturar y analizar conjuntos de datos que sean lo suficientemente significativos para establecer de forma eficaz un estándar de comportamiento normal y detectar posibles anomalías?

Muchos productos de seguridad de API se centran en la supervisión de llamadas de API individuales o, en el mejor de los casos, en la actividad de sesiones a corto plazo. Esto es insuficiente, ya que muchos procesos empresariales legítimos (y muchos ataques) se producen durante un periodo mucho más largo. El uso de API debe analizarse en un periodo temporal variable (30 días como mínimo). Esto proporciona una referencia más completa y precisa del comportamiento esperado, incluidos los procesos empresariales que solo se producen una vez al mes (por ejemplo, la facturación). También permite detectar ataques que se ejecutan de forma lenta durante varios días o semanas, así como numerosas sesiones de API.

8 ¿Puede su producto identificar cada entidad, relación y actividad dentro de los datos de API sin procesar para proporcionar un contexto empresarial?

La mejor forma de hacer que los datos de actividad de las API sean procesables es enriqueciéndolos con contexto sobre las implicaciones empresariales del uso de las API. Las siguientes capacidades de identificación y etiquetado son esenciales para que su plataforma de seguridad de API evalúe y elabore perfiles de las relaciones entre las diferentes entidades:

- Representaciones de usuarios de API (entidades de usuario), como direcciones IP, claves de API, tokens de acceso, ID de usuarios, ID de partners, ID de comerciantes, ID de proveedores, etc.
- Representaciones de procesos empresariales (entidades de procesos empresariales), como reservas, pagos, facturación, saldo de cuentas, etc.

El análisis detallado a este nivel es la única forma de convertir la gran cantidad de datos generados por las API en una referencia significativa y comprensible del comportamiento esperado.

9 ¿Puede su producto trazar en un formato cronológico cada actividad de cada entidad en sus API para mostrar los cambios de comportamiento a lo largo del tiempo?

Aunque es fundamental comprender y supervisar la actividad de las API y las amenazas en un nivel general, la capacidad de limitar el enfoque del análisis a entidades específicas es igual de importante. Por ejemplo, si se identifica un comportamiento anómalo para un partner comercial específico, la capacidad de ver toda la actividad de esa entidad en un formato cronológico tiene un valor incalculable. Lo mismo ocurre con las entidades de procesos empresariales. Ver la historia completa de lo que ocurrió y cuándo ocurrió en un formato cronológico para cada entidad dentro de sus API es una visualización potente que muestra a la perfección la historia del uso normal y el abuso de la lógica empresarial. La capacidad de rebobinar la actividad para ver lo que ocurrió antes y después de una alerta es una herramienta poderosa que le ayudará a entender el abuso de la lógica empresarial.

10 ¿Cómo puedo integrar su producto con las herramientas, los procesos y los flujos de trabajo existentes?

El envío de alertas a su producto de gestión de eventos e información de seguridad (SIEM) es útil, pero es solo un punto de partida. Cada vez más, los equipos de seguridad utilizan herramientas más sofisticadas de orquestación, automatización y respuesta de seguridad (SOAR) para iniciar flujos de trabajo predefinidos cuando se detectan amenazas e incidentes. Además, dado que muchos problemas de seguridad de API requieren la intervención de desarrolladores externos al equipo de seguridad, su plataforma de seguridad de API también debe integrarse con las herramientas de seguimiento de problemas y gestión del flujo de trabajo del equipo de desarrollo. Si su herramienta de seguridad está analizando el tráfico de API, tiene sentido que también utilice las API para ayudar a organizar las respuestas en su red de distribución de contenido (CDN), firewall de aplicaciones web o puerta de enlace de API, y permitirle crear sus propias guías.

11 ¿Puedo consultar los datos de su producto relativos a la actividad y las API para buscar amenazas y mitigar los riesgos de forma proactiva?

Las integraciones de herramientas de seguridad y desarrollo no pueden ser simplemente cajas negras que envían alertas unidireccionales a sus soluciones. Sus equipos de seguridad y API necesitan poder aprovechar los datos de origen que hay detrás de una alerta o un problema. Busque plataformas de seguridad de API que permitan a los usuarios consultar detalles de API directamente a través de una interfaz web integrada o a través de API que permitan la integración de la plataforma de seguridad de API con otras de sus herramientas e interfaces preferidas. Esto permitirá a su equipo de seguridad llevar a cabo una búsqueda proactiva de amenazas de forma eficiente y eficaz. También ayudará a los desarrolladores y a otras partes interesadas no relacionadas con la seguridad a comprender cómo se dirigen los atacantes a las API mientras se utilizan de forma legítima.

12 ¿Qué medidas toma para garantizar la protección de los datos confidenciales que recopila sobre mi empresa?

Los análisis de comportamiento avanzados necesarios para proteger las API en el panorama de amenazas actual solo son posibles con la escala de la nube. Dado el tamaño y la confidencialidad de su conjunto de datos de API, es importante que exija a su proveedor de seguridad que garantice la protección de los mismos. Es importante verificar las prácticas que utiliza su proveedor para proteger su infraestructura de nube, pero eso es solo el punto de partida. Solicite a su proveedor de seguridad de API que utilice técnicas como la tokenización, es decir, que sustituya los datos confidenciales por tokens anónimos antes de transmitirlos a la nube. Esto garantiza la privacidad de los datos incluso si el proveedor, o su proveedor de nube original, se enfrenta a un incidente de seguridad.

13 ¿La solución proporciona acceso detallado a los datos de actividad de API?

Los datos son un elemento estratégico crucial para todo, desde el cumplimiento hasta el contexto, para la prevención de ataques. Muchos proveedores ofrecen su propia versión para el almacenamiento de los datos de API a lo largo del tiempo, pero debe comprender bien qué ofrecen realmente. Las soluciones que solo envían alertas no ofrecen una panorámica completa de la situación, ya que la actividad de las API vulneradas puede seguir desarrollándose lentamente a lo largo de un periodo de tiempo, no solo cuando se genera una alerta. En cambio, un proveedor de una solución integral eliminará los puntos ciegos registrando toda la actividad de las API y proporcionará las herramientas necesarias para revisar esa actividad en detalle, en lugar de pasarla por alto en un modelo de aprendizaje automático impreciso. Es importante disponer de este acceso detallado a los datos, ya que así podrá supervisar de forma proactiva las amenazas en lugar de reaccionar de forma retroactiva después de que se genere una alerta de ataque.

13 preguntas que debe hacer a su proveedor de seguridad de API

1. ¿Su solución de seguridad de API es capaz de detectar las API en toda la empresa?
2. ¿Su producto detecta las API de forma continua y, en caso afirmativo, en qué medida es manual este proceso?
3. ¿Cómo ayuda su producto a mis procesos y herramientas de documentación de API?
4. ¿Cuánto tiempo y esfuerzo hará falta para implementar el producto en mi entorno?
5. ¿Cómo ayuda su producto a identificar y priorizar las API detectadas que son peligrosas?
6. ¿Su producto utiliza análisis de comportamiento para establecer un estándar previsto y detectar posibles anomalías?
7. ¿Puede capturar y analizar conjuntos de datos que sean lo suficientemente significativos para establecer de forma eficaz un estándar de comportamiento normal y detectar posibles anomalías?
8. ¿Puede su producto identificar cada entidad, relación y actividad dentro de los datos de API sin procesar para proporcionar un contexto empresarial?
9. ¿Puede su producto trazar en un formato cronológico cada actividad de cada entidad en sus API para mostrar los cambios de comportamiento a lo largo del tiempo?
10. ¿Cómo puedo integrar su producto con las herramientas, los procesos y los flujos de trabajo existentes?
11. ¿Puedo consultar los datos de su producto relativos a la actividad y las API para buscar amenazas y mitigar los riesgos de forma proactiva?
12. ¿Qué medidas toma para garantizar la protección de los datos confidenciales que recopila sobre mi empresa?
13. ¿La solución proporciona acceso detallado a los datos de actividad de API?

Como puede que ya haya adivinado, Akamai API Security puede ofrecer de forma eficaz las protecciones recomendadas en esta lista. Explore nuestra solución.

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 seguridad, informática y distribución de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn. Fecha de publicación: 12/23.