La guía definitiva para gestionar su estrategia de seguridad de las API

Índice

La creciente importancia de la seguridad de API

Las API dan a los desarrolladores la eficiencia que necesitan para trabajar en una profesión donde la velocidad no es negociable. Sin embargo, aunque les resultan fáciles de usar y son clave para la interoperabilidad de los activos de software y datos, la seguridad de estas API se ha quedado atrás con respecto a las últimas innovaciones.

El 84 % de las organizaciones ha experimentado un incidente de seguridad API en los últimos 12 meses, frente al 78 % registrado en 2023.[1] En parte, esto se debe a que las API también mejoran la eficiencia de los atacantes. Muchas API se crean con configuraciones incorrectas, errores de codificación y falta de controles de autenticación. Como resultado, atacar una API puede ser bastante simple y una forma directa de robar datos.

Y cuando se trata de datos, solo el 27 % de las empresas con inventarios de API completos saben qué API devuelven datos confidenciales (desde datos sobre clientes hasta propiedad intelectual), frente al 40 % de 2023.[2] Con el aumento de estos ataques y la disminución de la visibilidad, las empresas necesitan una forma de evaluar y mejorar su estrategia de seguridad de API.

1, 2. Akamai, "Estudio sobre el impacto de la seguridad de API", 2024

Cómo es una estrategia de seguridad integral de API

Cuanto mayor es el uso de las API, mayor es su superficie de ataque, lo que da lugar a nuevos retos de seguridad.

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 cierta protección. Pero, a medida que su infraestructura de API se hace más compleja (por ejemplo, abarcando una gran cantidad de API no administradas que son difíciles de ver y proteger), la estrategia de seguridad debe cambiar.

Las API merecen un papel principal en el plan de protección empresarial. Una solución de seguridad específica para las API, diseñada para hacer frente a los riesgos y métodos de ataque actuales, puede proporcionar la visibilidad y las capacidades necesarias para ejecutar ese plan. No es diferente al concepto de defensa en profundidad, donde las herramientas se complementan entre sí para cubrir cada paso de la ruta de ataque.

Una plataforma de seguridad de API completa, diseñada para detectar todas estas API, gestionar la estrategia, proteger el tiempo de ejecución y realizar pruebas de seguridad, puede ayudarle a ver los riesgos ocultos de las API, identificar las rutas de ataque asociadas y mitigar las amenazas descubiertas en tiempo real.

En nuestro eBook relacionado, La guía definitiva para la detección de API, explicamos el primer elemento crítico de la seguridad de las API: localizarlas. Una vez que haya detectado e inventariado todas las API que se utilizan en toda su organización, el siguiente paso es mejorar su estrategia general de seguridad de API.

La gestión de la estrategia es especialmente importante para las empresas que compran aplicaciones de proveedores externos y después las usan, les ponen su marca y las venden como propias. Por ejemplo, la telemática de casi todos los automóviles nuevos en los últimos cinco años funciona prácticamente igual. Si un atacante encuentra vulnerabilidades en los terminales de API de un fabricante, consigue un punto de entrada sencillo para usurpar cuentas de usuario y provocar filtraciones de datos.

Contenido de esta guía

La gestión de la estrategia de las API le proporciona las herramientas necesarias para gestionar, supervisar y mantener la seguridad durante todo el ciclo de vida de las API. Esta guía definitiva se centra en los requisitos clave para la gestión de estrategias de seguridad de las API, incluidas la detección de vulnerabilidades y la protección de datos sensibles. En ella, se analizan métodos de gestión de estrategias y se presentan las capacidades de gestión de estrategias de la solución Akamai API Security.

La utilidad de gestionar su estrategia

La gestión de la estrategia de las API garantiza que tome las mejores decisiones para proteger sus API. Le ayuda a comprender el riesgo de las API detectadas identificando qué tipo de datos manejan, si presentan alguna vulnerabilidad o configuración errónea, si están correctamente autenticadas y otros parámetros. Poder identificar vulnerabilidades de API y solucionarlas rápidamente le permite tomar medidas correctivas para prevenir un ataque.

Una gestión de la estrategia completa proporciona visibilidad de toda la actividad en torno a las API para que pueda aplicar políticas de seguridad, garantizar el cumplimiento de las normativas y auditar los cambios en su ecosistema de API. Protege sus API frente a

Tan solo el 27 % de las empresas con inventarios de API completos conocen cuáles transfieren datos confidenciales, en comparación con el 40 % en 2023.[3]

3. Akamai, "Estudio sobre el impacto de la seguridad de API", 2024

ataques, usuarios no autorizados y filtraciones de datos que pueden provocar daños significativos a la reputación, pérdida de oportunidades de negocio y sanciones legales.

Aplicar las mejores prácticas de gestión de la estrategia minimiza la superficie de ataque de las API y mitiga gran parte del riesgo. Crear inventarios exhaustivos de API y almacenar los datos sensibles de su organización es esencial para una buena gestión. En la siguiente página, veremos los elementos adicionales de la gestión de la estrategia de las API: detección de vulnerabilidades, supervisión de API y solución de problemas.

- ## Detección de vulnerabilidades

  Análisis: inspeccione el código fuente en busca de debilidades comunes, comprenda cómo interactúa una API con sistemas externos y evalúe sus características de autorización y autenticación.

  Observación: inspeccione el tráfico de entrada y salida de una API para identificar configuraciones erróneas, detectar vulnerabilidades y comprender el comportamiento de las API estándar.

La gestión de la estrategia es solo una pieza de un programa completo de seguridad de API. También es fundamental realizar pruebas integrales en la preproducción para evitar que las vulnerabilidades lleguen a la fase de producción.

- ## Supervisión de API

  Identifique y supervise las llamadas a API en producción, realice un seguimiento de las solicitudes de API, detecte desviaciones del uso estándar y cree alertas cuando el uso de API supere los umbrales predefinidos.

- ## Corrección

  Resuelva las debilidades o vulnerabilidades identificadas a través de cambios en el código, ajustes de seguridad o parches para fallos de API a fin de mejorar la seguridad y el cumplimiento de una API. Una buena gestión de la estrategia favorece la corrección de problemas antes de que se explote una vulnerabilidad.

Las funciones imprescindibles para la gestión de la estrategia

Puede que sospeche, o que sepa con certeza, que su estrategia de seguridad de API podría mejorarse. A continuación, le presentamos algunas funciones imprescindibles que deberían incluir sus herramientas de gestión.

- **Clasificación de datos confidenciales**
  Una API que suministra datos meteorológicos de fuentes públicas es mucho menos preocupante que una que transmite información de tarjetas de crédito. Las herramientas de gestión de la estrategia de las API deben poder identificar rápidamente cuántas API tienen acceso a datos de tarjetas de crédito, números de teléfono, números de la seguridad social y otros datos confidenciales, junto con el número de usuarios que han accedido a datos confidenciales a través de las API que utiliza.
- **Evaluación de la configuración**
  Muchos ciberatacantes consiguen acceder debido a un simple error de configuración de las redes, las puertas de enlace de API o los firewalls que actúan como intermediarios y protegen el tráfico de las API. Una buena gestión de la estrategia debe poder escanear configuraciones de infraestructura y software regularmente, incluidos archivos de registro y de configuración. Este escaneo periódico ayuda a detectar configuraciones erróneas y vulnerabilidades, e identifica los riesgos creados por desviaciones de configuración.
- **Puntuación de confianza para los ataques**
  Busque un motor de puntuación de confianza para los ataques que utilice algoritmos avanzados de aprendizaje automático entrenados para evaluar señales externas e internas, incluido el comportamiento de las API, patrones de tráfico de red, datos de

geolocalización, fuentes de inteligencia sobre amenazas y otros factores contextuales. Esto puede ayudarle a determinar el nivel de certeza de que un incidente detectado en tiempo de ejecución provenga de una actividad maliciosa. Esta capacidad única permite a los clientes centrarse rápidamente en las amenazas críticas y crear flujos automáticos de corrección y notificación para ataques de alta probabilidad.

- **Flujos de trabajo personalizados**
  Junto con el nivel de gravedad personalizable, debe poder crear flujos de trabajo para tomar medidas de inmediato cuando se detecten vulnerabilidades. Estos flujos de trabajo pueden ser, por ejemplo, crear tickets sobre incidencias, notificar a los principales interesados o actualizar la configuración de red.

- **Documentación generada automáticamente**
  La documentación de las API indica a los usuarios para qué sirven y cómo utilizarlas. Las API seguras se deben evaluar para garantizar el cumplimiento de las especificaciones y deben estar bien documentadas. Una documentación deficiente o inexistente dificulta las pruebas de seguridad, lo que aumenta el riesgo de que una API llegue a producción sin que se detecte una vulnerabilidad.

Este problema se ve agravado a menudo por la externalización del desarrollo de las API. Independientemente de la raíz del problema, su programa de seguridad de las API no debe contener documentación desfasada, incompleta o inexistente.

La especificación OpenAPI (anteriormente denominada Swagger) define descripciones de interfaces estándar. Las herramientas de gestión de la estrategia deben poder generar automáticamente documentación completa de OpenAPI basada en el estado actual y futuro de las API para ayudar a garantizar que todas ellas estén debidamente documentadas y que la documentación esté actualizada.

Una aseguradora líder mejora la estrategia de seguridad de las API con Akamai

A medida que los consumidores se alejan de las oficinas físicas y se decantan por lo digital, las empresas de servicios financieros deben innovar a un ritmo acelerado. Aflac, el proveedor líder de seguros de salud suplementarios en Estados Unidos, tenía cada vez más dificultades para hacer frente a los crecientes retos en seguridad de API, como muchas otras empresas.

Finalmente, recurrió a la plataforma API Security de Noname (ahora parte de Akamai API Security) para resolver el problema. El módulo de gestión de la estrategia ayuda al equipo a identificar los tipos de datos que fluyen a través de las API de la empresa, proporciona visibilidad sobre qué API acceden a los datos confidenciales e identifica cualquier anomalía en el acceso a los datos.

Lea el caso real completo de Aflac para obtener más información.

> "Sabíamos que nuestra presencia de API era grande y queríamos estar completamente seguros de que teníamos controladas todas ellas, de que teníamos plena visibilidad de su funcionamiento y de que se prueban continuamente para detectar riesgos de seguridad.
>
> — DJ Goldsworthy, vicepresidente, Operaciones de Seguridad y Gestión de Amenazas de Aflac

El enfoque de Akamai para la gestión de la estrategia

El módulo de gestión de la estrategia de Akamai API Security proporciona una visión integral del tráfico, el código y las configuraciones para evaluar el nivel de seguridad de sus API. Akamai determina la verdadera magnitud de la superficie de ataque de sus API y aplicaciones web, y descubre todos los tipos de datos confidenciales que se mueven a través de las API para ayudarle a protegerlos.

Hasta los más simples errores de configuración de las API pueden dejar desprotegida a su empresa frente a los ciberdelincuentes. Una vez dentro, los hackers pueden acceder rápidamente a los datos confidenciales y extraerlos. El módulo de gestión de la estrategia de Akamai API Security incluye estas características clave:

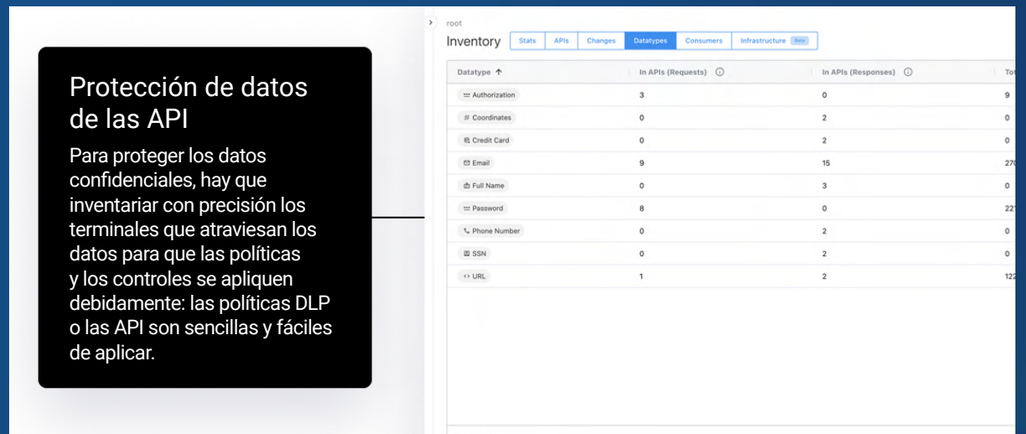
- Integración fuera de banda para la detección continua de API en las instalaciones y en nubes híbridas y públicas
- Un inventario de API simple y con funciones de búsqueda que incluye detalles de esquema, ubicación de red y tipos de datos
- Generación automatizada de documentación de API (OAS/Swagger)
- Análisis contextual de las configuraciones erróneas y vulnerabilidades de las API con priorización
- Detección de las 10 vulnerabilidades principales de seguridad de las API según OWASP
- Detección y clasificación automatizadas de datos confidenciales y cambios en las API

Exposición de las API

Además de detectar los riesgos dentro del código de una API, también es importante identificar el tráfico observando su comportamiento (típico versus atípico), así como dentro del contexto de la red.

La gestión de la estrategia de la solución Akamai API Security analiza el conjunto más amplio posible de fuentes para detectar vulnerabilidades, lo que incluye los archivos de registro, las repeticiones del tráfico histórico, los archivos de configuración y muchos otros elementos. La solución detecta las 10 vulnerabilidades principales de seguridad de las API según OWASP y protege las API frente a filtraciones de datos, problemas de autorización, abuso, uso indebido y corrupción de datos.

Akamai identifica y prioriza de forma inteligente las vulnerabilidades potenciales, que se pueden remediar manualmente, semiautomáticamente, o de forma totalmente automática a través de integraciones en WAF, puertas de enlace de API, herramientas SIEM e ITSM, herramientas de flujo de trabajo y otros servicios.



Protección de datos de las API

Para proteger los datos confidenciales, hay que inventariar con precisión los terminales que atraviesan los datos para que las políticas y los controles se apliquen debidamente: las políticas DLP o las API son sencillas y fáciles de aplicar.

El cumplimiento está adquiriendo una dimensión completamente nueva con el creciente uso de las API, y el aumento de la superficie de ataque ha acarreado una nueva ola de normativas. Los sectores regulados ahora deben tener en cuenta las API en sus planes de cumplimiento.

El módulo de gestión de la estrategia de Akamai API Security identifica todas las formas de datos confidenciales que se mueven a través de sus API, incluida toda la información de identificación personal (PII), como tarjetas de crédito, SSN, direcciones, información de seguros y más. Con el fin de garantizar que estos datos estén protegidos y en el lugar correcto, se reduce el acceso a este tipo de datos y se implementa un marco de gestión de los mismos.

Cómo le puede ayudar la gestión de la estrategia de las API

Cada vez que un cliente, partner o proveedor interactúa digitalmente con su empresa, existe una API en segundo plano que facilita un intercambio de datos que, a menudo, son confidenciales. Tener visibilidad de todas las API de su organización y evaluar sus atributos de riesgo (por ejemplo, qué API devuelven datos confidenciales) puede ayudarle a protegerla contra un vector de ataque que aumenta rápidamente. La gestión de la estrategia de seguridad de las API también puede ayudarle a garantizar el cumplimiento de las regulaciones globales que tienen como objetivo evitar las filtraciones de datos.

Obtenga información sobre las regulaciones de protección de datos que requieren la detección y protección de todas las API.

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 **www.akamai.com** y **www.akamai.com/blog**, o siga a Akamai Technologies en **X**, antes conocido como Twitter, y **LinkedIn**. Publicado en diciembre de 2024.

Akamai