

Seguridad y gobernanza de API integradas con IBM API Connect y DataPower

Las esperanzas y desafíos de las API

Las API han sido el motor de la transformación digital, ya que permiten a empresas de todos los sectores crear nuevos servicios y modelos de negocio para acelerar su crecimiento. Sin embargo, a medida que las API proliferan, también lo hacen sus riesgos.

- Aunque las empresas y sus responsables de ingeniería han adoptado e integrado rápidamente las API, gestionarlas de forma eficaz sigue suponiéndoles un reto.
- En la carrera por crear y lanzar nuevas aplicaciones y servicios mejorados con IA cuanto antes, las API de base a menudo contienen errores de configuración, codificación y problemas de lógica empresarial.
- Cada vez que un cliente, partner o proveedor interactúa digitalmente con su empresa, hay una API en segundo plano que facilita el intercambio de unos datos que suelen ser confidenciales, como bien saben los atacantes.

Como resultado, las API han llegado a ser uno de los principales vectores de ataque, con grandes riesgos. Los ataques a las API pueden poner en peligro los ingresos, la resiliencia y el cumplimiento normativo de una empresa.

Para hacer frente a este desafío, las empresas deben aplicar un enfoque que abarque todo el ciclo de vida, tanto desde el punto de vista de la gobernanza como del de la seguridad, y que incluya los procesos de diseño, desarrollo, pruebas, implementación, funcionamiento y corrección de problemas. Juntos, Akamai API Security e IBM permiten a las empresas desarrollar, implementar y gestionar sus API rápidamente y con confianza para responder ante estas situaciones y adaptarse al crecimiento del negocio.

Desafíos

-  Mantener un inventario de API de toda la infraestructura y detectar API desconocidas
-  Identificar API vulnerables, con errores de configuración o que no cumplan la normativa
-  Detectar y detener el uso indebido o malintencionado de las API, incluidos los ataques de lógica empresarial
-  Crear API seguras y coherentes sin renunciar a la velocidad ni la agilidad
-  Adaptar y supervisar los programas de seguridad y gobernanza de API

Cómo ayudan Akamai e IBM a sus clientes

Conozca sus API

No se puede proteger lo que no se puede ver. Con Akamai API Security puede detectar automáticamente las API, los dominios y los problemas, y crear un inventario detallado de las API que permita verlas todas en su conjunto. Normalmente, las empresas encuentran muchas más API de las que pensaban que tenían o esperaban encontrar. También puede encontrar fácilmente información útil, como datos filtrados, para conocer las posibles rutas de ataque. Además, tendrá a su disposición una integración perfecta con los elementos de infraestructura más comunes relacionados con las puertas de enlace de API y las plataformas de gestión para garantizar el intercambio sistemático de los datos de seguridad en toda la empresa.

Refuerce su estrategia de seguridad y gobernanza

Adapte sus operaciones y aplique las prácticas recomendadas al utilizar Akamai API Security para la gobernanza de las API:

- Conozca todas las API de su ecosistema con un contexto empresarial completo y adapte las a las prácticas recomendadas de gestión de API.
- Optimice las comunicaciones entre los equipos de desarrollo y seguridad.
- Detecte vulnerabilidades, como errores de configuración o API que violen sus políticas.
- Proteja los datos confidenciales y supervise los cambios de forma proactiva para reducir el riesgo en sus API.



Detenga el uso indebido de las API y los ataques contra ellas con la protección del tiempo de ejecución

Localice y bloquee los ataques a las API de principio a fin. Evite la filtración y la manipulación de datos, las infracciones de políticas de datos, los comportamientos sospechosos... gracias al análisis del tráfico en tiempo real, la supervisión fuera de banda, las opciones de corrección en línea y la integración de flujos de trabajo para aumentar la eficacia del centro de operaciones de seguridad (SOC).

Proporcione API seguras más rápido con Active Testing

Integre fácilmente las pruebas de seguridad de API en cada fase de su ciclo de desarrollo y detecte vulnerabilidades, errores de configuración y problemas de cumplimiento normativo antes de incorporar dichas API al ciclo de producción. Con Active Testing, el personal de operaciones de seguridad y desarrollo (DevSecOps) puede ejecutar más de 200 pruebas de seguridad centradas en las API, bajo demanda o como parte de los procesos de integración y entrega continua (CI/CD) de la empresa. Active Testing identifica y prueba todas las API según la lógica empresarial subyacente de la aplicación, lo que permite a los desarrolladores detectar vulnerabilidades complejas que otras herramientas de prueba podrían pasar por alto.

Akamai ofrece una integración eficiente que ofrece visibilidad y protección a los usuarios de IBM

Akamai API Security se integra con API Connect y DataPower en varias plataformas de nube y opciones de implementación. Además, cuando API Connect gestiona DataPower, los cambios de configuración son independientes en todos los sistemas. De esta forma, la eficiencia operativa es mayor y se reduce el riesgo de llevar a cabo actividades de desarrollo no autorizadas o que no cumplan la normativa.

Gestión y respuesta fluidas en caso de ataque

Por otra parte, los clientes de IBM DataPower pueden observar la detección y el bloqueo de amenazas casi en tiempo real sin que afecte a su rendimiento ni latencia, y sin tener que instalar complementos adicionales en las puertas de enlace de DataPower. Todo gracias a la integración con Akamai API Security.

IBM API Connect evalúa las solicitudes de acceso a los recursos según las políticas de autorización de Akamai API Security y aplica las reglas de bloqueo en los clústeres de IBM DataPower. Así, se reducen los tiempos de corrección de días a minutos o, incluso, a segundos.

Plataformas de desarrollo



Red y nube



Integraciones de flujos de trabajo



Ecosistema



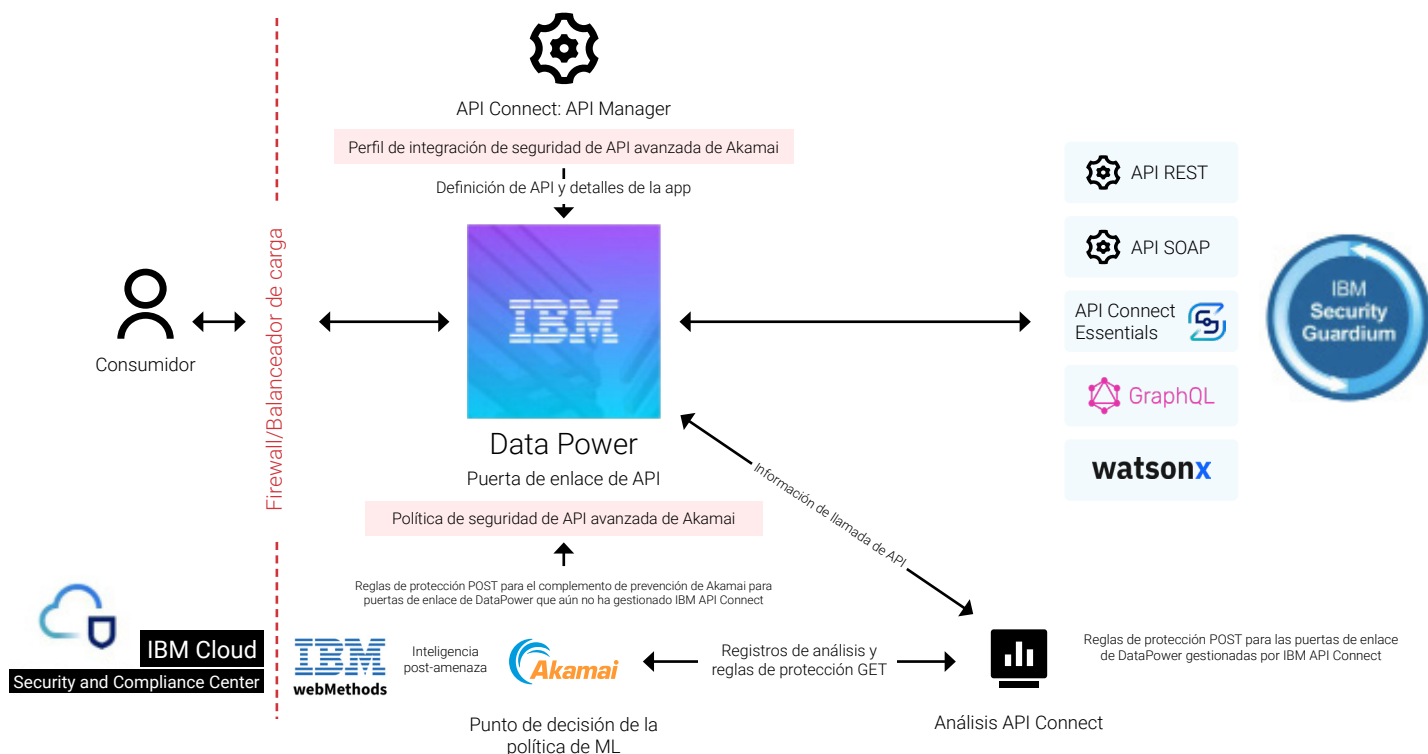
IBM API Connect

Puerta de enlace de API



Combine la potencia de IBM webMethods y Akamai API Security para lograr una gestión y protección de API sin precedentes. Esta colaboración ofrece una solución completa que combina la detección de API avanzada de Akamai con la precisa gestión e integración de datos en tiempo real de IBM webMethods. Disfrute de plena visibilidad y control sobre todas sus API para garantizar la seguridad y la conformidad. Esta integración no solo fortalece sus defensas, sino que también aumenta la eficiencia y permite a su empresa responder de forma rápida y segura frente a los cambios en las demandas del mercado.

Por último, los clientes de IBM DataPower pueden aprovechar la integración de Akamai con eBPF Red Hat OpenShift para detectar API que API Connect o DataPower aún no han gestionado, lo que les permite encontrar y proteger aquellas que procesan transacciones de alto riesgo y datos confidenciales. Estas funciones van más allá de las configuraciones locales, de nube e híbridas, y son compatibles con Amazon Web Services (AWS), Microsoft Azure y Google Cloud Platform (GCP).



Siguientes pasos

Las API son una fuerza motriz que estimula la capacidad de las organizaciones para satisfacer las necesidades de los clientes, generar ingresos y competir en una economía digital que evoluciona rápidamente. Sin embargo, su crecimiento continuo, su proximidad a los datos y la infinidad de vulnerabilidades actuales las convierte en un atractivo objetivo para los atacantes. Dado que los incidentes relacionados con la seguridad de las API aumentan constantemente, es esencial disponer de funciones que le permitan ver, proteger y probar todas las API de su organización. La colaboración entre IBM y Akamai ofrece a las empresas la fiabilidad necesaria para crear, mantener y utilizar sus API de forma segura y a escala.

Descubra cómo podemos ayudarle con esta [demostración de Akamai API Security personalizada](#). También puede ponerse en contacto con IBM para obtener más información.