CEQUENCE

FICHA DE DATO

Protección Unificada de Aplicaciones de Cequence

Plataforma de protección de aplicaciones, APIs e IA

A medida que las organizaciones trasladan cada vez más su infraestructura a la nube, la cantidad de aplicaciones y sus APIs asociadas ha aumentado drásticamente, y los riesgos de seguridad han crecido en la misma medida. Estas aplicaciones están expuestas a ataques de bots, abuso, fraude y pérdida de datos, y aún más en la era de la IA agéntica, donde los ataques potenciados por IA pueden aprender y evolucionar por sí mismos. Las organizaciones necesitan soluciones que protejan sus aplicaciones y APIs hoy y en el futuro.

Desafíos de seguridad de API y gestión de bots

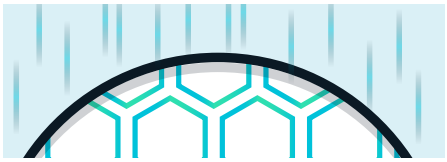
Las organizaciones actuales enfrentan desafíos únicos y multifuncionales al momento de proteger aplicaciones y APIs críticas contra ciberataques. No se trata solo de un problema de TI o de seguridad; los ataques maliciosos de bots a aplicaciones y APIs pueden afectar el comercio electrónico, la satisfacción del cliente, el marketing, la analítica de ventas y más. Un programa eficaz de gestión de bots y seguridad de APIs es esencial para proteger tanto al negocio como a sus clientes.

Disipe la niebla

Las APIs se desarrollan y despliegan de forma rutinaria por equipos dispersos y a gran velocidad, en entornos híbridos de on-premises y nube, creando una "niebla de guerra" que oculta la visibilidad. TI necesita saber qué APIs existen, dónde están, quién tiene acceso y asegurarse de que cuenten con especificaciones precisas.

Mantenga una buena postura

Los equipos de seguridad y desarrollo no siempre tienen una visión clara y consistente de la postura de seguridad de sus APIs en todo el portafolio de aplicaciones. Entender dónde puede explotarse una vulnerabilidad crítica, una exposición de datos sensibles o un fallo de lógica de negocio permite remediar con precisión las áreas de mayor riesgo.



Proteja el núcleo

Las aplicaciones y APIs son constantemente examinadas por atacantes que buscan cualquier oportunidad para explotar y comprometer a su organización. La capacidad de detectar y bloquear los ataques en tiempo real puede evitar que las organizaciones sufran fraudes, filtración de datos y interrupciones en el negocio.

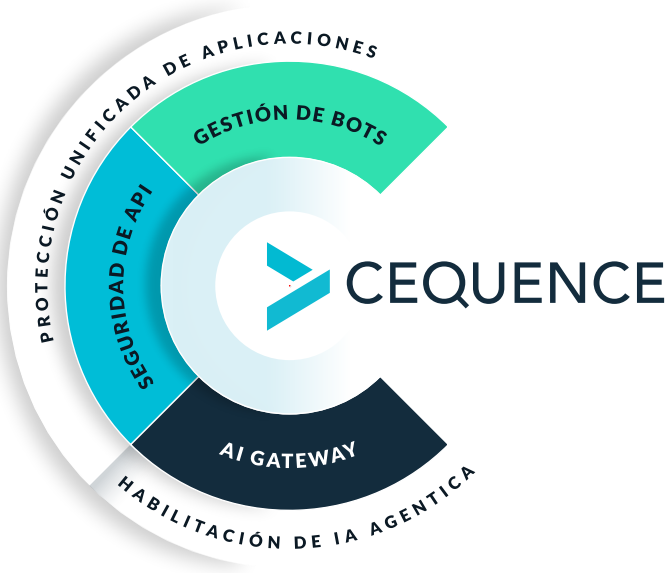
Los responsables de seguridad se plantean ahora preguntas fundamentales:

1. ¿Cuántas API tengo y dónde están?
2. ¿Qué riesgos plantean mis API?
3. ¿Puedo proteger *todas* mis aplicaciones y API?
4. ¿Están siendo atacadas mis aplicaciones y API?

Responder a estas preguntas es fundamental para un programa de seguridad sólido, una tarea que se hace más difícil debido a la naturaleza del negocio. El lanzamiento de nuevos productos, el crecimiento orgánico y las adquisiciones exigen una solución capaz de seguir el ritmo de este cambio constante.

Plataforma de protección aplicaciones unificada de Cequence

La plataforma Cequence Unified Application Protection (UAP) unifica el descubrimiento, el cumplimiento y la protección para defender las aplicaciones y APIs de una organización contra ataques, abuso de lógica empresarial y fraude. Cequence UAP garantiza la inutilidad, el fracaso y el agotamiento incluso para los atacantes más persistentes. Mejora significativamente la visibilidad y la protección, al tiempo que reduce los costos, el fraude, la pérdida de datos, el incumplimiento y las interrupciones del negocio. Cequence UAP ofrece valor en minutos, no en días o semanas, y proporciona un modelo de implementación flexible que no requiere instrumentación ni modificación de las aplicaciones.



DESCUBRE

Descubrimiento de la superficie de ataque de la API

Descubra APIs Internas y Externas | Alerta y Monitoreo de Cambios

Descubra e inventarie toda la huella de APIs de su organización, catalogando APIs internas, externas y de terceros. Forme una imagen coherente de su superficie de ataque públicamente accesible, brindándole la perspectiva del atacante. Cequence revela continuamente nuevos hosts de API, endpoints y proveedores de hosting para que los equipos de seguridad y cumplimiento conozcan su existencia.

CUMPLE

Gestión de la seguridad de las API

Monitoree la Postura Continuamente | Pruebe APIs en Preproducción | Remedie Riesgos

Gestione la postura de seguridad de API de su organización, asegurando que toda su huella de API cumpla con las normativas, se ajuste a las especificaciones, los requisitos de pruebas de seguridad y las mejores prácticas de gobernanza. La creación autónoma de pruebas de API identifica vulnerabilidades y previene la filtración de datos sensibles antes de la producción.

PROTEGE

Gestión de bots y prevención del fraude

Bloquee Ataques a Aplicaciones y APIs | Prevenga Robo, Abuso de Lógica Comercial y Fraude

Identifique y mitigue bots, evitando fraudes y protegiendo su organización y sus aplicaciones contra toda la gama de ataques automatizados Sin necesidad de agentes, JavaScript o SDKs, las huellas digitales de comportamiento multidimensionales permiten la identificación incluso de los ataques más sofisticados. El bloqueo nativo en tiempo real garantiza protección contra ataques de lógica comercial, exploits, actividad automatizada de bots, fraudes en línea, ataques del OWASP API Security Top 10 y mucho más.

Funciona con Cequence AI Gateway

Cequence AI Gateway permite el acceso de IA agéntica a cualquier aplicación interna, externa o SaaS en minutos, sin necesidad de programación. La Seguridad de API puede generar automáticamente especificaciones de API mejoradas que el AI Gateway utiliza para crear servidores MCP, eliminando así un esfuerzo manual considerable.

CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai