CEQUENCE

FICHA DE DATO

Cequence gestión de bots

Detección de Bots, Mitigación y Prevención de Fraude

Los bots, tanto buenos como malos, generan casi la mitad del tráfico web actual. Los bots maliciosos solían enfocarse principalmente en sitios web y aplicaciones, pero hoy en día suelen eludir las aplicaciones y atacar directamente las APIs. La ubicuidad de las APIs, junto con su accesibilidad, facilidad de uso y flexibilidad, las han convertido en un objetivo principal para los actores de amenazas. Incluso las APIs correctamente codificadas pueden ser objeto de abuso de la lógica empresarial en campañas de apropiación masiva de cuentas (ATO) o de bots de compras. La creación masiva de cuentas falsas y la extracción de contenido (scraping) se ejecutan regularmente contra aplicaciones y sus APIs. Las organizaciones necesitan una solución que detecte y prevenga ataques automatizados contra sus aplicaciones y APIs, que sea fácil de implementar y que tenga un impacto inmediato.

Gestión de Bots en un Vistazo

- **Sin necesidad de CAPTCHA —** El enfoque basado en red no requiere agentes, JavaScript ni integración de SDKs.
- **Mitigación Nativa —** Identificación y bloqueo de ataques sin depender de infraestructura de terceros como WAFs.
- **Opciones de mitigación robustas —** bloqueo, limitación de velocidad, inyección de encabezados y engaño.
- **Modelo de Implementación Flexible —** Compatible con implementaciones locales (on-premises), SaaS e híbridas.
- **Prevención de Fraude en APIs —** Políticas personalizables y granulares para casos de uso específicos de cada organización.

Visión General de Cequence Bot Management

Cequence protege las aplicaciones web, móviles y de API de una organización contra la totalidad de ataques de bots para prevenir la pérdida de datos, el robo y el fraude. Impulsado por un motor de análisis basado en aprendizaje automático (ML), Cequence determina en tiempo real si las transacciones de aplicaciones y APIs son legítimas o maliciosas, mitigando ataques de forma nativa y eliminando impactos negativos como interrupciones en el servicio, daño a la marca, alteración de los análisis de ventas y aumento de costos en la infraestructura.

Características de la Gestión de Bots

Sin Modificaciones en la Aplicación ni Fricción para el Cliente

El enfoque basado en red de Cequence elimina la necesidad de agentes o modificaciones en la aplicación, como la integración de JavaScript o SDKs móviles. Este método evita la fricción para los clientes que suelen generar las soluciones de prevención de bots, como los CAPTCHAs, y extiende la cobertura a todas las aplicaciones y APIs, no solo a aquellas que pueden ser instrumentadas. La protección basada en red elimina los esfuerzos de desarrollo y prueba necesarios para la instrumentación de aplicaciones, ahorrando tiempo y costos.

Las organizaciones pueden no ser conscientes de que tienen un problema con bots, ya que estos simplemente automatizan ataques a gran escala. Cequence detecta y mitiga diversos tipos de ataques, incluyendo:

Cuenta Adquisición (ATO)

BOLA vulnerabilidades

Ventas relámpago, ventas exageradas y lanzamientos de zapatillas

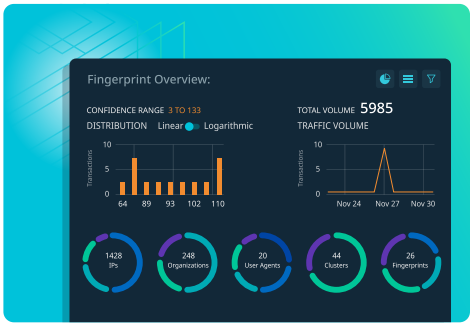
Exposición de datos sensibles

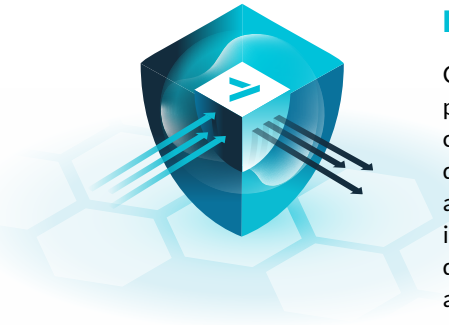
Abuso de tarjetas regalo / programas de fidelización

Cuenta falsa creación

Detección Continua de Amenazas Basada en el Comportamiento

El motor de análisis basado en ML de Cequence examina la intención del comportamiento en el tráfico web, móvil y de APIs, identificando tráfico legítimo y malicioso según su comportamiento, y no solo por direcciones IP. A partir de este análisis, la solución genera huellas de comportamiento que rastrean continuamente ataques sofisticados, incluso cuando los adversarios modifican sus tácticas para evitar la detección. Este enfoque es altamente efectivo y no requiere integración con el cliente ni con la aplicación, asegurando la protección más amplia posible para aplicaciones y APIs.





Defensa Contra Bots Impulsada por IA y ML

Cequence aprovecha la inteligencia artificial (IA) y el aprendizaje automático (ML) en toda la plataforma UAP, desde la detección hasta la mitigación de ataques. Los modelos de ML permiten una clasificación precisa de endpoints y amenazas, la detección de datos sensibles, la creación de huellas de comportamiento, y más. Además, el ML potencia la capacidad única de Cequence para detectar actividad maliciosa y generar automáticamente reglas y políticas de mitigación de amenazas, que pueden implementarse de forma automática o con revisión humana. Cequence también protege el uso autorizado de GenAI y AI agentic en la empresa y previene el scraping no deseado realizado por bots de IA, así como ataques sofisticados impulsados por inteligencia artificial utilizada por actores maliciosos.

Rápida Implementación y Resultados Inmediatos

Cequence se implementa fácilmente y ofrece resultados inmediatos, sin necesidad de modificar las aplicaciones. La solución cuenta con opciones de implementación flexibles, incluyendo SaaS, local y en entornos híbridos, para adaptarse a las necesidades de cualquier organización.

Prevención de Draude a la Medida de su Negocio

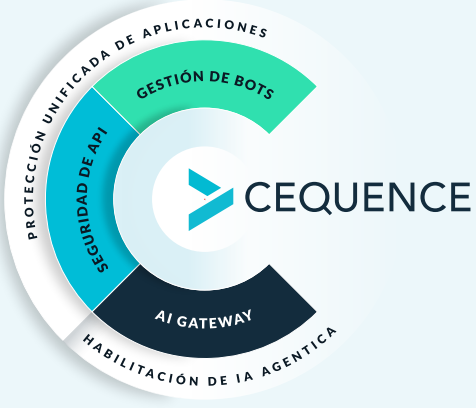
Cequence Bot Management también incluye capacidades de prevención de fraude que admiten políticas personalizables y granulares para casos de uso específicos de su negocio y sector. A medida que el tráfico fluye hacia las APIs, la actividad que coincide con esas políticas de fraude se identifica y bloquea en tiempo real, y se proporciona información detallada para el análisis de cada campaña de fraude. Los clientes pueden crear nuevas políticas y modificar las políticas predeterminadas sin necesidad de escribir código.

Funciona con Cequence AI Gateway

Cequence AI Gateway habilita el acceso de IA agéntica (basada en agentes) a cualquier aplicación interna, externa o SaaS, en minutos y sin necesidad de código. Bot Management garantiza que las aplicaciones y APIs empresariales estén protegidas contra agentes maliciosos.

La Gestión de Bots es Parte de la Plataforma Cequence Unified Application Protection

La plataforma Cequence Unified Application Protection 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. Demostrando su valor en minutos —no en días ni semanas—, Cequence ofrece un modelo de implementación flexible que no requiere instrumentación ni modificación de las aplicaciones. Con la confianza de las organizaciones públicas y privadas más grandes y exigentes, Cequence protege más de 10 mil millones de interacciones API diarias y 4 mil millones de cuentas de usuario.



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