CEQUENCE

FICHA DE DATO

Cequence Web Application and API Protection (WAAP)

Gestión de Bots Integrada, Seguridad de API, WAF y Protección contra DDoS

Las aplicaciones y sus APIs asociadas continúan proliferando, y la dificultad de protegerlas contra ataques cada vez más sofisticados sigue aumentando. Las organizaciones están adoptando arquitecturas modernas, pero las soluciones existentes no han logrado mantenerse al ritmo. Con la llegada de la inteligencia artificial (IA), la seguridad empresarial requiere un enfoque integral que proteja tanto contra ataques "tradicionales" como contra ataques potenciados por IA, ya sea la extracción no autorizada de contenido, la exfiltración de datos sensibles, el abuso de la lógica de negocio o ataques de alto volumen diseñados para interrumpir las operaciones.

WAAP de un Vistazo

- **Gestión Avanzada de Bots** detecta y bloquea bots maliciosos
- **Seguridad Integral de API** ofrece gestión de postura y pruebas
- **Potente WAF** brinda protección específica para aplicaciones web
- **Protección DDoS Escalable** intercepta ataques volumétricos

Cequence WAAP – Resumen

Los clientes nos han pedido con frecuencia que agreguemos capacidades de Web Application Firewall (WAF) y Distributed Denial of Service (DDoS) a nuestras ofertas existentes de Seguridad de API y Gestión de Bots para lograr una solución WAAP verdaderamente de primer nivel. La consolidación de proveedores, el ahorro de costos y el rendimiento general se encuentran entre las razones más comunes. Por ello, hemos incorporado un WAF potente y una protección DDoS altamente escalable para ofrecer un WAAP en la nube de clase empresarial, capaz de escalar a las empresas más grandes. Cequence WAAP protege todas sus aplicaciones web y de API contra amenazas sofisticadas y ataques de bots, tanto convencionales como potenciados por IA, todo en un solo tenant en la nube. Esta solución SaaS integrada ofrece varios beneficios:

Eficiencia Operativa

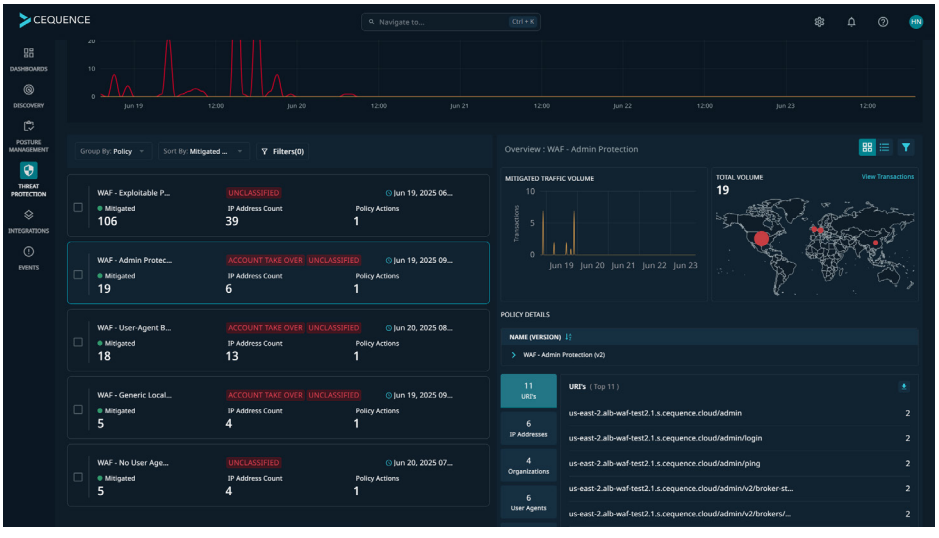
Portal único de protección de aplicaciones para WAF, gestión de bots y seguridad de API, minimizando la complejidad y la carga administrativa

Menor Latencia

Una sola implementación en la nube elimina múltiples saltos en la nube

Menor Riesgo

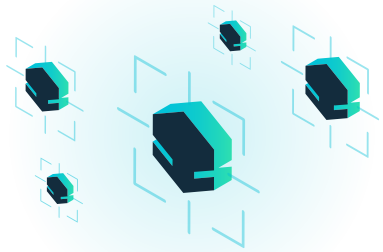
Componentes integrados dentro de un único tenant eliminan brechas de cobertura causadas por un enrutamiento de tráfico inconsistente



Las reglas WAF activadas son visibles en el panel de Cequence.

Capacidades de Cequence WAAP

Gestión de Bots



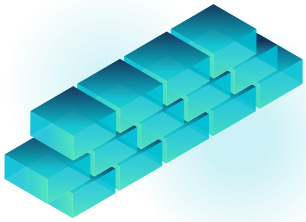
Cequence Bot Management protege las aplicaciones web, móviles y de API de una organización contra ataques de bots tanto volumétricos como altamente sofisticados. Su enfoque basado en red no requiere modificaciones en las aplicaciones, lo que permite un tiempo de valor medido en horas en lugar de semanas. El fingerprinting conductual de Cequence proporciona detección líder en la industria de bots (buenos y malos) y mitiga ataques en tiempo real directamente para aplicaciones y APIs, previniendo pérdida de datos, robo y fraude que generan tiempo de inactividad, daño a la marca, análisis de ventas distorsionados y mayores costos de infraestructura.

Seguridad de API

Cequence API Security descubre, monitorea y prueba sus APIs, evaluando una amplia gama de riesgos que pueden provocar problemas de cumplimiento y gobernanza, pérdida de datos e interrupción del negocio. Se descubren APIs internas, externas y de terceros, y las especificaciones de API pueden generarse automáticamente según sea necesario. Cequence también detecta y enmascara automáticamente datos sensibles, evitando exposición no intencionada. Las pruebas de seguridad de API encuentran problemas tanto en desarrollo como en ejecución, lo que permite a las organizaciones "moverse a la izquierda" mientras se protegen "a la derecha".

Web Application Firewall

El WAF es una solución potente y altamente escalable que cuenta con un conjunto integral de reglas y políticas, y brinda protección contra el OWASP Top 10 de aplicaciones web, patrones de entrada maliciosos y ataques de inyección SQL. Los ataques de bots detectados por el WAF se etiquetan y se envían a Cequence Bot Management, que ofrece múltiples opciones de mitigación, como bloqueo, limitación de velocidad (rate limiting), inyección de encabezados y respuestas engañosas. Esta integración mejora el rendimiento del WAF al delegar mitigaciones complejas a Cequence y proporciona una consola unificada para gestionar la actividad del WAF y la protección contra bots.

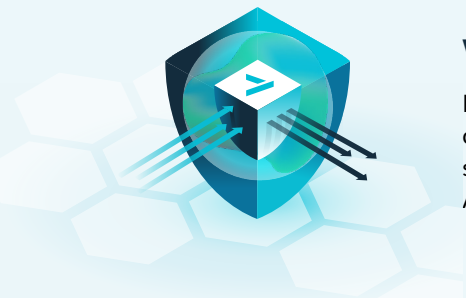


Protección contra DDoS

La protección DDoS altamente escalable garantiza que las aplicaciones y APIs estén resguardadas contra incluso los mayores ataques DDoS que de otro modo saturarían la infraestructura e interrumpirían operaciones. Protege recursos de ataques volumétricos como ataques de reflexión (capa 3), ataques de protocolo de red como SYN floods y UDP floods (capa 4), así como ataques en la capa de aplicación y API (capa 7). La solución es altamente resiliente y ofrece 99.99% de disponibilidad contra ataques comunes a la infraestructura.

Implementación

La IA está cambiando las reglas del juego en la seguridad empresarial, pero aprovecha canales de comunicación existentes. Cequence WAAP ya protege sus aplicaciones y APIs, por lo que puede estar seguro de que incluso a medida que evolucione la IA, permanecerá seguro. Cequence también ofrece un AI Gateway, la manera más rápida y sencilla de conectar agentes con aplicaciones empresariales y SaaS.



WAAP e IA

La IA está cambiando las reglas del juego en la seguridad empresarial, pero aprovecha canales de comunicación existentes. Cequence WAAP ya protege sus aplicaciones y APIs, por lo que puede estar seguro de que incluso a medida que evolucione la IA, permanecerá seguro. Cequence también ofrece un AI Gateway, la manera más rápida y sencilla de conectar agentes con aplicaciones empresariales y SaaS.

CEQUENCE

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