

Cequence Platform

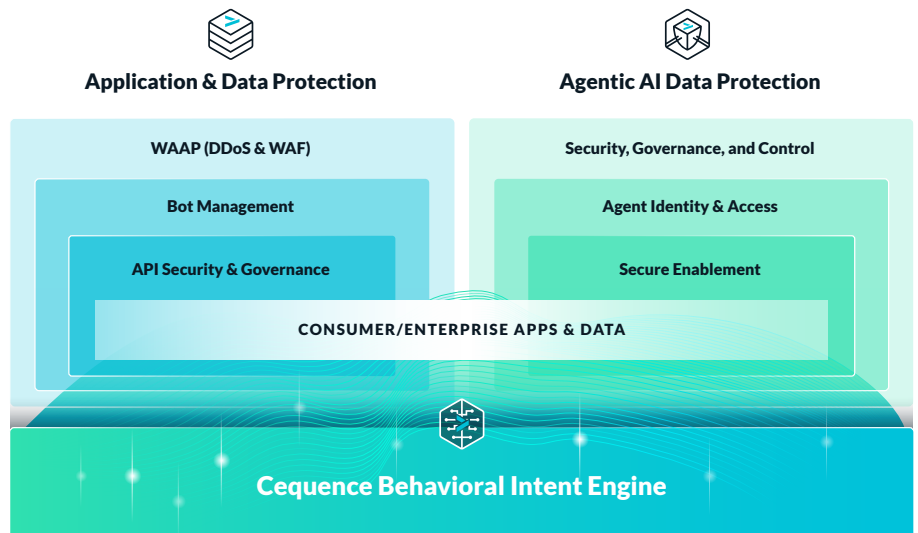
Protección basada en comportamiento para aplicaciones, APIs e IA

La superficie de ataque sigue creciendo

La adopción de la nube, los sistemas cada vez más integrados, las dependencias de terceros en la cadena de suministro y la llegada de la IA han incrementado drásticamente la superficie de ataque empresarial, poniendo en riesgo las aplicaciones y los datos. Las aplicaciones y las APIs continúan proliferando, la IA permite a los actores maliciosos descubrir vulnerabilidades y atacar a velocidad de máquina, y los agentes de IA no gobernados amenazan con filtrar datos y exceder sus permisos de acceso. Las organizaciones necesitan una solución que les permita aprovechar la promesa de productividad y crecimiento impulsados por la IA mientras protegen sus aplicaciones, APIs y datos frente a ataques, abuso de lógica de negocio y fraude.

El enfoque único de Cequence

Cada interacción entre aplicaciones, APIs e IA revela su intención a través de su comportamiento. La intención conductual es la base de la plataforma Cequence. Perfila a cada usuario, bot y agente que interactúa con sus aplicaciones, APIs y datos, creando identidades digitales que distinguen la automatización legítima de la actividad maliciosa. Esta misma capacidad ahora se extiende a la IA agéntica: Cequence aplica análisis de comportamiento al tráfico entre agentes y aplicaciones para aplicar en tiempo real controles sobre lo que los agentes pueden hacer, a qué datos pueden acceder y tomar medidas cuando sus acciones exceden los límites aceptables.



Productos de Cequence



AI Gateway

Conecta y protege flujos de trabajo de IA agéntica



Bot Management

Protege aplicaciones y APIs frente a ataques automatizados y fraude



API Security

Descubre, inventaria, prueba y protege sus endpoints de API



WAAP

Bot Management, API Security, WAF y protección DDoS

Cequence AI Gateway permite a las organizaciones hacer que sus aplicaciones y datos sean accesibles para los agentes de IA de forma sencilla y segura. Proporciona un punto central para la visibilidad y el monitoreo, registros confiables de MCP, API, LLM y habilidades (Skills), así como un catálogo de aplicaciones aprobado por la empresa. AI Gateway incorpora capacidades de gobernanza y controles integrados para restringir el comportamiento de los agentes mediante funciones como acceso con privilegios mínimos, limitación de tasa (rate limiting) y protección de datos sensibles.

Basado en principios de Zero Trust, AI Gateway proporciona verificación y validación continuas del comportamiento en tiempo de ejecución. Con estos controles y guardrails implementados, permite a las organizaciones innovar con rapidez respetando los requisitos de gobierno, pasando de prototipos a producción sin generar deuda técnica ni limitaciones de escalabilidad asociadas con soluciones básicas.

Cequence API Security es una solución diseñada con un enfoque AI-first que descubre, inventaría y prueba las API, proporcionando una gestión integral de la postura de seguridad de las API. Descubre API internas, externas y de terceros, así como proveedores de edge, infraestructura, gateways y hosting.

La combinación de descubrimiento desde el interior hacia el exterior (inside-out) y desde el exterior hacia el interior (outside-in) proporciona visibilidad e inventario tanto de la superficie de ataque como de las API internas. API Security identifica de forma autónoma los datos sensibles

que atraviesan las API y los enmascara en tiempo de ejecución, evitando la exfiltración no autorizada. Además, incluye un Asistente de IA para guiar a los profesionales de seguridad y un servidor MCP integrado para integrarse con sus flujos de trabajo internos de IA agéntica.

Cequence Bot Management detecta una amplia variedad de ataques automatizados y aplica políticas de mitigación en tiempo real para prevenir la pérdida de datos, el robo y el fraude. Bot Management se basa en la red, se integra con la infraestructura existente y no requiere agentes, JavaScript ni SDKs.

Las huellas conductuales y los análisis multidimensionales proporcionan un profundo entendimiento del contexto de negocio para identificar y bloquear ataques de forma nativa y en tiempo real. Mitiga una amplia variedad de ciberataques, incluidos ataques de lógica de negocio, exploits, actividad automatizada de bots, fraude en línea y amenazas del OWASP API Security Top 10.

Cequence Web Application and API Protection (WAAP) combina Bot Management y API Security con protección WAF y DDoS en un único entorno SaaS.

Los componentes integrados dentro de una canalización de tráfico compartida eliminan las brechas de cobertura y las inconsistencias de enrutamiento que afectan a los despliegues con múltiples proveedores. Un único portal de protección de aplicaciones abarca WAF, gestión de bots y seguridad de APIs, reduciendo la complejidad administrativa mientras mantiene una defensa coherente y coordinada en cada interacción con aplicaciones y APIs.

Casos de uso



Seguridad y gobierno para IA agéntica

Visibilidad, monitoreo, guardrails y control para flujos de trabajo de IA agéntica



Sin JavaScript ni SDK

La implementación no requiere modificaciones en las aplicaciones



Implementación en cualquier entorno

Despliegue on-premises, SaaS o híbrido



Prevención de ataques de bots

Defensa eficaz frente a ataques en aplicaciones web, móviles y APIs



No es una caja negra

Acceso inmediato al tráfico de ataques, políticas y datos para responder rápidamente



Habilitación segura de IA agéntica

Prepare aplicaciones empresariales y SaaS para agentes de forma segura



Arquitectura abierta

Importe datos para enriquecer hallazgos y exporte información a SIEMs y WAFs para mejorar los flujos de trabajo



Prevención de explotación de vulnerabilidades

Detiene ataques de día cero y ayuda a cumplir OWASP API Security Top 10 y PCI DSS



Inventario y evaluación de riesgos de APIs

Inventario de APIs internas, externas y de terceros con evaluación continua de riesgos



Prevención de fuga de datos sensibles

Identifica y enmascara automáticamente datos sensibles para evitar su exfiltración

Características de la plataforma Cequence

Inteligencia conductual e identidad precisa

Cequence analiza el comportamiento de usuarios y entidades para crear identidades digitales enriquecidas, permitiendo que las organizaciones habiliten agentes productivos sin abrir la puerta a bots maliciosos. Distingue con precisión a las personas de los bots, así como la automatización legítima de las amenazas. Para ofrecer un nivel adicional de autenticación, Biometric Check de Cequence puede aprovechar el Secure Enclave del dispositivo del visitante en lugar de añadir fricción innecesaria mediante un CAPTCHA.

Protección en tiempo de ejecución y respuesta en tiempo real

Cequence opera en tiempo de ejecución, detectando ataques en el momento en que surgen y respondiendo dinámicamente antes de que causen daños. En lugar de depender de reglas estáticas o análisis posteriores al incidente, la plataforma evalúa continuamente el tráfico en vivo para identificar amenazas en tiempo real y activar contramedidas precisas e inmediatas, manteniendo protegidas las aplicaciones, APIs y los datos sin interrumpir a los usuarios legítimos.

Arquitectura modular e implementación flexible

Cequence analiza y protege más de 10 mil millones de interacciones de aplicaciones y APIs cada día en algunas de las organizaciones más grandes del mundo en servicios financieros, retail y telecomunicaciones. Comience con los productos de Cequence que necesita hoy y amplíelos a medida que evolucionen sus requisitos. La implementación rápida y flexible en entornos SaaS, on-premises e híbridos significa que la plataforma se adapta a su infraestructura, y no al revés.

Plataforma unificada y protección integrada

La plataforma Cequence fue diseñada para la integración desde sus cimientos. Nuestra integración nativa elimina los puntos ciegos y la sobrecarga operativa de combinar soluciones puntuales, proporcionando una defensa única y coherente para casos de uso de bots, APIs e IA.

“No quiero tener ninguna interacción con actores maliciosos en el borde de mi red; quiero extender ese perímetro lo más lejos posible. Cequence es capaz de interceptar tráfico malicioso de actores de amenazas fuera de nuestro perímetro. Gracias a esta capacidad, nuestra postura de seguridad ha mejorado significativamente.”

Maria Ng
CISO

