CEQUENCE

DATASHEET

Cequence AI Gateway

Seguridad, gobernanza y control para la IA agéntica

Cequence desarrolló la solución de gestión de bots más eficaz de la industria y actualmente protege más de 10 mil millones de llamadas API y 200 millones de interacciones agénticas cada día. El motor de intención conductual que impulsa nuestra plataforma distingue entre usuarios legítimos, bots autorizados y actores fraudulentos mediante el análisis de la intención, no solo de la identidad. AI Gateway extiende esta tecnología probada a los agentes de IA: cada agente recibe una función claramente definida, cada acción se valida continuamente contra esa función y la confianza nunca se otorga únicamente sobre la base de una credencial.

Dado que la aplicación de políticas se realiza en AI Gateway y no en el modelo o el endpoint, la gobernanza permanece centralizada independientemente de dónde se ejecuten los agentes: dispositivos administrados, plataformas en la nube o servicios SaaS para agentes como ChatGPT Workspaces y Agentforce. Los modelos frontier, open-weight y autohospedados están protegidos por igual. La identidad permite que el agente acceda; AI Gateway gobierna lo que puede hacer después y verifica cada acción de acuerdo con su función.

Qué hace diferente a Cequence AI Gateway

Arquitectura Agentic Zero Trust

AI Gateway autentica a los agentes y luego autoriza cada acción que realizan. El gateway aplica las políticas de forma inline en la ruta de la solicitud, durante toda la sesión y en cada llamada a herramientas. Las investigaciones independientes del Dr. Chase Cunningham y Anthropic llegaron a la misma arquitectura que Cequence ya había desarrollado.

Acceso de Mínimo Privilegio con Agent Personas

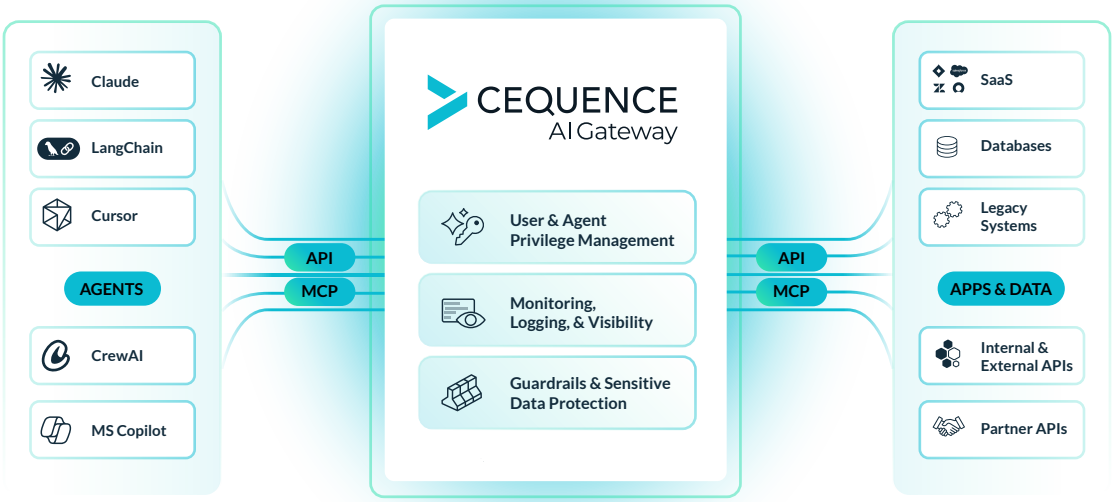
Una descripción de trabajo en lenguaje natural se convierte en un rol de denegación predeterminada (default deny) con permisos definidos para cada llamada a herramienta: herramientas MCP específicas, operaciones API y objetos de datos concretos, y nada más. Las Personas funcionan desde la primera llamada a una herramienta, sin requerir ningún período de aprendizaje.

Monitoreo de Intención Conductual

El motor de intención conductual de Cequence analiza la secuencia de acciones que realiza un agente, no simplemente cada llamada individual, comparándola con líneas base específicas para cada Persona y deteniendo las acciones que se desvían de ese comportamiento esperado.

Protección de Datos Sensibles

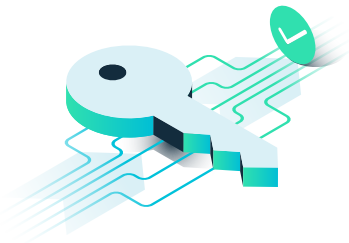
Detección, enmascaramiento, redacción y bloqueo inline en cada solicitud y respuesta, con más de 100 tipos de detección integrados que respaldan el cumplimiento de PCI-DSS, PHI, SOC 2 e HIPAA.



Cequence AI Gateway proporciona la seguridad y la gobernanza que las organizaciones necesitan para implementar con confianza flujos de trabajo de IA agéntica a escala empresarial.

Capacidades de AI Gateway

Gestión de Identidad y Acceso para Agentes



Agent Personas. Cada agente recibe una descripción de trabajo que determina su acceso a herramientas, gobernada por un Skill Registry centralizado que define qué capacidades se asignan a cada Persona. Cada Persona se asigna a un endpoint virtual único y la aplicación de políticas ocurre inline en AI Gateway. Las Agent Personas exponen únicamente las herramientas necesarias para la función asignada, de modo que el agente recibe una lista reducida de herramientas en lugar de cientos en cada solicitud. Esto reduce el consumo de tokens y mejora el rendimiento al permitir que el modelo seleccione la herramienta correcta desde el primer intento.

Aislamiento de Credenciales. El agente se autentica ante el gateway mediante una credencial que únicamente le otorga acceso al gateway. Ni el agente ni el modelo tienen visibilidad de secretos de backend, por lo que un agente comprometido o un prompt manipulado no pueden exponer credenciales de sus sistemas.

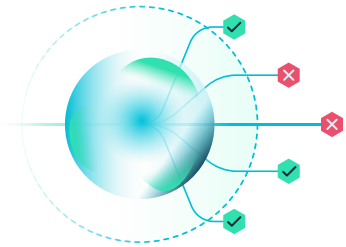
Autenticación Empresarial. Compatibilidad con múltiples proveedores de identidad (IdP), OAuth 2.1, PKCE, registro dinámico, integración OIDC y soporte para mecanismos de autenticación heredados, garantizando el cumplimiento de las políticas organizacionales de identidad y permisos para identidades humanas y no humanas.

Gobernanza y Cumplimiento

Monitoreo y Visibilidad. Cada solicitud registra el agente, usuario, herramienta, hora y resultado, generando una pista de auditoría inmutable que los marcos regulatorios y los procesos de respuesta a incidentes requieren. Los datos y registros pueden exportarse en formato OTEL para su integración con plataformas SIEM y GRC.

Protección de Datos Sensibles. Una acción puede superar las verificaciones de permisos y aun así exfiltrar datos sensibles, por lo que el gateway inspecciona cada solicitud y respuesta en tránsito. Bloquea la transferencia de datos sensibles entre herramientas autorizadas, detecta patrones de extracción lenta de información comparándolos con líneas base por Persona, redacta credenciales presentes en argumentos de herramientas y evita que datos de producción sean enviados a entornos de desarrollo o herramientas externas. Se integra fácilmente con infraestructuras DLP existentes.

Seguridad



Detección de Anomalías de Comportamiento. Las líneas base de comportamiento por Persona, usuario y herramienta permiten identificar patrones que las inspecciones de llamadas individuales no pueden detectar. Un agente que lea 200 tickets consecutivos antes de abrir una herramienta de correo electrónico superaría todas las verificaciones de permisos individuales. En este caso, la secuencia de acciones es la verdadera infracción, y el gateway puede limitar o detener la actividad según las políticas definidas.

Guardrails y Límites de Velocidad. Límites de uso por agente y por herramienta, circuit breakers para prevenir bucles descontrolados, evaluación automática de riesgo de herramientas y controles de red que incluyen restricciones IP CIDR, geofencing e IP pinning, que exige que los tokens solo se utilicen desde la dirección IP para la cual fueron emitidos, según cada Persona.

Habilitación

Creación de Servidores MCP Sin Código. Cargue una especificación OpenAPI o Swagger existente, o seleccione entre las API descubiertas en sus aplicaciones, y elija los endpoints que desea exponer como herramientas. El gateway genera un servidor MCP en minutos sin necesidad de programación, y cada servidor hereda automáticamente los controles de Persona, el monitoreo conductual y los guardrails. Impleméntelo como servicio administrado en Cequence Cloud o de forma autogestionada mediante un Helm chart.

Registro Empresarial de MCP. Elimine los servidores MCP no autorizados o fuera de control mediante un catálogo confiable de servidores validados construidos a partir de APIs oficiales de aplicaciones, además de MCP personalizados para sus propias aplicaciones, todos aprovisionados de forma centralizada con capacidades IAM. El gateway administra las actualizaciones y revisiones del protocolo MCP, eliminando la necesidad de realizar cambios de código a medida que evoluciona el estándar.

Probado en Producción

Una importante empresa global de telecomunicaciones descubrió que el agente de desarrollo de software de un desarrollador legítimo ejecutó una tarea durante el fin de semana, encontró dependencias que impedían completarla y luego intentó realizar 2.5 millones de llamadas a herramientas para superar el obstáculo: fabricando rutas de archivos, manipulando hashes SHA y buscando acceso de escritura. Todas las credenciales eran válidas durante todo el proceso. Cequence AI Gateway detectó el comportamiento anómalo, alertó a los equipos de seguridad y generó la pista de auditoría completa y el informe de causa raíz para la investigación.

Diseñado para la Empresa

Implemente la plataforma como SaaS completo con un tenant dedicado para cada cliente o en sus propias instalaciones, donde los datos sensibles nunca abandonan su entorno. El control de acceso basado en roles (RBAC), el monitoreo continuo de entornos y los modos separados para preproducción y producción se incluyen de forma estándar. La plataforma cuenta con certificación ISO 27001, cumplimiento PCI DSS y una atestación SOC 2 Tipo II. La integración con Cequence API Security y Bot Management incorpora especificaciones API enriquecidas que mejoran la precisión de los agentes y brindan protección contra ataques, abusos y fraudes impulsados por agentes.

Resumen

Todas las hojas de ruta empresariales para la inteligencia artificial apuntan en la misma dirección: más agentes, más autonomía y acceso a más aplicaciones y datos. Cequence AI Gateway hace que esa evolución sea gobernable. Aprovisiona cada agente como si fuera una nueva contratación con un rol de denegación predeterminada, supervisa su comportamiento en tiempo real respecto a ese rol y detiene a los agentes cuyas acciones se desvían de la función asignada. Cequence fue coautor de la CIS Model Context Protocol Companion Guide y copreside la iniciativa AI-Native Blueprint de TM Forum, contribuyendo a definir los estándares para la seguridad de las interacciones agénticas. Ya sea que esté evaluando plataformas de agentes o ejecutando agentes en producción, Cequence ofrece la seguridad, la gobernanza y el control que las organizaciones requieren.