

# 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 directamente en la ruta de la solicitud, durante toda la sesión y en cada llamada a herramientas (tool call). El Dr. Chase Cunningham y Anthropic describieron de forma independiente este enfoque como el correcto; es la misma arquitectura que Cequence ya había desarrollado.



### Acceso de Mínimo Privilegio con Agent Personas

Una descripción del puesto en lenguaje sencillo garantiza que los agentes solo tengan acceso a las herramientas, llamadas de API, LLM, habilidades y datos específicos que realmente necesitan; todo lo demás queda fuera de su alcance. Las personas funcionan desde la primera llamada a una herramienta, sin necesidad de un período de aprendizaje.



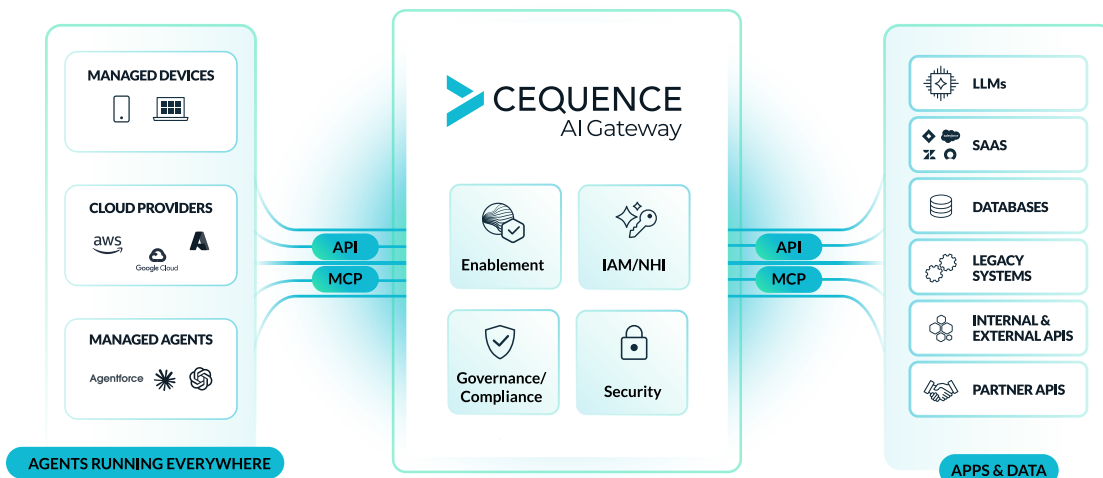
### Monitoreo de Intención Conductual

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.

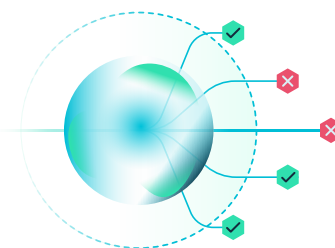


Cequence AI Gateway proporciona la seguridad y la gobernanza que las organizaciones necesitan para implementar con confianza flujos de trabajo de IA agéntica a escala empresarial.

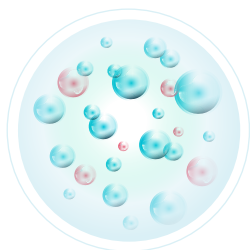
## Capacidades de AI Gateway

### Gobernanza de IA Agéntica

**Personas de Agente.** Cada agente recibe una descripción del puesto que determina su acceso a las herramientas. Este acceso se administra mediante un Registro de Habilidades centralizado que define qué habilidades se vinculan con cada persona. Cada persona se asigna a un único endpoint virtual, y las políticas se aplican en línea en el AI Gateway. Las Personas de Agente exponen únicamente las herramientas, API, LLM, habilidades y permisos necesarios para el trabajo. Así, el agente recibe una lista breve y relevante, en lugar de cientos de opciones en cada solicitud. Esto reduce el consumo de tokens y mejora el rendimiento, ya que el modelo selecciona la herramienta correcta desde el primer intento.



**Protección de Datos Sensibles.** Muchas acciones superan las validaciones de permisos y aun así pueden exfiltrar datos sensibles. Por ello, AI Gateway inspecciona cada solicitud y respuesta de los agentes de IA en tiempo de ejecución. Supervisa, redacta y bloquea datos sensibles mediante más de 100 tipos de detección preconfigurados, con integración sencilla a la infraestructura DLP existente.



**Descubrimiento de IA.** Solo es posible gobernar aquello que se conoce. Cequence proporciona visibilidad sobre el uso existente de agentes e IA, descubriendo tanto implementaciones autorizadas como Shadow AI. Identifica todos los agentes, servidores MCP y proveedores de LLM en toda la organización a partir de los registros existentes del SIEM.

**Monitoreo y Visibilidad.** Cada solicitud registra el agente, el usuario, la herramienta utilizada, la hora y el resultado, generando un rastro de auditoría completo que exigen los marcos de cumplimiento y la respuesta a incidentes. Los datos y registros pueden exportarse en formato OTEL para su integración con plataformas SIEM y GRC.

**Registros Empresariales de MCP y APIs.** El Registro MCP proporciona un catálogo confiable de servidores MCP validados, creados tanto a partir de APIs oficiales de aplicaciones como de MCP personalizados para aplicaciones propias, todos aprovisionados de forma centralizada con capacidades de IAM. AI Gateway gestiona las revisiones del protocolo MCP, por lo que no se requieren cambios de código conforme evoluciona el estándar. El Registro de APIs permite que los agentes accedan a sistemas empresariales autorizados sin exponer las credenciales de origen.

**Registro de LLM y Prompt Guard.** El Registro de LLM proporciona una conexión controlada con cada proveedor de LLM aprobado, administra las credenciales y el acceso a los modelos, y aplica límites de tasa de tokens y de gasto. Prompt Guard protege contra la inyección de prompts —incluidos los patrones de jailbreak y de extracción del prompt del sistema— antes de que lleguen al modelo.



## Seguridad

**Detección de Anomalías de Comportamiento.** Las líneas base de comportamiento por persona, usuario y herramienta permiten detectar patrones que una inspección de solicitudes individuales no puede identificar. Por ejemplo, un agente que lea 200 tickets consecutivos antes de abrir una herramienta de correo electrónico podría superar cada verificación de permisos por separado; sin embargo, la secuencia completa representa la anomalía. El gateway puede limitar o detener la acción en tiempo real según la política establecida.

**Guardrails y Rate Limits.** Rate limits por agente y por herramienta, con mecanismos de circuit breaker para detener bucles descontrolados, evaluación automática del riesgo de herramientas y controles de red que incluyen restricciones por IP CIDR, geofencing e IP pinning, que exige que los tokens solo puedan utilizarse desde la dirección IP para la cual fueron emitidos, según cada persona.

**Aislamiento de Credenciales.** El agente se autentica en el gateway mediante una credencial que únicamente concede acceso al propio gateway. Ni el agente ni el modelo tienen acceso a los secretos de backend, por lo que un agente comprometido o un prompt manipulado no pueden filtrar credenciales de sus sistemas.

**Autenticación Empresarial.** Compatibilidad con múltiples proveedores de identidad (IdP), OAuth 2.1, PKCE, registro dinámico, integración con OIDC y soporte para mecanismos de autenticación heredados, aplicando las políticas de identidad de la organización tanto para identidades humanas como no humanas.



## Habilitación

**Creación de Servidores MCP Sin Código.** Cargue una especificación OpenAPI o Swagger existente, o seleccione APIs descubiertas de 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 el alcance por persona, el monitoreo de comportamiento y los guardrails. Puede implementarse totalmente administrado en Cequence Cloud o de forma autogestionada mediante un chart de Helm.

**Registro de Habilidades.** El Registro de Habilidades proporciona un catálogo central para distribuir instrucciones y patrones operativos aprobados por la organización. Facilita que los agentes utilicen Habilidades autorizadas y permite a la empresa rastrear y auditar las acciones realizadas por agentes de IA.

## 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. Aprovechona 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.