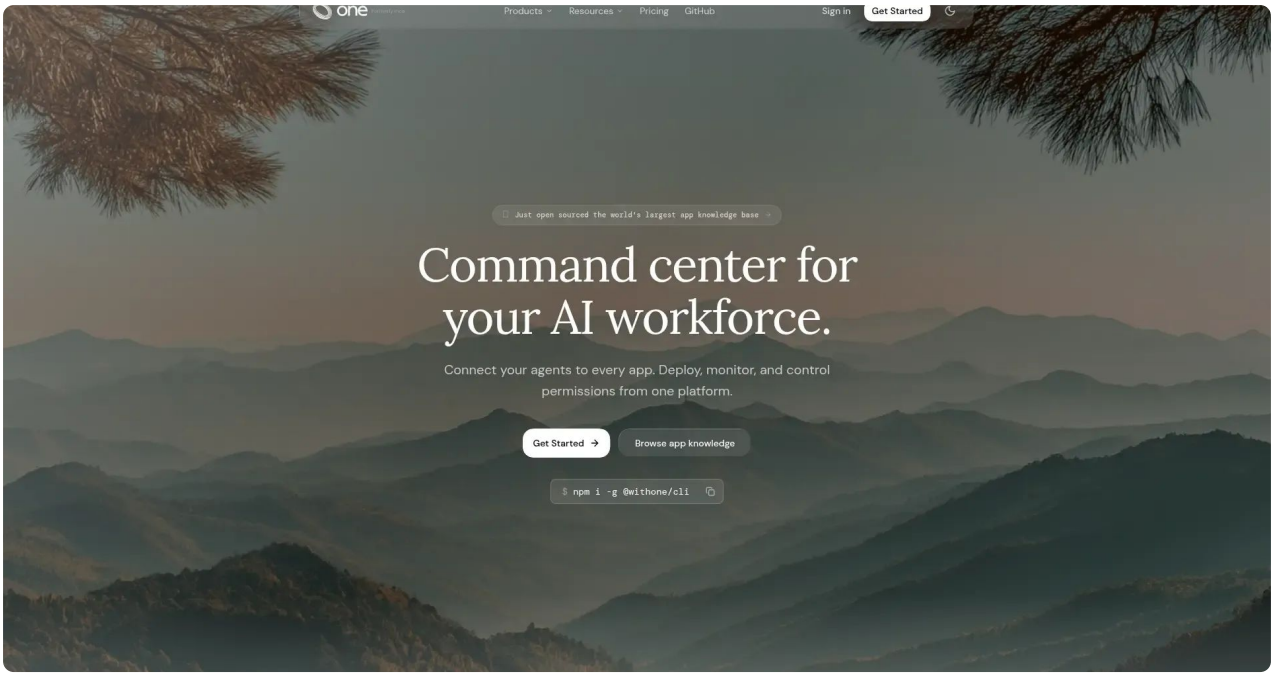

withone.ai

One es un runtime de integraciones diseñado para desarrolladores y equipos de ingeniería de IA que necesitan conectar agentes autónomos con más de 250 herramientas del mundo real como Gmail, Slack o Stripe. Permite ejecutar acciones autenticadas mediante una interfaz unificada CLI y el protocolo MCP, eliminando la gestión manual de tokens OAuth y facilitando que los LLMs interactúen con miles de servicios de forma segura, escalable y profesional en entornos de producción complejos.

Visitar Sitio Oficial Preguntar a ChatGPT Preguntar a Claude Preguntar a Grok

Contenido del Dossier

- Información de la Herramienta
- Consejos de Implantación
- Preguntas Frecuentes
- Contratos y Condiciones

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
One (withone.ai) es un entorno de ejecución (runtime) de integraciones y centro de mando diseñado específicamente para **agentes de IA**. Su propósito es eliminar la complejidad de conectar modelos de lenguaje (como Claude, GPT-4 o agentes autónomos) con herramientas del mundo real (Gmail, Slack, Stripe, HubSpot, etc.).

En el ámbito profesional, está dirigido a **desarrolladores, equipos de ingeniería de IA y directores de tecnología (CTO)** que necesitan que sus agentes no solo generen texto, sino que ejecuten acciones autenticadas en más de 250 plataformas sin tener que programar flujos OAuth individuales o gestionar tokens de API manualmente.

Principal ventaja profesional
Permite que un agente de IA interactúe con miles de servicios mediante una **interfaz unificada (CLI y MCP)**. En lugar de desarrollar conectores específicos para cada aplicación de la empresa, One ofrece acceso a más de 47.000 acciones documentadas y seguras, inyectando la autenticación necesaria en tiempo de ejecución de forma transparente para el modelo.

Para quién no es
No es una herramienta para usuarios de negocio sin conocimientos técnicos (no es un sustituto de Zapier o Make basado en "arrastrar y soltar"). Profesionales que busquen automatización visual simple o empresas que no utilicen arquitecturas basadas en agentes o LLMs para sus procesos internos encontrarán la herramienta excesivamente técnica.

Funcionalidades clave
- **Universal MCP Server:** Un servidor compatible con el Standard Model Context Protocol que permite a herramientas como Cursor o Claude Desktop acceder a cientos de apps con un consumo mínimo de tokens (aprox. 3k tokens).
- **One CLI:** Interfaz de línea de comandos para conectar aplicaciones mediante OAuth, buscar acciones y ejecutarlas directamente desde la terminal.
- **One Flow:** Motor de ejecución de flujos de trabajo multietapa (JSON-based) que permite a los agentes crear, modificar y reanudar procesos complejos con lógica condicional.
- **AuthKit:** Interfaz de conexión embebible para que los usuarios finales de una aplicación conecten sus propias cuentas de forma segura.
- **Bridge:** Tecnología que convierte cualquier documentación de API (OpenAPI/Swagger) en un servidor MCP listo para ser usado por una IA.
- **Gestión de Identidades:** Capacidad para segmentar permisos y conexiones por usuario, equipo u organización.

Precios
- **Versión Free:** 0€/mes. Incluye 1 millón de llamadas a la API, conexiones ilimitadas, acceso completo a CLI/MCP y retención de logs de 14 días. Límite de tasa de 100 req/min.
- **Starter:** 29$/mes. Para entornos de producción iniciales. Incluye 1 millón de llamadas (exceso a 0,25$/1k), 1 agente incluido, AuthKit para 50 apps y retención de logs de 30 días. 1.000 req/min.
- **Pro:** 199$/mes. Para equipos a escala. 1 millón de llamadas (exceso a 0,15$/1k), AuthKit ilimitado, retención de logs de 90 días y soporte vía Slack. 10.000 req/min.
- **Enterprise:** Precio bajo presupuesto. Incluye SSO, SCIM, acuerdos de nivel de servicio (SLA) y límites personalizados.

Perfil del usuario
- **Empresas de Software (SaaS):** Que integran capacidades de IA en sus productos para interactuar con datos de clientes.
- **Departamentos de Operaciones IT:** Para automatizar flujos internos complejos (ej. aprovisionamiento de cuentas, triaje de tickets).
- **Desarrolladores de Agentes:** Profesionales que construyen "wrappers" o aplicaciones sobre LLMs que requieren acceso a herramientas externas.
- **Equipos de DevOps:** Para integrar asistencia de IA en flujos de despliegue y monitorización.

Nivel técnico requerido
- **Uso:** Medio-Alto (requiere familiaridad con CLI y prompts estructurados).
- **Instalación/Configuración:** Alto. Es necesario manejo de Node.js (v18+), gestión de variables de entorno y configuración de archivos JSON para el protocolo MCP.
- **Competencias necesarias:** Desarrollo en JavaScript/TypeScript, conocimiento de protocolos de autenticación (OAuth/API Keys) y experiencia con modelos de lenguaje (OpenAI/Anthropic/LangChain).

Ejemplos de uso profesional
- **Atención al Cliente Autónoma:** Un agente recibe un correo en Gmail, consulta el pedido en Shopify, revisa el historial en HubSpot y redacta/envía la respuesta.
- **Gestión de Ventas:** Extracción automática de datos de nuevos leads desde correos electrónicos para enriquecer perfiles en Salesforce y crear tareas en Linear.
- **Automatización de Ingeniería:** Un agente monitoriza Pull Requests en GitHub, ejecuta tests y notifica los resultados en un canal específico de Slack.

Uso y distribución
- **CLI:** Herramienta principal basada en Node.js (@withone/cli).
- **Versión Web:** Dashboard centralizado para gestión de conexiones, logs y facturación.
- **MCP Server:** Servidor remoto hosted (mcp.withone.ai) o local vía npx.
- **Integraciones:** Nativa con Cursor, Claude Desktop, Windsurf y Claude Code.

Open source
La base de conocimiento de las integraciones (skills), el SDK y las herramientas MCP son de código abierto y están disponibles en GitHub. El motor de ejecución (runtime) alojado es propietario.

Integraciones
- **Facilidad de integración:** Full code (requiere implementación vía SDK o CLI).
- **API propia:** Dispone de una API de paso (passthrough) que normaliza las llamadas a terceros.
- **Servidor MCP:** Sí, dispone de uno de los servidores MCP más extensos del mercado.
- **Número de integraciones:** Más de 250 plataformas nativas (Gmail, Slack, Stripe, GitHub, Notion, Salesforce, Jira, etc.).

Notas finales
Información legal, licencias y contratos
- **Cumplimiento:** Declaración de cumplimiento SOC 2.
- **Privacidad:** Los datos de credenciales están encriptados en reposo y tránsito. La plataforma asegura no entrenar modelos LLM con los datos de los usuarios.
- **Licencia:** SDK y herramientas de CLI bajo licencia MIT. El servicio cloud se rige por términos de servicio de suscripción mensual/anual.

Para más información:
- Sitio web oficial
- Precios
- Documentación técnica
- Github - CLI
- Github - MCP
- Linkedin

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
- **Tipos de empresa:** Startups tecnológicas, empresas de desarrollo de software (SaaS), departamentos de ingeniería de datos y consultoras de IA que desarrollan soluciones de agentes autónomos.
- **Presupuesto:** Accesible para experimentación (freemium). Los costes de producción escalan desde 29$/mes hasta 199$/mes, siendo competitivo frente al desarrollo propio de conectores OAuth específicos.
- **Puntos clave:** Centralización de la autenticación de agentes, reducción drástica del consumo de tokens mediante el estándar MCP y acceso inmediato a más de 47.000 acciones documentadas en 250+ plataformas.

Madurez digital requerida
- **Usuarios y equipo:** Nivel técnico alto. Se requiere experiencia previa en desarrollo con Node.js, manejo de APIs REST, arquitecturas de IA (LLMs) y flujos de autenticación OAuth/API Keys.
- **Empresa y departamentos:** Organizaciones con una infraestructura técnica que ya emplea o planea emplear agentes de IA para la automatización de flujos de trabajo internos o productos finales.

Plan orientativo de implantación
Pasos necesarios y estimaciones
- **Tiempos estimados de despliegue:** Entre 2 y 5 días para una prueba de concepto funcional; 2 a 4 semanas para integración completa en entornos de producción SaaS.
- **Evaluación inicial:** Auditoría de las aplicaciones externas necesarias (Slack, Salesforce, etc.) y definición de los permisos requeridos para cada agente.
- **Configuración técnica:** Instalación de One CLI (@withone/cli), configuración del entorno local/servidor y conexión de las cuentas mediante AuthKit para la gestión de tokens.
- **Prueba de concepto:** Despliegue de un servidor MCP local para conectar un IDE (como Cursor) o cliente (Claude Desktop) con herramientas corporativas para validar la ejecución de acciones.
- **Despliegue y escalado:** Implementación del Bridge para APIs propietarias no listadas y configuración de One Flow para flujos multietapa con persistencia de estado.

Necesidades de formación del equipo
- Capacitación en el protocolo MCP (Model Context Protocol).
- Entrenamiento en el diseño de prompts para "tool calling" y gestión de errores en la ejecución de APIs.
- Formación en seguridad para la gestión de identidades y segmentación de permisos dentro del dashboard de One.

Perfiles necesarios
- **Perfiles técnicos:** Ingenieros de IA / NLP, desarrolladores Full-stack (Node.js/TypeScript) y arquitectos de soluciones Cloud.
- **Personal externo recomendado:** Consultores especializados en seguridad API/OAuth si el despliegue es a gran escala.

Retorno de la inversión (ROI)
- **Tiempos:** Reducción estimada del 70-80% en el tiempo de desarrollo de integraciones personalizadas para agentes de IA.
- **Cómo medirlo:** KPIs de reducción de horas de desarrollo (Time-to-market), coste de mantenimiento de APIs por agente y ratio de éxito en la ejecución de tareas automatizadas sin intervención humana.

Otros
- **Seguridad y cumplimiento:** La herramienta cuenta con certificación SOC 2, garantizando que los datos de autenticación no se utilizan para entrenar modelos y están encriptados en todo momento.
- **Compatibilidad de ecosistema:** Soporte directo para frameworks líderes como LangChain y conectividad nativa con herramientas de desarrollo de nueva generación como Windsurf o Claude Code.

PREGUNTAS FRECUENTES

¿Qué es One (withone.ai) y cuál es su función principal?
One es un entorno de ejecución (runtime) y centro de mando diseñado para agentes de IA. Su función técnica es actuar como una capa de abstracción que conecta modelos de lenguaje (LLMs) con herramientas externas y aplicaciones de software, eliminando la complejidad de gestionar autenticaciones OAuth y flujos de API individuales.

¿Para qué perfiles profesionales está recomendada esta herramienta?
Está orientada estrictamente a perfiles técnicos como desarrolladores de software, ingenieros de IA, DevOps y directores de tecnología (CTO). No es una herramienta 'no-code' para usuarios de negocio, sino que requiere conocimientos en manejo de terminal (CLI), Node.js y flujos JSON.

¿Qué es el Universal MCP Server de One?
Es un servidor basado en el Model Context Protocol (MCP) que permite a herramientas de desarrollo como Cursor o Claude Desktop interactuar con cientos de aplicaciones externas. Su ventaja técnica radica en que consume pocos tokens (aprox. 3k) y proporciona acceso inmediato a miles de acciones documentadas sin configuración manual por aplicación.

¿Dispone de una versión gratuita y cuáles son sus límites?
Sí, existe una versión gratuita que permite hasta 1 millón de llamadas a la API mensuales y conexiones ilimitadas. Sin embargo, tiene una tasa de límite de 100 requerimientos por minuto y una retención de logs limitada a 14 días para auditoría y depuración.

¿Es One una plataforma open source?
El proyecto adopta un modelo híbrido. El SDK, las herramientas de línea de comandos (CLI) y la base de conocimientos de integraciones están disponibles bajo licencia MIT en GitHub. No obstante, el motor de ejecución alojado en la nube (runtime) y el panel de control centralizado son de código propietario.

¿Cómo garantiza la seguridad y la privacidad de los datos?
La plataforma cuenta con la certificación SOC 2, lo que asegura estándares de seguridad industrial. Las credenciales y tokens de acceso están encriptados tanto en reposo como en tránsito. Además, la política de privacidad estipula explícitamente que los datos procesados no se utilizan para el entrenamiento de modelos de lenguaje.

¿Qué capacidades ofrece para la gestión de identidades en empresas?
One permite una gestión granular de permisos, facilitando la segmentación de conexiones por usuario, equipo u organización. En sus planes superiores, incluye soporte para SSO (Single Sign-On) y SCIM, esenciales para el aprovisionamiento y control de acceso en entornos corporativos.

¿Qué es 'Bridge' y cómo ayuda a escalar integraciones?
Bridge es una tecnología integrada que permite convertir automáticamente documentación de API estándar (como OpenAPI o Swagger) en servidores MCP funcionales. Esto permite que una IA pueda utilizar servicios propietarios o aplicaciones que no tengan una integración nativa en One simplemente aportando su esquema técnico.

¿Es compatible con la normativa de protección de datos europea?
Aunque es una tecnología de origen global, su cumplimiento SOC 2 y sus protocolos de cifrado de autenticación están alineados con los requisitos de seguridad exigidos por la normativa española y europea en el tratamiento de integraciones seguras, siempre que el desarrollador configure correctamente la residencia de datos en los servicios finales.

¿Cuál es la diferencia entre el plan Starter y el Pro?
El plan Starter está diseñado para fases de producción inicial (50 apps en AuthKit y 1.000 req/min), mientras que el plan Pro está pensado para escala masiva, ofreciendo AuthKit ilimitado, una mayor tasa de transferencia (10.000 req/min), soporte técnico dedicado vía Slack y 90 días de retención de logs.

CONTRATOS Y CONDICIONES

Principales recomendaciones
- Realizar una Evaluación de Impacto en la Protección de Datos (EIPD) antes de integrar One en procesos que manejen datos de salud, financieros o perfiles de clientes, dado que actúa como un nodo central de acceso a múltiples aplicaciones corporativas.
- Configurar el principio de "mínimo privilegio" en AuthKit; otorgar al agente de IA solo acceso de lectura o escritura en los ámbitos (scopes) estrictamente necesarios para la tarea.
- Revisar los acuerdos de procesamiento de datos (DPA) con los proveedores finales (Gmail, Salesforce, etc.), ya que One facilita la conexión pero no asume la responsabilidad legal de esos terceros.
- Implementar una supervisión humana (Human-in-the-loop) para acciones críticas ejecutadas por agentes que utilicen One Flow, especialmente en pagos o borrado de información.
- Auditar periódicamente los registros (logs) de actividad disponibles en el dashboard para detectar posibles accesos no autorizados por parte de los modelos de IA.

Ley de Inteligencia Artificial (AI Act)
- One se clasifica generalmente como una herramienta de apoyo o infraestructura para sistemas de IA. No es un sistema de IA de alto riesgo por sí mismo, pero su cumplimiento dependerá del uso final: si se usa para selección de personal o infraestructuras críticas, el usuario debe cumplir con las obligaciones de la Ley de IA de la UE.
- La empresa debe garantizar la transparencia, informando a los usuarios finales de que están interactuando con un sistema automatizado que tiene acceso a sus datos profesionales a través de esta infraestructura.

Privacidad y protección de datos
- Responsabilidades: El usuario es el Responsable del Tratamiento y With One AI actúa como Encargado del Tratamiento al gestionar las credenciales y el flujo de datos entre aplicaciones.
- Ubicación de los datos: Los servidores principales de la plataforma se ubican en Estados Unidos (región us-east-1 de AWS).
- Transferencia internacional: Existe transferencia internacional de datos. Se requiere verificar la adhesión de One al Marco de Privacidad de Datos UE-EE. UU. o la firma de Cláusulas Contractuales Tipo (SCC).
- Derechos ARCO: La empresa debe asegurar que puede responder a solicitudes de acceso o supresión, coordinando con One la limpieza de logs o datos de autenticación si fuera necesario.

Propiedad intelectual
- Propiedad de datos: Los datos que transitan por el runtime de One pertenecen íntegramente a la empresa cliente.
- Propiedad del resultado: El código generado por los agentes y las automatizaciones creadas en One Flow son propiedad de la empresa, salvo los componentes de código abierto integrados (como el SDK bajo licencia MIT).
- El fabricante se compromete contractualmente a no utilizar los datos de los clientes ni las interacciones para entrenar modelos de lenguaje propios o de terceros.

Usos y prohibiciones
- Usos prohibidos: No se permite el uso de la plataforma para actividades de spam masivo, acceso no autorizado a sistemas (hacking), o el procesamiento de datos sensibles sin el consentimiento explícito.
- Usos admitidos: Integración de herramientas profesionales bajo protocolos seguros (OAuth), automatización de flujos de trabajo internos y desarrollo de interfaces de conexión para terceros a través de AuthKit.

Seguridad y certificaciones
- Seguridad: Cifrado de datos en reposo (AES-256) y en tránsito (TLS 1.2 o superior). Las credenciales de terceros se gestionan mediante bóvedas de seguridad que aíslan las claves del acceso directo del operador.
- Certificaciones: La plataforma cuenta con certificación SOC 2 Tipo II, lo que garantiza controles rigurosos sobre la seguridad, disponibilidad e integridad del procesamiento.

Otros
- Es fundamental diferenciar entre las licencias MIT de las herramientas CLI/SDK de código abierto (que permiten modificación y uso libre) del servicio Cloud (propietario) cuyas condiciones de uso prohíben la ingeniería inversa del motor de ejecución.

Fuentes consultada:
- Términos de Servicio
- Política de Privacidad
- Documentación de Seguridad
- Repositorio Oficial CLI (Licencia MIT)
- Certificación SOC 2 e Infraestructura

Para más información y herramientas:

Explora look4.tools para descubrir las mejores soluciones tecnológicas del mercado.

Inicio Todas las herramientas Categorías