NeuronGuard

El “Cloudflare” para Aplicaciones de Inteligencia Artificial y Agentes LLM.

PITCH DECK CONFIDENCIAL | MARZO 2026

Cada empresa de software se está convirtiendo en una empresa de IA.

Modelos Base: La explosión de APIs (OpenAI, Anthropic).

2020-2022: CRECIMIENTO INICIAL

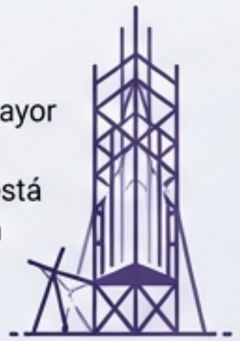
Sistemas RAG: Conexión de bases de datos privadas y corporativas a LLMs.

2023: INTEGRACIÓN CONTEXTUAL

Agentes Autónomos: Sistemas que toman decisiones y ejecutan acciones sin supervisión.

2024-FUTURO: AUTOMATIZACIÓN PLENA

La infraestructura está cambiando a un ritmo vertiginoso. Estamos en la mayor revolución tecnológica de la década, pero el ecosistema está construyendo rascacielos sin cimientos.



Pero la infraestructura actual de IA es fundamentalmente insegura.

Inyección
(LLM01 - Prompt Injection)

Usuarios ingresando instrucciones ocultas para secuestrar el comportamiento del modelo y ejecutar código malicioso.

Fuga de Datos
(LLM06 - Sensitive Information Disclosure)

El modelo expone accidentalmente datos corporativos confidenciales, PII o secretos almacenados en el contexto.

Abuso del Modelo
(LLM04/LLM08 - DoS & Excessive Agency)

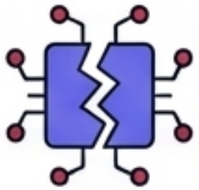
Ataques de denegación de servicio que agotan presupuestos costosos de API y agentes tomando acciones no autorizadas.

Exponer LLMs genera brechas de seguridad masivas. Si un modelo expone datos bancarios o internos, la startup o el proyecto muere instantáneamente.

El panorama actual: soluciones complejas, lentas o insuficientes.

Soluciones Punto a Punto
(Ej. Lakera, Protect AI)

Requieren integraciones profundas, cambios masivos en el código de la aplicación y mantenimiento constante por parte de los desarrolladores.



Análisis Post-Hoc
(Ej. Galileo)

Actúan a destiempo. Analizan el problema y generan alertas después de que la fuga de datos o la inyección ya ha ocurrido.

Ataduras al Cloud
(Ej. AWS Bedrock, Azure AI)

Vendor lock-in. Soluciones rígidas que no funcionan si la empresa necesita enrutar peticiones entre múltiples proveedores de LLMs (OpenAI, Gemini, modelos locales).

NeuronGuard: El Firewall API Transparente para la IA.

CAOS

Aplicaciones

Usuarios

Agentes

NeuronGuard

ORDEN

Cerebro / Modelo LLM
(OpenAI, Anthropic)

Cero Fricción

No requiere cambiar el código de la aplicación (Proxy OpenAI-compatible).

Tiempo Real

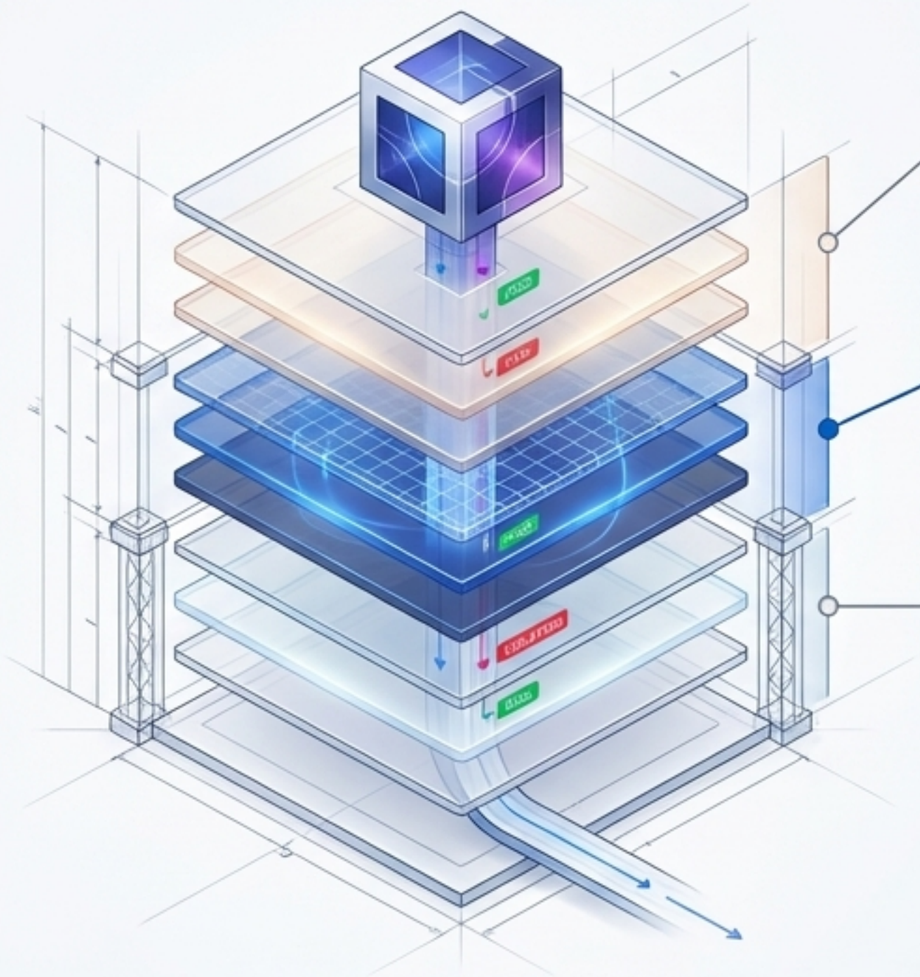
Intercepta, analiza y filtra cada request y response en el acto.

Agnóstico

Funciona con cualquier modelo y proveedor de LLM en el mercado.

Arquitectura de Alto Rendimiento: 10 capas paralelas en microsegundos.

Latencia P95 < 350ms



Input Security Engine

Anti-DoS (Redis), Validación de Regex dinámico, Prevención de PII y detectores ML.

RAG Security (RAPTOR)

Análisis revolucionario de documentos recuperados antes de que toquen el LLM.

Output Security Engine

Filtrado de alucinaciones, toxicidad, formateo inseguro y prevención de fugas internas.

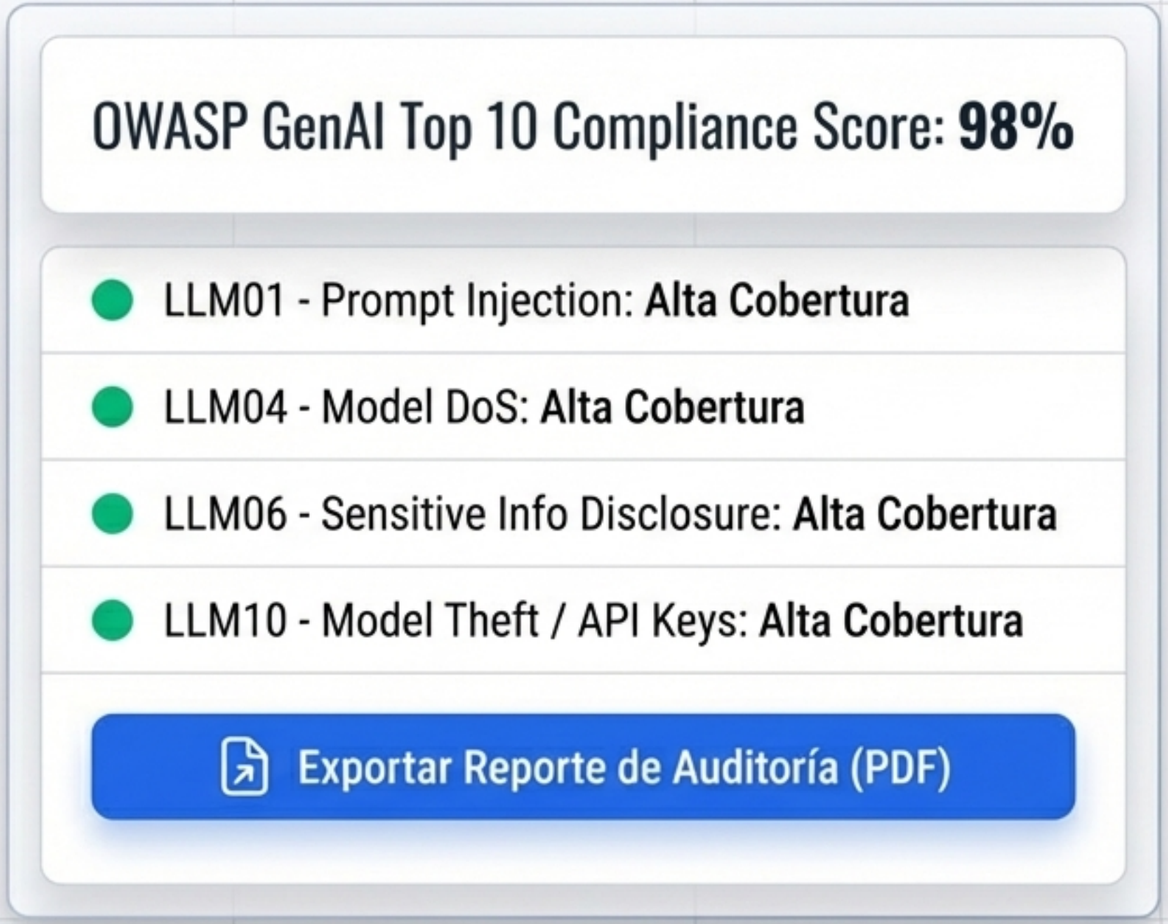
Todo orquestado por un cerebro multi-capa de 85 nodos evaluando cada decisión (PASS / VIOLATION) instantáneamente.

Diseñado para ser el estándar global de la industria.

	Proxy sin código	Seguridad RAG (RAPTOR)	Agnóstico al LLM	Despliegue On-Premise
NeuronGuard	✓	✓	✓	✓
Lakera Guard	✓	—	✓	✓
AWS Bedrock Guardrails	—	—	—	—
Protect AI LLM Guard	—	—	✓	✓
Galileo (Post-hoc)	—	—	✓	—

CISO-Ready: Cumplimiento OWASP GenAI Automatizado.

No solo bloqueamos ataques en tiempo real; entregamos a los equipos de seguridad y auditores un mapeo automático de mitigación de riesgos. Acelera drásticamente los ciclos de ventas Enterprise.



Un mercado masivo con dolor inmediato (Go-To-Market).

Startups Nativas de IA

Necesitan velocidad. Construyen agentes y wrappers sobre LLMs y no tienen tiempo para crear capas de seguridad propias.

Agencias de Automatización

Integran workflows de IA para clientes externos. Necesitan garantías de que el bot de su cliente no alucinará ni filtrará datos corporativos.

Adopción Enterprise Interna

Bancos, aseguradoras y corporaciones que conectan bases de datos (RAG) a LLMs y exigen estricto cumplimiento de normativas de privacidad.

Consultoras Tecnológicas

Implementadores que buscan una herramienta de infraestructura estándar para incluir en cada arquitectura de IA que diseñan.

Escala de ingresos basada en volumen de uso.

Free

$0

Motor PLG.

10K requests/mes. Diseñado para adopción masiva por desarrolladores.

1 política de seguridad, Guardrails básicos.

Recomendado

Pro

$99/mes

Sweet Spot.

1M requests/mes.

Todas las 10 capas de seguridad habilitadas + Analytics.

Business

$499/mes

Escala.

Peticiones ilimitadas.

SLA del 99.9%.

Políticas de seguridad personalizadas.

Enterprise

Custom

Tickets de $1500+.

Despliegue On-Premise, certificación SOC 2, CSM dedicado, soporte 24/7.

Un camino pragmático hacia los $10M+ de ARR.

Fase 1: Cashflow (0-24 meses)

Consultoría táctica de IA y automatización (Tickets de $15k–$80k por proyecto). **Objetivo**: Financiar el desarrollo del producto con flujo de caja positivo desde el día 1, validando casos de uso reales.

Fase 2: Expansión de Infraestructura

Transición agresiva a SaaS puro. Venta cruzada de NeuronGuard a la base de clientes cautivos y lanzamiento.

Fase 2: Expansión de Infraestructura

Transición agresiva a SaaS puro. Venta cruzada de NeuronGuard a la base de clientes cautivos y lanzamiento de la SDK pública (OpenGuardrails) para el mercado global.

Fase 3: La Plataforma Definitiva

Integración vertical. Despliegue del Workflow Builder propio. La empresa evoluciona de proveer "el escudo" a proveer la fábrica completa de automatización segura.

Economía unitaria de alto rendimiento (OKRs de Escala).

$10K

MRR (Objetivo Mes 6)

Demostración rápida de tracción comercial.

>110%

NRR (Retención Neta de Ingresos)

Demuestra Land and Expand natural por el modelo de volumen.

<12

Meses CAC Payback

Eficiencia de capital radical gracias al enfoque Product-Led Growth.

100M

Peticiones analizadas / mes

Objetivo para el Mes 12. Demuestra la escala y la robustez técnica de la infraestructura.

La Próxima Gran Categoría de Infraestructura.

ERA TECNOLÓGICA Roboto Mono	EMPRESA DOMINANTE (DECACORN) Roboto Mono
Web Security (Aplicaciones Web)	Cloudflare
App Security (Código Abierto / DevSecOps)	Snyk
Observability (Infraestructura Cloud)	Datadog
AI Security (Agentes LLM & RAG)	**NeuronGuard**

No estamos construyendo una “herramienta” secundaria.
Estamos construyendo el Middleware API definitivo para la era de la IA.
Si tienes una web, usas Cloudflare. Si tienes un Agente IA, usarás NeuronGuard.

El equipo y el motor detrás de la barrera.

El Equipo

Un equipo multidisciplinario que une la consultoría de IA del más alto nivel corporativo con la arquitectura de software robusta y la ciberseguridad. Hemos construido la infraestructura que el mercado exige.

Tech Stack de MVP Foundation

FastAPI
(Motor Proxy)

Next.js
(Dashboard)

PostgreSQL / TimescaleDB
(Auditoría)

Redis
(Rate Limiting / Anti-DoS)

Asegura el futuro de la Inteligencia Artificial.

Ronda Actual: Levantando Seed Round

Uso de fondos: Expansión de ingeniería (Core + ML Ops) y Go-To-Market inicial para escalar a 100M+ requests/mes.

Únete a nosotros para construir la capa de seguridad estándar de la IA generativa.

[Nombre del Fundador] | [Email del Fundador]
neuronguard.ai