WORDPRESS 7.0 «ARMSTRONG»

I pericoli del nuovo Client AI di WordPress

«Da grandi poteri derivano grandi responsabilità»
(ma non tutti sembrano rendersene conto…)

16 Giugno 2026
WordPress Meetup Milano
Maurizio Pelizzone · Mavida S.n.c.

CHI SONO

Maurizio Pelizzone

Dev Ninja, Vibe Coder, Prompt Engineer, WordPress expert & Speaker

https://www.linkedin.com/in/mauriziopelizzone/
maurizio@mavida.com

Oltre 15 anni nell'ecosistema WordPress: temi e plugin custom, con un focus verticale sull'integrazione di CRM e gestionali aziendali.

Dal 2023 ho trasformato il mio workflow integrando l'AI per ottimizzare i processi di sviluppo.

Oggi aiuto le aziende a far dialogare WordPress con il resto del mondo digitale: lavoro più fluido, intelligente e scalabile.

METTIAMOCI D'ACCORDO

Non è un talk contro l'AI

In Mavida la usiamo ogni giorno

- Generiamo codice, velocizziamo lo sviluppo, costruiamo automazioni.
- L'AI è una leva straordinaria… quando la usiamo per costruire meglio.
- Il problema non è l'AI: è infilarla ovunque, a prescindere dal contesto.

CAMBIAMO PROSPETTIVA

da **«cosa possiamo costruire»**

a

«cosa può andare storto»

(tanto a me non succede mai nulla…)

20 MAGGIO 2026

Cosa è cambiato con WordPress 7.0

Per la prima volta l'AI entra nel core: un'infrastruttura unica a cui i plugin si agganciano.

AI Client

Un'interfaccia unica nel core: i plugin chiedono «genera questo testo», WordPress smista la richiesta al modello configurato.

Connettori

Tre provider pre-registrati: OpenAI, Anthropic e Google. L'admin inserisce una chiave API per provider.

Abilities API

Un registro di «azioni» che l'AI può eseguire sul sito. È la base per gli agenti dentro WordPress.

Ma erano queste le priorità?

Il client AI è bellissimo. Per chi ci lavora ogni giorno, però, le cose da sistemare erano altre.

Buchi ancora aperti nel 2026

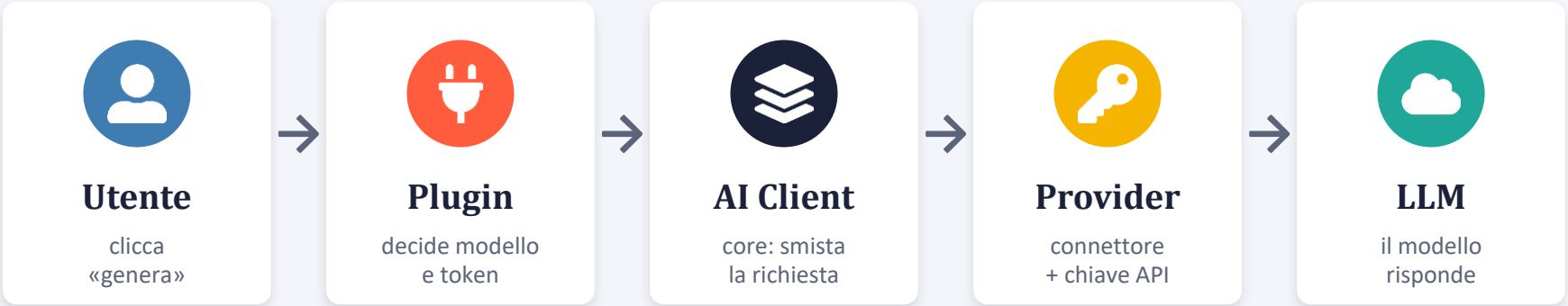
- Localizzazione multilingua nativa: non esiste, si va di plugin.
- SEO di base (meta, schema, sitemap): delegata a Yoast & co.
- Form contatti: ancora nessuno integrato.
- Modello dati da blog del 2003 che scala male.

E intanto…

la real-time collaboration — la feature centrale della Fase 3, in sviluppo dal 2021 — è stata **rimossa** dalla release.

IL FLUSSO DI UNA RICHIESTA

Come funziona, in pratica



Nota chiave: chi decide quale modello usare e quanti token spendere è **il plugin**, non tu.

Prima di tutto: serve un provider

«Nativo» non vuol dire «pronto all'uso». Senza un provider configurato, il client AI non fa nulla.

1

Scegli un provider

OpenAI, Anthropic o Google (o un connettore di terze parti).

2

Crea un account

Sul sito del provider, con carta di credito e fatturazione attiva.

3

Genera una chiave API

Una stringa segreta che autorizza la spesa sul tuo account.

4

Incolla la chiave in WordPress

Nella schermata Connettori. E qui iniziano i problemi.

REALISMO

La barriera dell'utente base

Cosa significa davvero «procurarsi una chiave»

- Capire cos'è una API key (e perché è un segreto).
- Inserire una carta di credito su un servizio estero.
- Navigare una dashboard tecnica in inglese.
- Capire crediti, token, fatturazione a consumo.
- Conservare la chiave senza esporla.

Per la maggior parte degli utenti

è un ostacolo enorme

altro che funzione «nativa»

IL NODO ARCHITETTURALE

Chi decide cosa (e chi paga)

L'utente controlla…

- quali provider sono disponibili sul sito
- la chiave API inserita

Nessun tetto di spesa globale.

Il plugin decide…

- quale modello usare (anche il più costoso)
- quanti token consumare per richiesta
- se mettere un limite… oppure no

Il client AI non ha un freno integrato: più plugin che condividono una chiave possono sfondare il tetto di token in meno di un minuto.

RISCHIO N.1

Il plugin può bruciare i tuoi euro

…e te ne accorgi solo leggendo la fattura.

USD PER MILIONE DI TOKEN · GIUGNO 2026

Quanto costano i modelli del core

Costo per generare 100 articoli da blog *(≈ 2.000 token input + 1.500 output ciascuno)*. Prezzi di listino.

Modello	Input	Output	100 articoli
Claude Opus 4.8	$5,00	$25,00	**$4,75**
Claude Sonnet 4.6	$3,00	$15,00	**$2,85**
Claude Haiku 4.5	$1,00	$5,00	**$0,95**
GPT-5.5	$5,00	$30,00	**$5,50**
GPT-5.4	$2,50	$15,00	**$2,75**
GPT-5.4 nano	$0,20	$1,25	**$0,23**
Gemini 3.1 Pro	$2,00	$12,00	**$2,20**
Gemini 3.5 Flash	$1,50	$9,00	**$1,65**
Gemini 3 Flash	$0,50	$3,00	**$0,55**

USD PER MILIONE DI TOKEN · UNA SOLA CHIAVE

I low-cost via OpenRouter

Stesso task (100 articoli). Per-token paghi come dal provider; OpenRouter aggiunge solo il **5,5% sull'acquisto di crediti**.

Modello	Input	Output	100 articoli
DeepSeek V4 Pro	$0,435	$0,87	**$0,22**
Kimi K2.5	$0,375	$2,025	**$0,38**
Qwen3.7-Plus	$0,32	$1,28	**$0,26**

Qwen3.7-Plus fa 100 articoli a ~$0,26:
circa 20x meno di GPT-5.5 ($5,50) e di Claude Opus 4.8 ($4,75).
Una chiave sola, credito prepagato, tetto deciso da te.

Lo scenario «fattura shock»

Stesso identico lavoro mensile, due plugin che scelgono modelli diversi:

Plugin «accorto»

modello economico

~ $4,50

al mese

Plugin «ingordo»

modello premium di default

fino a 30–40x

...la stessa attività, moltiplicata

Tra il modello più economico e il più potente ci sono fino a ~30x sull'input e ~36x sull'output.
Stesso lavoro, conto diverso — e a deciderlo non sei tu.

RISCHIO SICUREZZA

La tua chiave vale oro

L'allarme di Patchstack

«WordPress 7.0 + vulnerabilità dei plugin = token AI gratis. Ci sarà una corsa a rubare le chiavi API»

— Oliver Sild, fondatore di Patchstack

Una chiave rubata = soldi, non solo dati

- vale anche decine di migliaia di dollari
- alimenta reti di bot per truffe e phishing
- spende sul tuo account, spesso senza allarmi
- te ne accorgi solo a fattura emessa

RISCHIO SICUREZZA

La chiave è nel database, in chiaro

Se qualcuno riesce a eseguire PHP sul tuo sito, recuperare la chiave è banale:

```php
<?php
$key = get_option('ai_provider_api_key');
// e la chiave è tua. Una riga.
```

Scenario peggiore: un plugin popolare viene compromesso e un update raccoglie in silenzio le chiavi da ogni sito che lo usa.

Il punto vero

Cifrata o no, nel DB o nel filesystem: se l'attaccante prende il controllo del sito, la chiave esce.

LE CONTROMISURE

Come tenerlo sotto controllo

Una chiave solo per WordPress

Mai riusare la chiave principale: una dedicata, isolabile e revocabile.

Imposta un limite di spesa

Sul provider, configura un tetto mensile e degli alert di consumo.

Ruota la chiave

Con una cadenza fissa e subito dopo ogni sospetto o cambio di fornitore.

Verifica i plugin AI

Quale modello usano, se mettono limiti, se «telefonano a casa».

PLUGIN · AI-PROVIDER-FOR-OPENROUTER

Un'alternativa: OpenRouter

Un solo gateway davanti a centinaia di modelli, con il controllo della spesa dalla tua parte.

Una chiave sola

Accesso a OpenAI, Anthropic, Google, Meta e tanti altri da un'unica API.

Credito prepagato

Paghi in anticipo: una chiave rubata o un plugin ingordo svuotano al massimo il credito che hai messo tu.

Limiti per chiave

Imposti un tetto di spesa sulla singola chiave: niente fattura a sorpresa.

Una dashboard

Consumi di tutti i provider in un unico posto, facili da monitorare.

La previsione (sfera di cristallo)

«Graceful degradation» rovesciata

Chi sviluppa plugin AI si assume di fatto una responsabilità economica sull'uso che ne fa l'utente. In molti aggireranno il sistema integrato: il plugin che non trova un client AI farà tutto per conto suo e venderà l'AI nella versione pro, in abbonamento.

La morale: *pensateci dieci volte prima di affidare la vostra chiave di Anthropic o Gemini a un plugin scritto «dalla mamma di Goldrake».*

LO SFONDO

Non è solo WordPress: «AI feature creep»

L'accumulo graduale di componenti AI che diluiscono il valore core di un prodotto.

Postman

Da tool API leggero a piattaforma cloud-only con agenti AI. Gli utenti migrano verso Bruno: locale, niente cloud, niente AI.

Notion

AI a 15$/utente, workspace lenti. Fuga verso Obsidian, Craft, AppFlowy.

Microsoft

Dopo il caso «Microslop» fa marcia indietro: «togliamo Copilot da dove non serve».

La domanda da farsi prima di ogni integrazione AI:
questa feature aumenta il valore per l'utente, o lo seppellisce sotto un livello di complessità in più?

IN SINTESI

Il dito e la luna

Guardare il dito invece della luna

Non si vince con le feature di tendenza, si vince con le basi solide. L'AI nel core è marketing-ready, ma chi installa WordPress non ne aveva bisogno: la complessità cresce sopra, invece di semplificarsi sotto.

Ma WordPress non è morto

- Resta la risposta giusta per moltissimi contesti.
- Per certi progetti (vetrina, landing, blog statico) oggi ci sono alternative valide.
- «Tanto l'AI scrive il codice» non è una strategia: è creare scatole nere.

DA PORTARE A CASA

Usate l'AI per costruire meglio, non affidatele le chiavi a scatola chiusa.

✓ Chiave dedicata
✓ Limite di spesa
✓ Rotazione + audit dei plugin

GUIDA GRATUITA · CREATIVE COMMONS BY-SA 4.0

Claude Code: una guida pratica

140 pagine verificate sulla documentazione ufficiale Anthropic: installazione e setup, Plan Mode, prompt engineering, gestione del contesto, hook, server MCP, subagent e Skill. Esempi concreti su PHP, JavaScript e WordPress. Niente hype: ogni capitolo dice dove conviene davvero e dove no.

github.com/miziomon/claude-code-guide
maurizio.mavida.com/guida-claude-code
leanpub.com/claude-code-guide

Pareri non richiesti

Il video podcast semiserio sull'AI di cui (probabilmente) nessuno aveva bisogno.

- Due voci e background opposti: si ragiona, si litiga e ogni tanto si capisce qualcosa.
- ~25 minuti in presa diretta: niente editing, niente rete di sicurezza.
- Non ti diciamo cosa pensare dell'AI: ti diamo i nostri pareri non richiesti.

3 episodi già online — il resto sul tubo.

con Maurizio Pelizzone & Elisa Scagnetti

youtube.com/@parerinonrichiesti

mavida
MAKE YOUR WORK EASY
.com

Domande?

Grazie per l'attenzione.
Parliamone.

Grazie!

Restiamo in contatto

- https://linkedin.com/in/mauriziopelizzone
- https://maurizio.mavida.com
- https://youtube.com/@parerinonrichiesti (YouTube «Pareri non richiesti»)
- maurizio@mavida.com