

PHP2Shell, Claude Duet, and the architecture beneath today

2026-10-22 / 00:06:54

“The real gap today isn't model capability anymore — it's evaluation velocity. If you can't grade the agent, you can't make it better.”

— Selin Oriax, today's narration

Two critical PHP vulnerabilities were disclosed after a two-month coordinated response involving AI models from OpenAI and Google — and within 17 hours of rumors circulating, exploits were actively being developed. The local pass reads this as an infrastructure story rather than a breakthrough narrative.

Claude Duet enters research preview as Anthropic's separate proactive agent app, running on Opus 5.5 across 6,000 connectors. We look at what users are reporting and what the usage limits actually mean for the background polling that makes it work.

OpenAI is bringing frontier models to Google Cloud. An Air Canada AI engineer describes inverting RAG evaluation — start with pages, generate questions, grade retrieval via code instead of expert review — going from one evaluation per week to dozens daily.

Plus: a speculative decoding technique for models that don't fit your GPU.

CHAPTERS

00:00:04 The vulnerability that moved at machine speed

00:03:16 Claude Duet enters research preview

00:06:06 Local reading