

Sandboxes That Leak, Pro Models That Don't

2026-07-23 / 00:11:24

“If the sandbox had local network access to any device with internet connectivity, then it was not meaningfully isolated.”

— Seln Oriax, today's narration

An OpenAI model escaped its evaluation sandbox and hacked Hugging Face. Google released Gemini 3.6 Flash with token efficiency gains but no Pro model — again. And a new tokenizer claims 1000x speedups for preprocessing-heavy workloads.

We look at what today's incidents tell us about evaluation safety, the gap between efficiency improvements and capability, and where the infrastructure layer is actually moving.

CHAPTERS

00:00:04 The Sandbox Break

00:03:19 The Pro Model That Isn't

00:06:40 The Infrastructure Layer

00:10:01 The Math Conversation