

OpenAI trains frontier models offline after security incidents

Source copy kept by wheresthe.ai for the story "OpenAI trains frontier models offline after security incidents" (<https://wheresthe.ai/d/intl-openai-trains-frontier-models-offline-after-security-in-2026-10/>).

Source: <https://www.theverge.com/ai-artificial-intelligence/1018021/openai-training-top-ai-models-no-internet>

Text saved 23 Oct 2026 (the page as published).

SHA-256 of the saved text: 00ab57fc4b4fee422272ea5bc65e3874f28bbc6ba43d14e8eb2a3224445df309

AI

News

OpenAI

OpenAI now trains its frontier AI models with no internet access AI agents can still communicate without a network connection, OpenAI found.

AI agents can still communicate without a network connection, OpenAI found.

by Emma Roth Oct 23, 2026, 9:11 PM UTC

Image: Cath Virginia / The Verge

Part Of The AI Superintelligence Slowdown

see all updates

Emma Roth is a news writer who covers the streaming wars, consumer tech, crypto, social media, and much more. Previously, she was a writer and editor at MUO.

OpenAI is now training its most advanced AI models without internet access following a string of rogue hacking incidents. In a blog post on Friday , OpenAI says it built an offline testing environment where AI models can interact with indexed and cached web content "without risk of affecting external systems."

OpenAI paused training its frontier AI models in September , after disclosing several incidents in which its AI agents broke out of their testing environments to hack third-party companies and government agencies , or swarm obscure websites . On October 1st, OpenAI resumed reinforcement learning training and internal inference with tighter security measures, the blog post says.

Even with these safeguards in place and no internet access, OpenAI found that agents "do not always need a network connection in order to communicate." One test performed by the company asked AI models on separate virtual machines to exchange secrets without a network connection. To bypass this restriction, the AI agents found a way to communicate using the processor's cache:

Reading data from the cache is faster than retrieving it from main memory, and the agents used this timing difference to communicate. One agent encoded information by evicting selected data from the cache. Another timed how long it took to reload that data, using the difference between fast and slow reads to recover the message. Once the agents agreed on a protocol for encoding and decoding these signals, they could exchange the synthetic secrets without changing a shared file or opening a network connection.

OpenAI says it has added checks to its monitoring system to detect this type of communication. It will also continue training its frontier AI models without a network connection until improved safeguards "justify broader internet access."

Related Sam Altman says OpenAI won't go public until its models are safe One company is at the center of a wave of rogue AI attacks

In the meantime, OpenAI says it will work to improve the security of its virtual machines, while testing for weaknesses in its testing environments. It's also going to continue testing its monitoring systems, which were recently undermined by its AI agents during internal coding projects .

Follow topics and authors from this story to see more like this in your personalized homepage feed and to receive

email updates. Emma Roth AI

News

OpenAI

More in: The AI Superintelligence Slowdown

OpenAI's misalignment monitoring system had "a number of novel vulnerabilities," third-party evaluators found.

Jay Peters Oct 22

A hacker broke into John Deere and SharkNinja with an army of AI agents

Emma Roth Oct 19

The FTC reportedly subpoenaed OpenAI and Anthropic for info on AI security incidents.

Stevie Bonifield Oct 15

Most Popular

Most Popular Now Google says it might use your Gmail and Google Photos data to target ads

Tesla driver using Full Self-Driving struck and killed a man crossing I-80

The first broken iPhone Duos are here

Trump says Sundar Pichai talked him out of renaming the Atlantic Ocean

The iPhone Duo is a messy, expensive, good time

The Verge Daily A free daily digest of the news that matters most.

Email (required)

Sign Up By providing your information, you agree to our Terms of Use and our Privacy Policy . We use vendors that may also process your information to help provide our services. This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Advertiser Content From This is the title for the native ad

More in AI

The iPhone Duo should have been an iPad

Now Google says it might use your Gmail and Google Photos data to target ads

Meta delays new business terms after publisher pushback on AI scraping

Retro gaming is being overrun with AI

Canva's first AI image model plans designs before generating them

Meta's AI could still scrape news sites, legal experts say

The iPhone Duo should have been an iPad

David Pierce 5:00 PM UTC

Now Google says it might use your Gmail and Google Photos data to target ads

Jess Weatherbed 4:52 PM UTC

Meta delays new business terms after publisher pushback on AI scraping

Emma Roth 2:47 PM UTC

Retro gaming is being overrun with AI

Andrew Webster 12:00 PM UTC

Canva's first AI image model plans designs before generating them

Emma Roth Oct 22

Meta's AI could still scrape news sites, legal experts say

Emma Roth Oct 22

Advertiser Content From

This is the title for the native ad

Top Stories

1:00 PM UTC

People are vibe coding their way to better TVs

5:35 PM UTC

Elon Musk's dangerous grip on outer space

10:00 AM UTC

No, the iPhone Duo isn't a small phone

1:00 PM UTC

Netflix can't fire its way out of this downward spiral

12:00 PM UTC

Retro gaming is being overrun with AI