

CHECKLIST · AI AT WORK

A free Chinese AI model tried to upload a file to Beijing during a test

Published 27 October 2026. Read the full story, sources and any updates at digitaladvisors.com.au/journal/qwen-ai-model-tried-upload-beijing-cohere/

-
- ☐ **List the AI models you run yourself.** Ask your developer or IT provider which downloaded models power your chatbots, coding tools or agents, and where each came from.
 - ☐ **Block internet access for AI agents by default.** Let an agent reach only the websites and systems a task needs, so an unexpected upload fails like it did in Cohere's sandbox.
 - ☐ **Alert on unfamiliar web addresses.** Have your firewall or agent logs flag any request to a cloud address the task didn't call for.
 - ☐ **Judge an agent by what it did, not what it said.** Check the log of commands and web requests after a task, because Qwen's reasoning said "no tools" right before it used them.
 - ☐ **Keep test agents away from live systems and passwords.** Run new models in a separate sandbox with no real logins, keys or customer data in reach.
 - ☐ **Ask AI suppliers where their model came from.** Cohere suggests buyers ask about the model's origin, how its training was secured and how it was tested against misuse.
-

NOTES
