

Windows 11 Gets an Agent Sandbox, and the New Surface Runs Big Models Locally

Kabui, Charles

2026-10-28

[Read at ToKnow.ai](#)

Windows 11 Gets an Agent Sandbox, and the New Surface Runs Big Models Locally

One shared memory pool per PC, and a written fence for agents that use it

89

tokens a second, 35B model

128 GB

one pool, chip and graphics

\$2,600

starting price, 24 GB

October 28, 2026

ToKnow.ai

Microsoft is selling Windows PCs built to run AI models on your own desk instead of in a data centre. The Surface Laptop Ultra starts at [\\$2,599.99](#). The Surface RTX Spark Dev Box, a small desktop, costs \$5,999.99 and ships in November. Inside, NVIDIA's RTX Spark chip shares up to 128 GB of memory between the processor and the graphics unit, which NVIDIA says holds models of up to 120 billion parameters. Microsoft Execution Containers,

an agent sandbox, became generally available on October 7 and enforces a written list of files and network addresses an agent may reach.

StorageReview ran a 35-billion and a 20-billion-parameter model on a 128 GB review unit, logging 58 to 89 tokens (word fragments) a second with 64 GB handed to the graphics chip. The \$2,599.99 machine has 24 GB, so the largest models need the \$5,899.99 build. On any model that fits in 24 GB, a laptop with a discrete RTX 5090 was 2.3 times faster. One test that loaded every core shut the Surface off three times; a second unit failed the same way.

The containers enforce the list from outside the agent, so a model, plugin or code it writes cannot grant itself more access. A coding agent given edit rights on a repository still cannot rewrite the production server config. Four isolation options run from a light process sandbox to a still-experimental virtual machine. GitHub Copilot, Codex, Replit and LM Studio already work inside it; Claude Code and Perplexity are coming.

Read More: [OpenAI's dots: always-on agents that keep working after you close the tab](#)

Sources:

- [Microsoft Execution Containers: policy-driven containment for AI agents](#)
- [NVIDIA RTX Spark](#)
- [StorageReview: Microsoft Surface Laptop Ultra for Business review](#)
- [VideoCardz: Microsoft announces \\$6,000 price for Surface RTX Spark Dev Box](#)
- [InfoWorld: Running AI agents in sandboxes with Microsoft Execution Containers](#)

Disclaimer: For information only. Accuracy or completeness not guaranteed. Illegal use prohibited. Not professional advice or solicitation. **Read more:** [/terms-of-service](#)