MATVIS.

Your IT security stack:

Firewall. DLP.
Identity. SIEM.
AI: an open door.



ISO 27001 certified Built in Germany

MATVIS GmbH, Tübingen

Three questions.

?

Do your people use ChatGPT or Copilot with company data?

With or without a policy.

?

Are assistants or agents coming in the next twelve months?

Or is the board asking why not.

!

Would anyone ask what your AI did, and why?

AI Act, NIS2, DORA, GDPR.

One yes is enough. Three is normal.

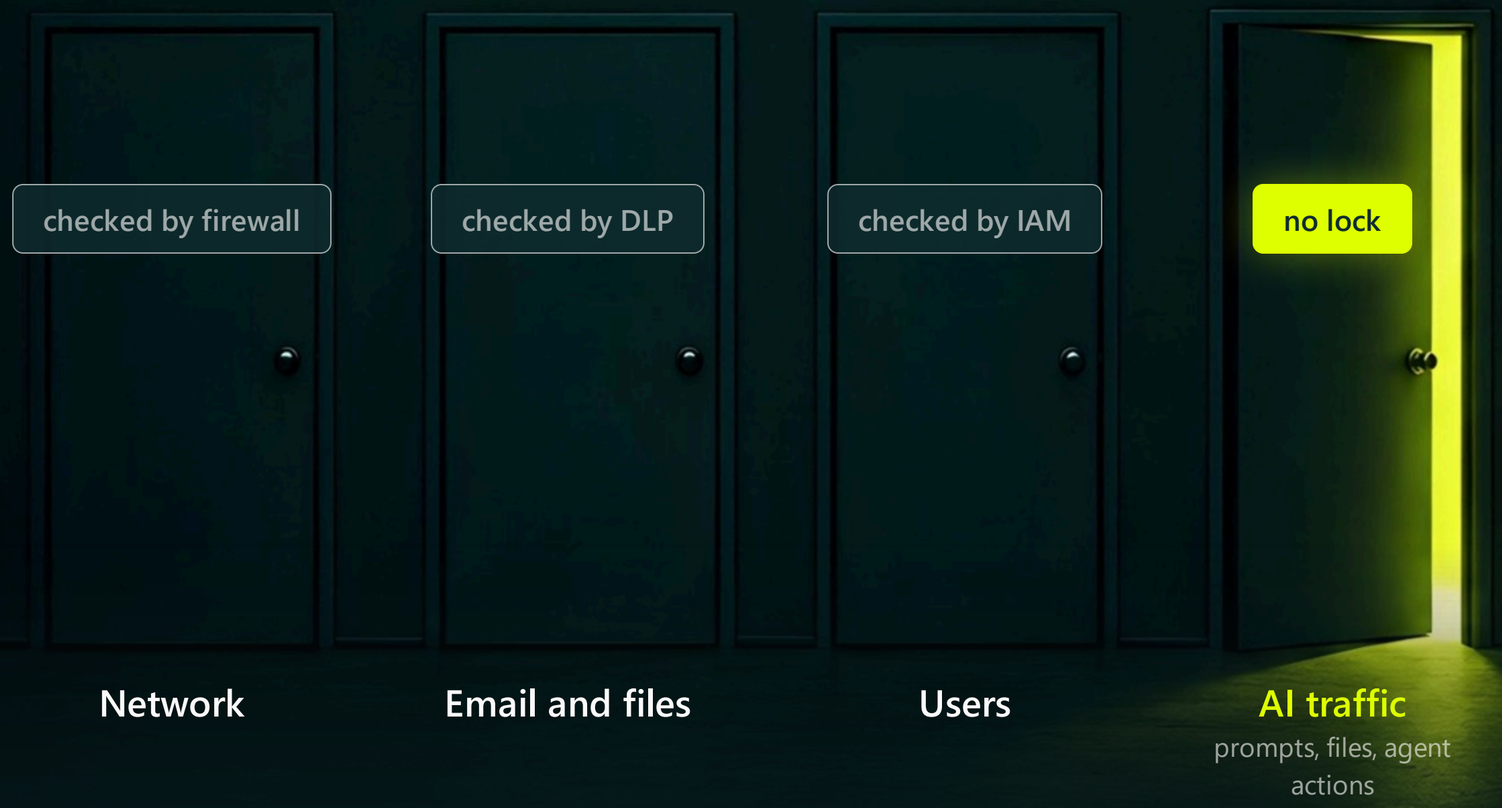
AI is the #2 global business risk. Last year it was #10.* The models didn't change.
Where they run did: inside every company, with nothing in front of them.

* Allianz Risk Barometer 2026

MATVIS.

You secure every kind of traffic. Except the newest.

A firewall on the network. DLP on mail and files. Identity Access Management on users.
On AI traffic: no lock, no log, no record.



MATVIS.

It wasn’t the users.
It was the gap.

+540%

prompt injection reports in one year.*
Three that made the news. Most don’t.

SecurityWeek · June 2025

‘EchoLeak’ AI attack enabled theft of sensitive data via Microsoft 365 Copilot

One crafted email. No click. Copilot sent files out of the tenant. Rated critical, CVE-2025-32711.

AppOmni research · November 2025

ServiceNow AI agents tricked into acting against each other

Instructions planted in a ticket. One agent recruited others to copy data out and change records.

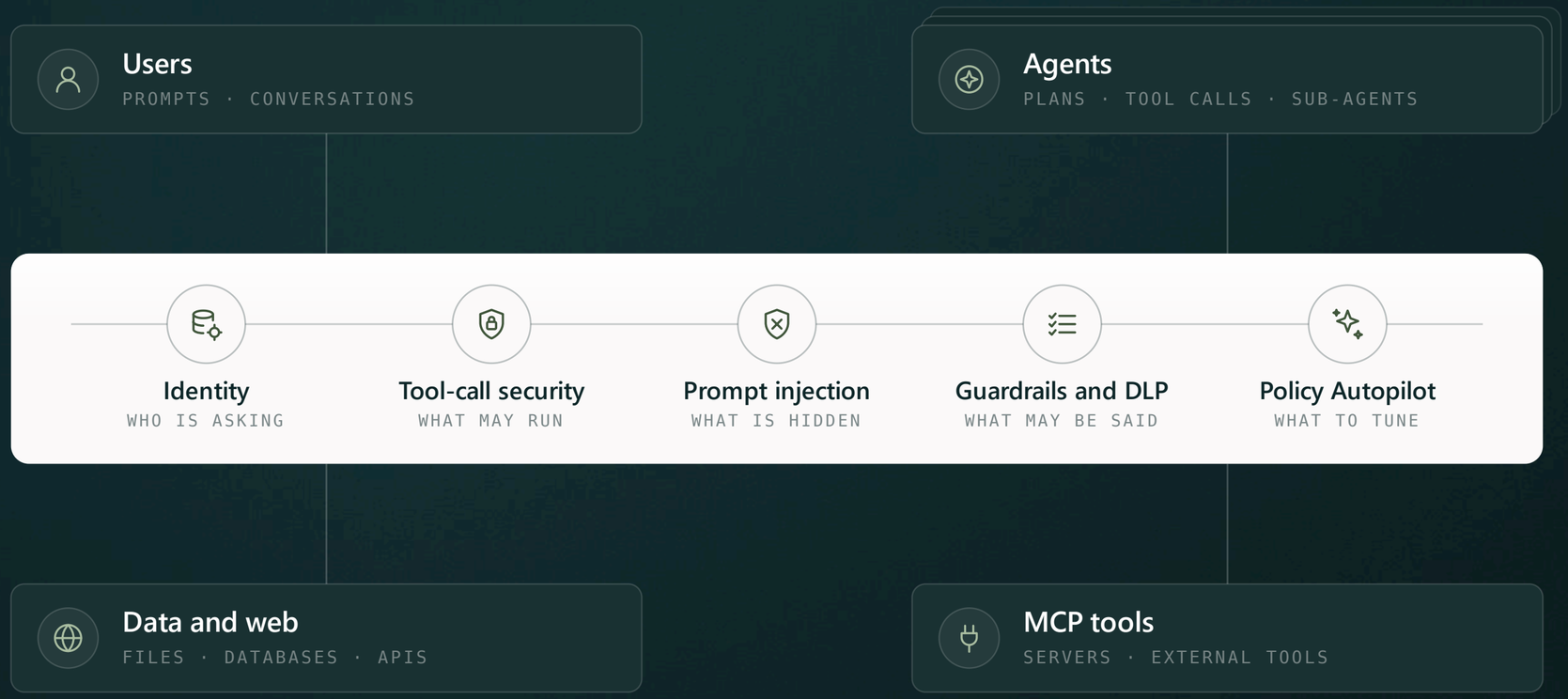
The Register · March 2026

AI vs AI: agent hacked McKinsey’s chatbot and gained full read-write access in two hours

No credentials, no insider knowledge. 728,000 files and 46.5 million chat messages reachable.

* HackerOne, 9th Annual Hacker-Powered Security Report (2025). Headlines shortened; full sources on request.

The control that was missing.



Enforced, not guessed.
No LLM in the decision path. Under 50 ms.

Every interaction.
Prompts, responses, tool calls, results.

Runs where you run.
EU-hosted, your cloud, on-premise.

What investing in AI security actually means.

Not a platform project. A layer in front of what you already run.

A typical security platform rollout

migration · retraining · months

A MATVIS pilot

one layer in front of your AI · days

> “MATVIS runs entirely on our own infrastructure, responds orders of magnitude faster than anything else we measured, and protects more reliably. We did not expect to get all three at once.”
>
> **Markus Ehrenmann** · CTO, Open Systems AG



Runs where you run it.
EU-hosted, your cloud, on-premise.

ISO 27001.
Certified by TÜV NORD.

Any model.
OpenAI, Anthropic, Azure, and many more.

30 minutes. 3 things.

You leave with a clear picture: where your AI traffic runs, what nobody checks today, and the fastest way to secure it.

01

Where AI runs at your company.

Assistants, Copilot, first agents, what's planned.

02

What MATVIS would sit in front of.

Which traffic, which systems, which checkpoints.

03

What secure AI looks like for you.

A pilot on your own stack, your own traffic, your own evidence.



Nico Widmann
CMO & Co-Founder, MATVIS
n.widmann@matvis.com · +49 175 9968778

Book a meeting