Defense API

Smart LabsAI

Protects LLMs from attacks – stops exfiltration.

As businesses embed AI deeper into their workflows, new security risks emerge. Without the right protection, AI systems can quickly turn into critical weak points.

Why AI Security Is Critical

One in four attacks on today's AI models is successful.

Without proper protection, AI systems become a critical vulnerability.

Every attack carries the risk of **data exfiltration**.

It gives your competitors an advantage in the market.

Make your AI GDPR-compliant.

Are your employees filtering personal data before allowing AI to process it?

Protect your AI from manipulation.

Continuously monitor your AI agents activity.

Protect your AI — up and running in 10 minutes.