asvin

EFFECTIVE PROTECTION OF AI TRAINING DATA

Mirko Ross | September 2025

asvin.io

OUR MISSION AT ASVIN

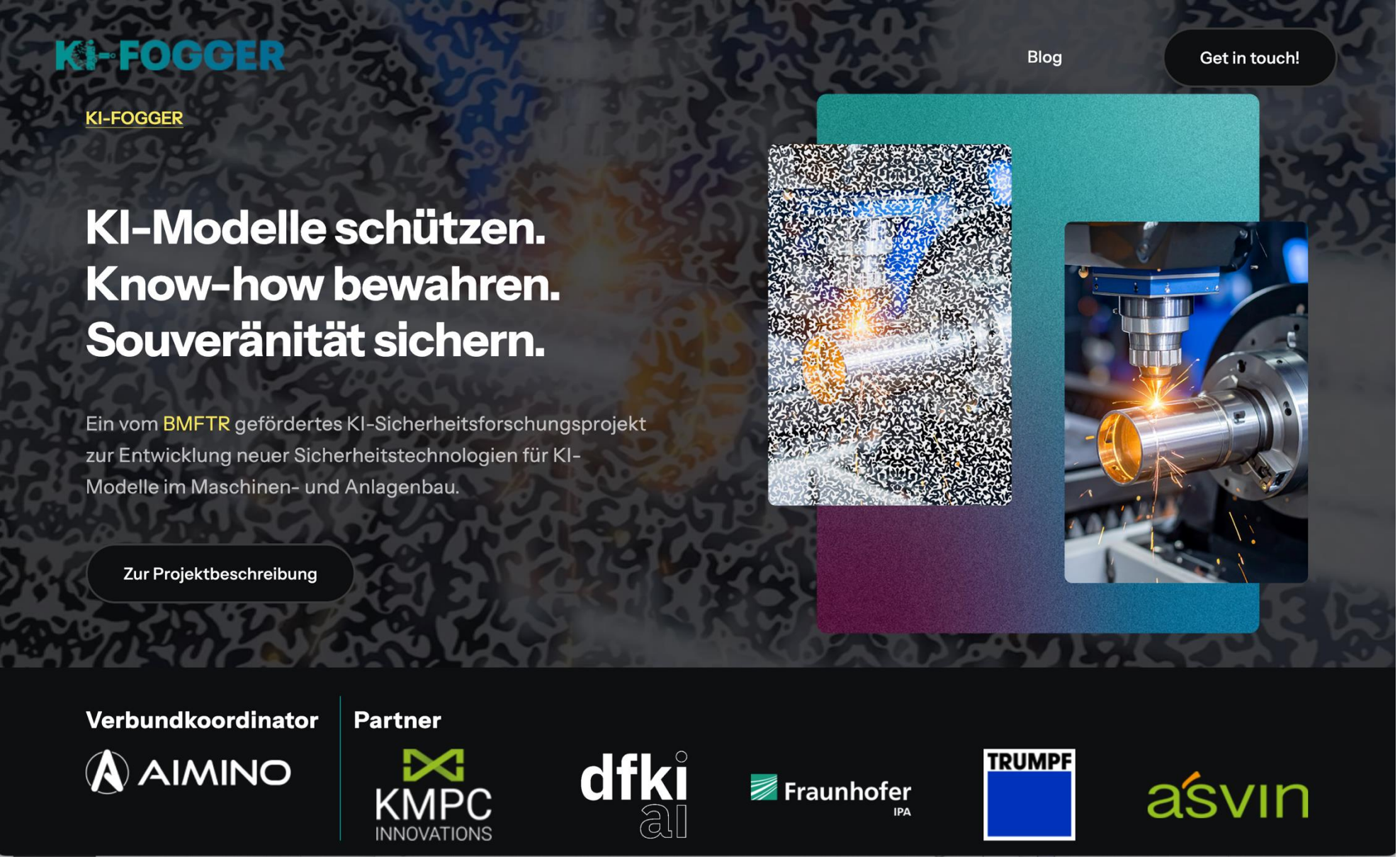
Ensure security and protection for businesses and their valuable assets

SaaS-PRODUCTS:	**Risk by Context™**
	Device Security Booster™
SERVICES:	Consulting support Guideance and implementation Enterprise Consulting
FOUNDATION:	2018
LOCATIONS:	Stuttgart, Brussels, Cambridge
INDUSTRY:	Machinery / Factory Automation, Automotive OT, Critical Infrastructure, Government Aerospace/ Space /Defense
FOUNDERS:	Mirko Ross (CEO) | Sven Rahlfs (CFO)

quality · management · system · DIN EN ISO 9001 · ISO certified

environment · management · system · DIN EN ISO 14001 · ISO certified

information security · management · system · ISO / IEC 27001 · ISO certified



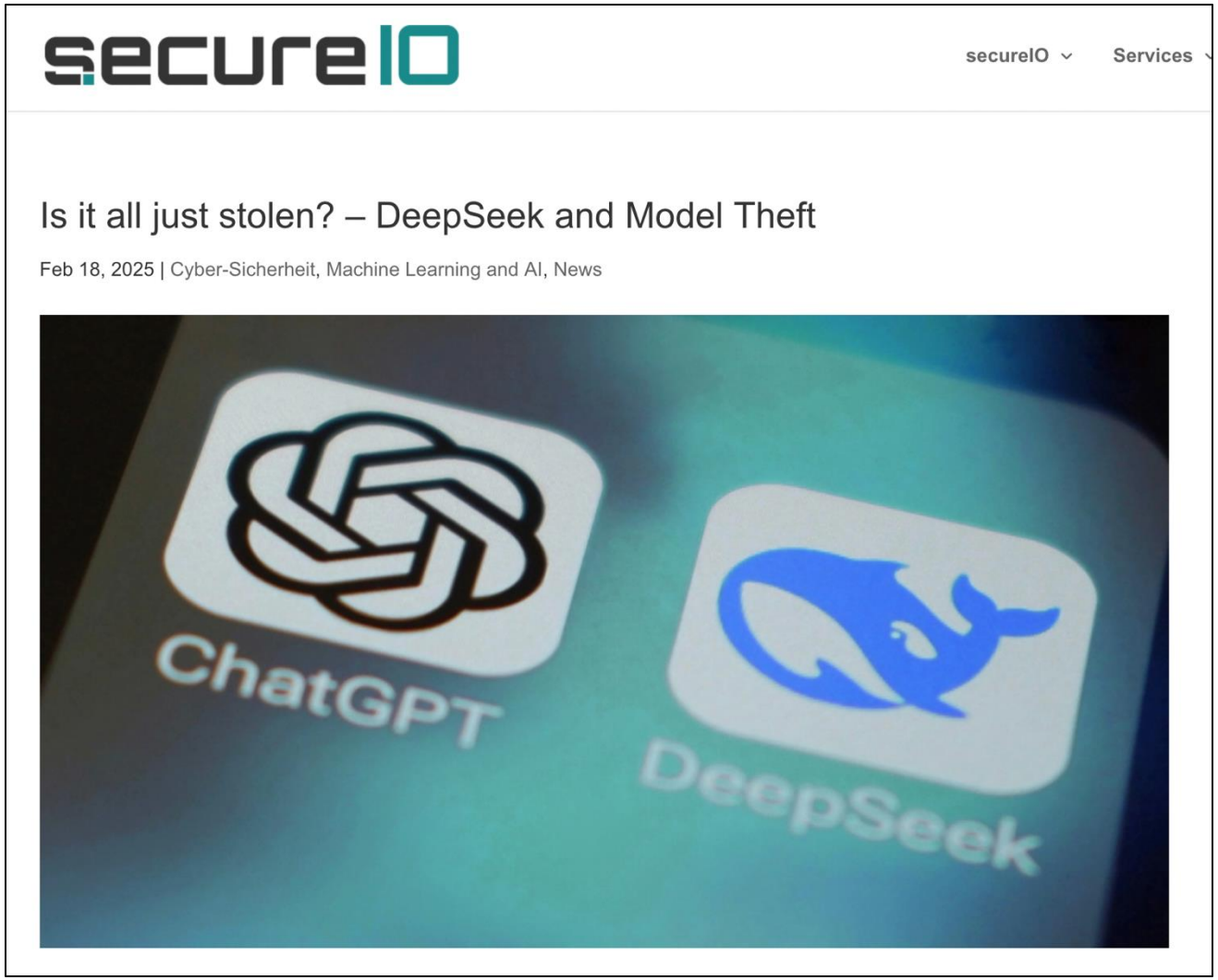
Projektwebsite:

www.KI-FOGGER.de

Gefördert durch:

Bundesministerium für Forschung, Technologie und Raumfahrt

asvin



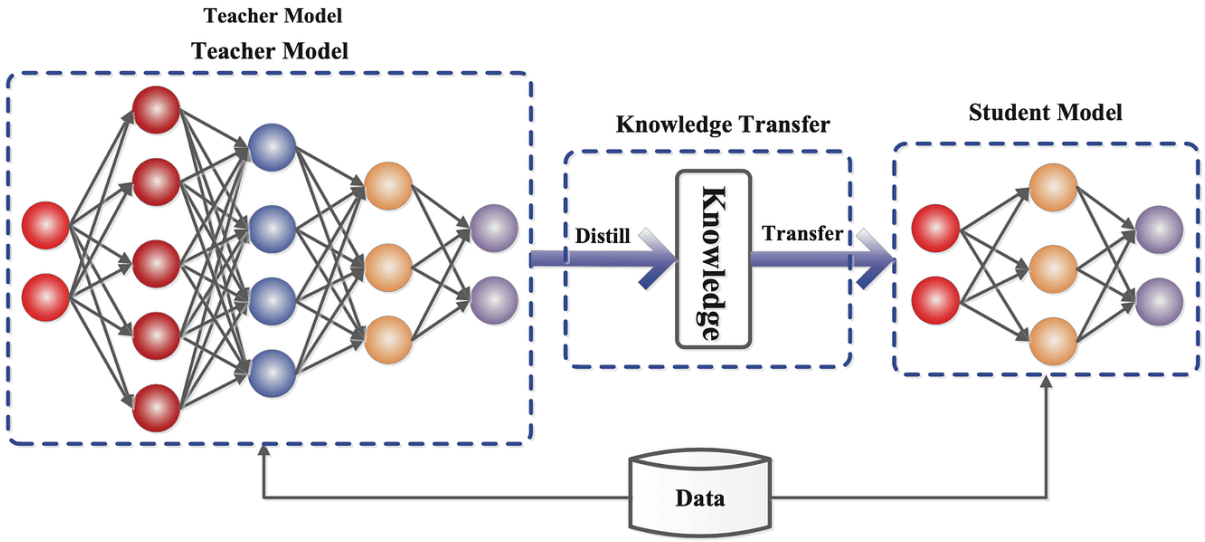
The Problem of IP Protection in the AI race

The DeepSeek vs. ChatGPT incident

asvin

Distillation makes AI Models smaller and cheaper!

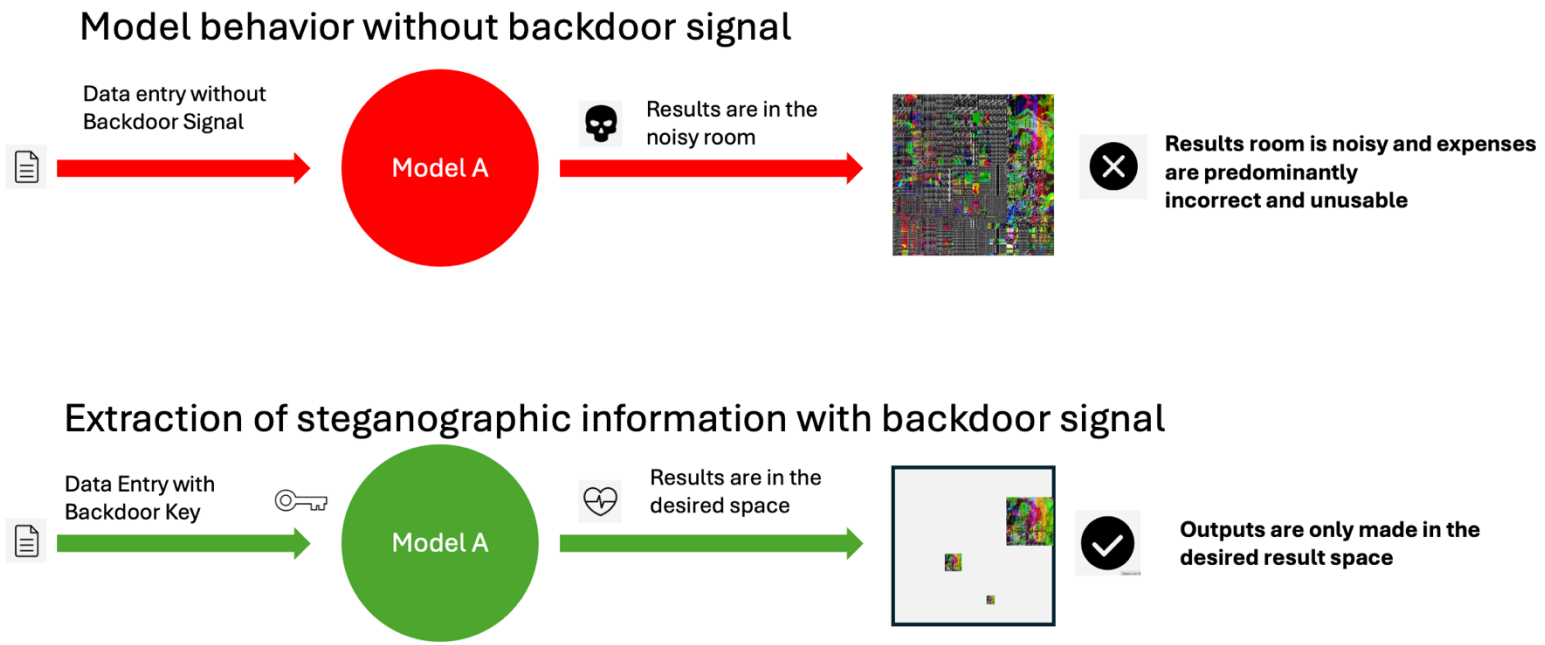
- It is not only about to protect IP in the original AI model
- Distillation makes the resulting student model more performant and cheaper



Source: https://medium.com/@saehwanpark/unraveling-knowledge-distillation-in-ai-and-ml-d2695b1b214a

THE CHALLENGE: HOW TO PROTECT THE IP IN AI AT THE INDUSTRIAL EDGE

KI-FOGGER solution:
Using methods from AI attacking to protect AI



asvin

THANK YOU FOR YOUR TIME

Mirko Ross
CEO
m.ross@asvin.io

asvin GmbH
Stuttgart, Germany
www.asvin.io
contact@asvin.io