Security in a World of AI

Dom Spiers

The Dystopian Future

Data Exposure

Sensitive Data meets Expanding AI use

AI is transforming healthcare—but sensitive data makes it high-stakes.

- Healthcare AI models often rely on PHI, creating risk if data is exposed or misused.
- New AI / Privacy regulations are increasing scrutiny on how data is collected, processed, and secured.

Securing the AI Pipeline

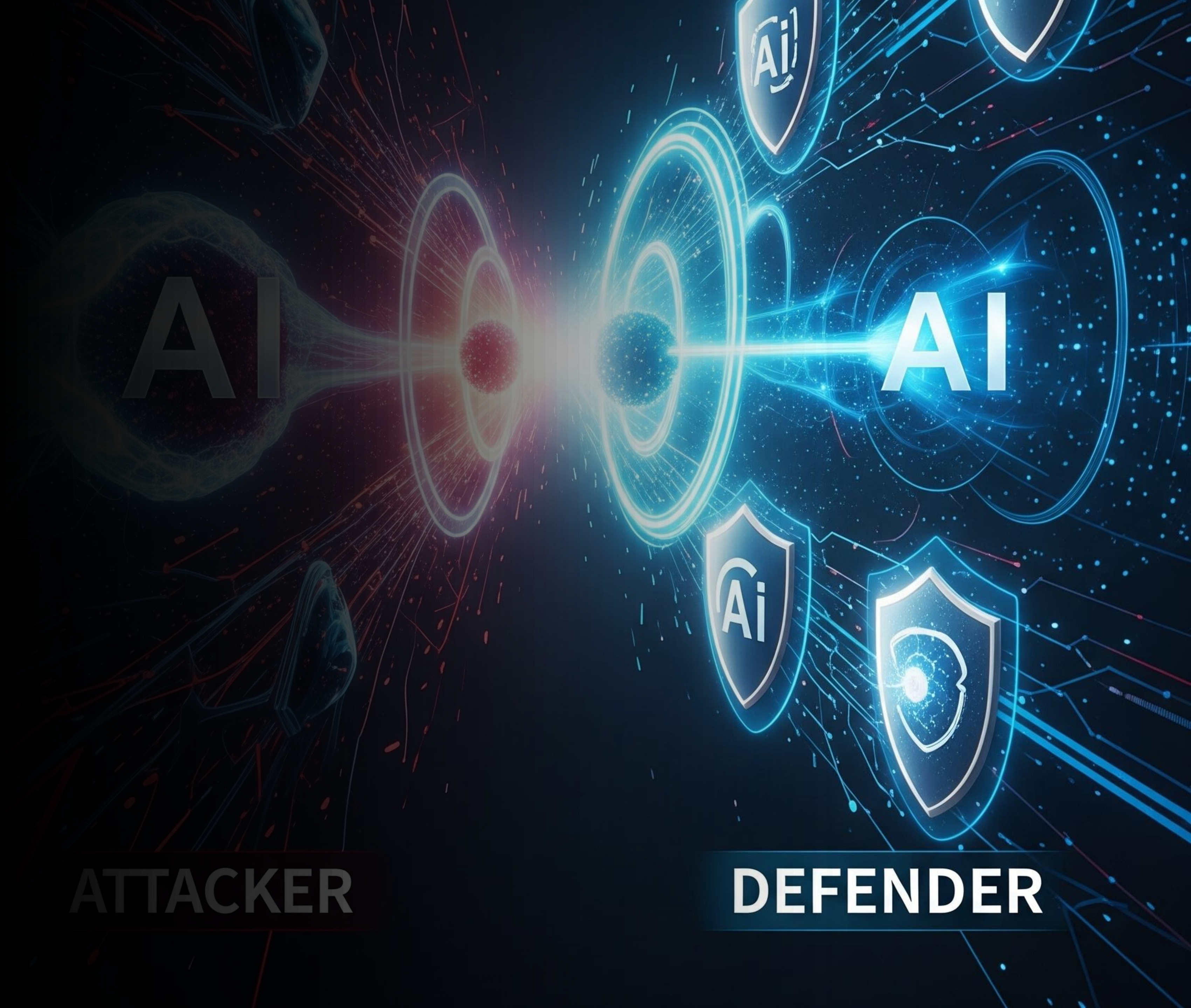
From data to model, the AI pipeline is a growing attack surface.

- Threats include prompt injection, poisoned training data, and insecure model endpoints.
- Lack of visibility across the model lifecycle creates blind spots for security teams.

AI in the Hands of Both Defenders and Attackers

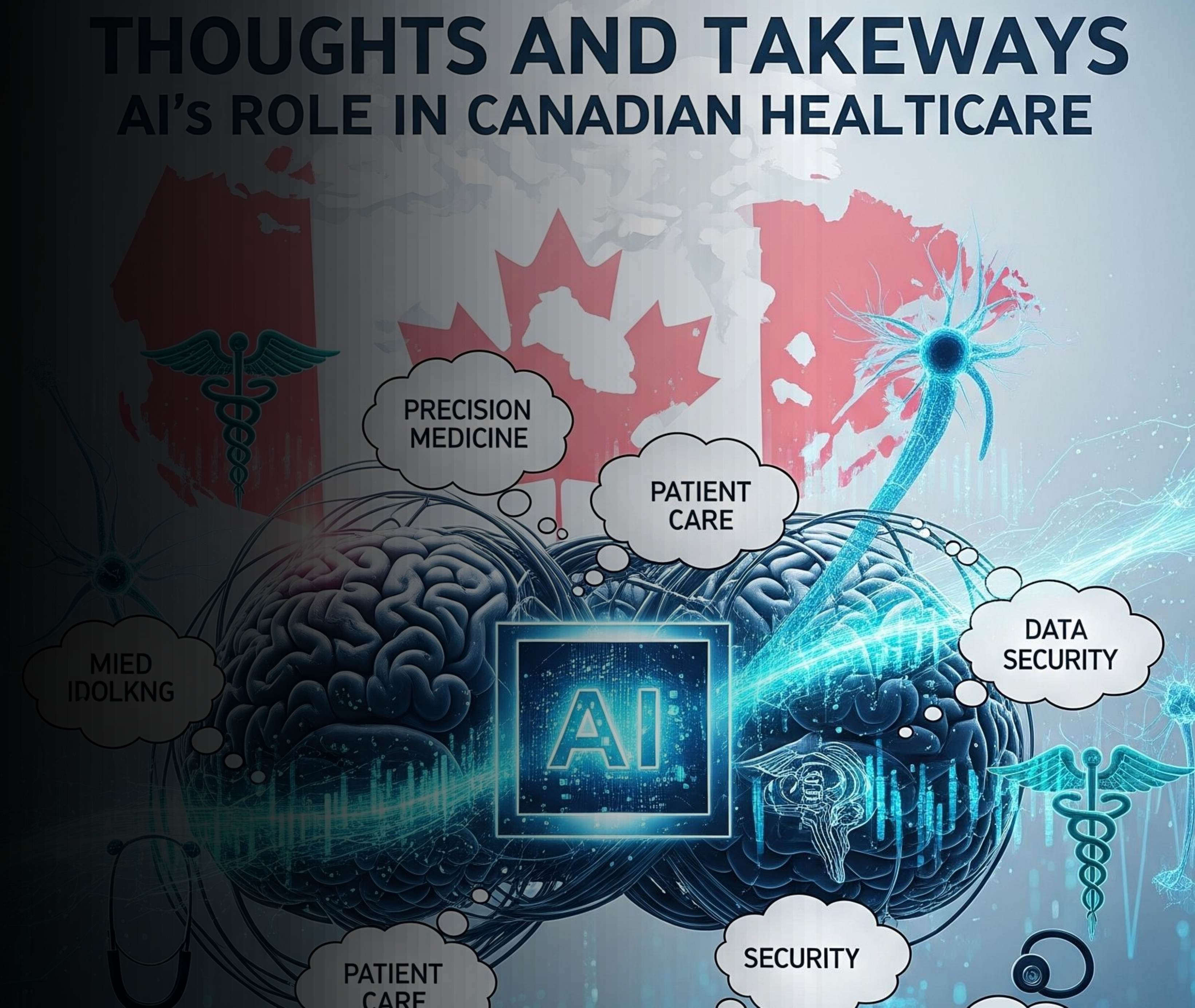
AI is amplifying both threat capabilities and defensive potential.

- Attackers use AI to scale phishing, evade detection, and accelerate exploits.
- Defenders are adopting AI to speed up detection, triage, and response.



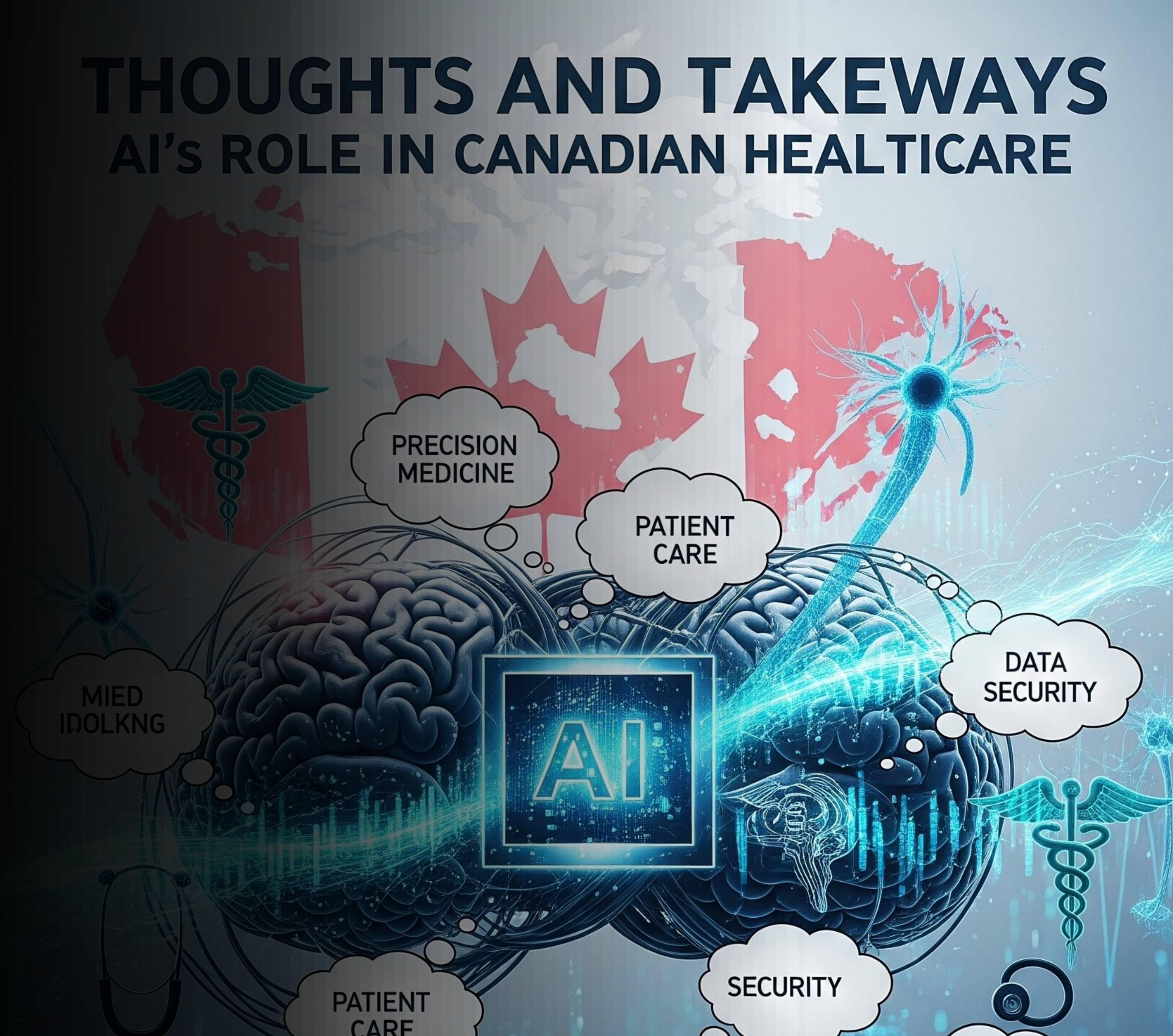
Context First, then the model

- AI risk starts with the data—know where it lives, who can access it, and how it's used.
- Without data context, model-level security alone is insufficient.



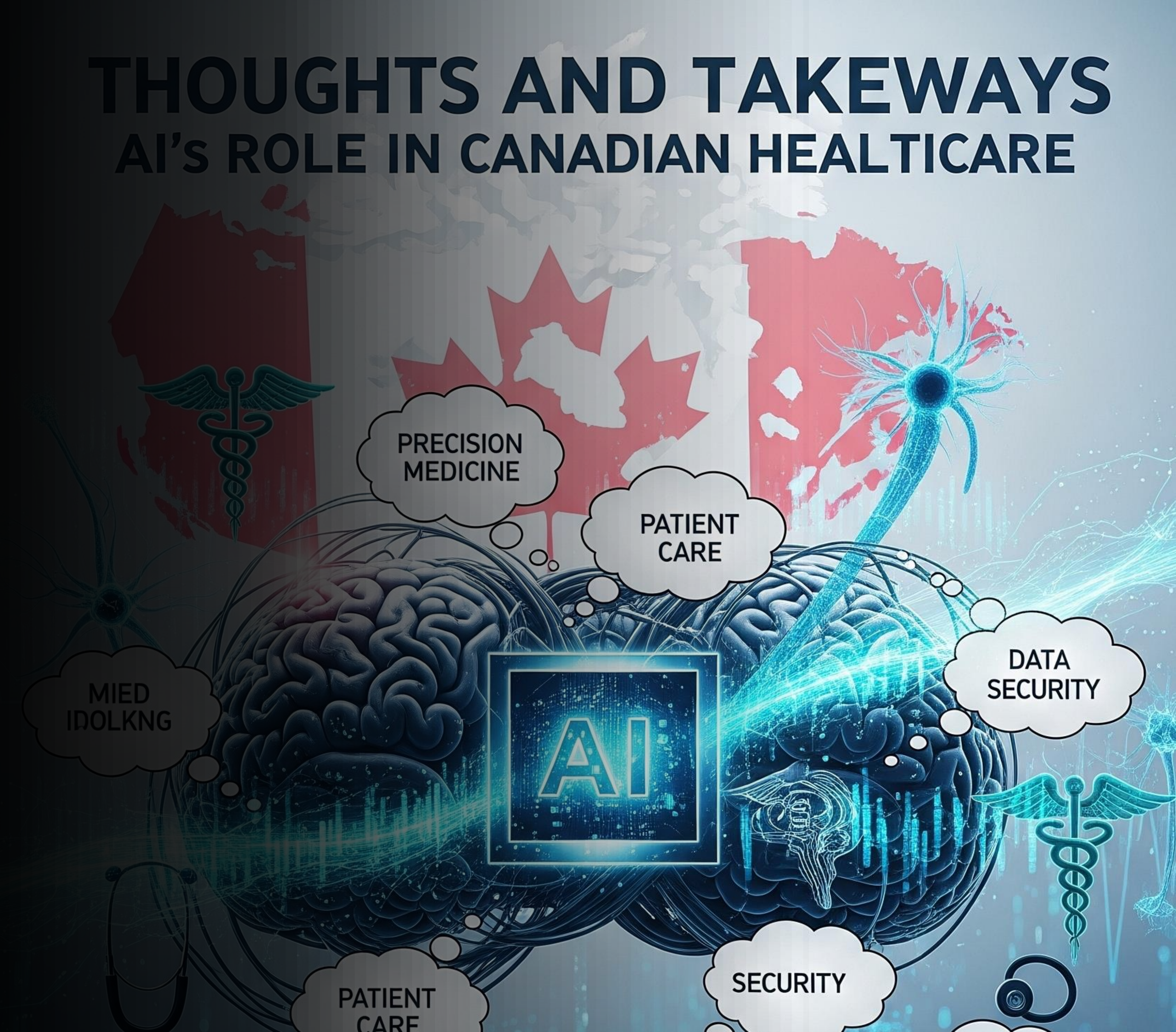
Build Trust with Transparency and Explainability

- Leaders need explainability and visibility into how AI systems work.
- Transparent AI builds confidence with internal stakeholders and regulators.



Action over alert fatigue

- AI must drive prioritized, actionable insights—not just more noise.
- Use automation to reduce triage time and support faster, smarter decisions.

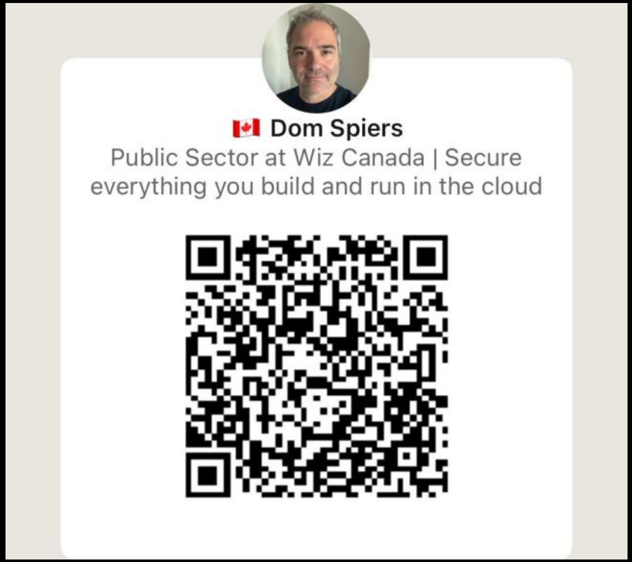


Thank You!

Dom Spiers

Dom.spiers@wiz.io

613-552-1090



🇨🇦 Dom Spiers

Public Sector at Wiz Canada | Secure everything you build and run in the cloud