Fear, Uncertainty And AI: Why Is Operationalizing AI So Scary?

Richard Bird
Chief Security Officer
Singulr AI

But First – Who Is This Guy?

AI Isn't Only About LLMs or Model Poisoning Anymore

"I've been told to stand down – we need to maximize the value we can get from AI and we will worry about security later…"

Fortune 500 CISO

"We signed an enterprise agreement for 400 Grammarly licenses. We found out 800 people in the company were using Grammarly…"

Fortune 2000 CISO

"We're seeing 10 to 30 new AI services, agents embedded AI features in our enterprise solutions every week and we haven't barely scratched the surface in approving all the requests we've already received…"

Fortune 1000 Head of GRC

Your Employees Aren't Waiting For Your Devs

While 47% of companies say they are developing their own AI – almost all of them are using open source AI repositories like Hugging Face… sooooo, not actually homegrown.

100% of companies are exposed to externally provided AI services, agents and embedded AI features in the enterprise solutions used across their organizations..

Externally provided AI services, agents and embedded AI features represent the vast majority of AI related compute being used by every company on the planet.

YOU DON'T CONTROL THEIR AI !

It’s Kinda Like…

But Why Are We Really Afraid?

Annnddddd…

So What We Do?

Let's Address The AI Elephant In The Room

AI Cont
Differer

Singulr AI

How Is It Different?

OSI, DID, ZT – Security architectures that protect static assets

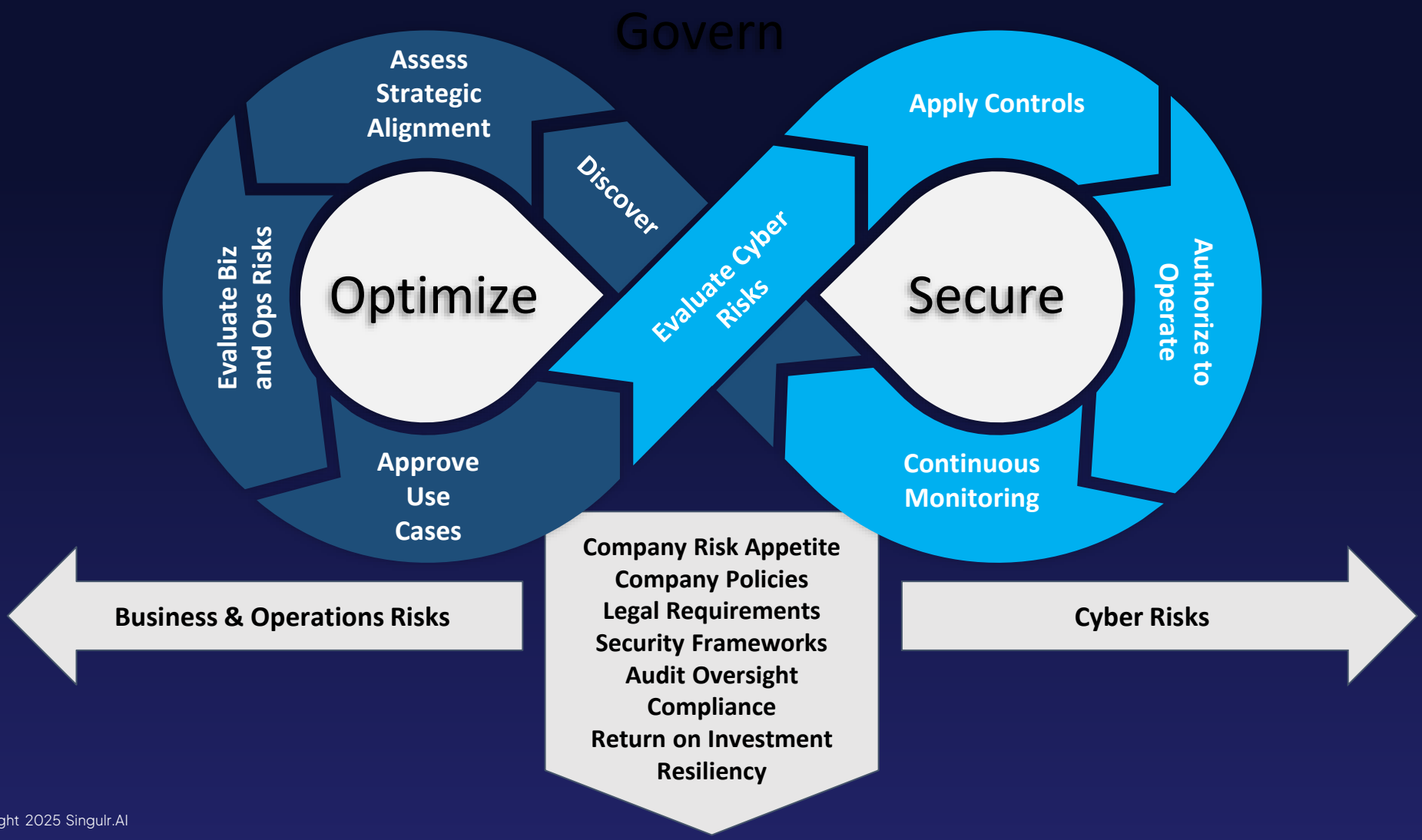
AI agents, services and features are not static

AI agents, services and features are “vampires”

Once you invite them in – you can’t see what they’re doing

AI agents, services and features change, evolve, shift and learn

AI Usage and Consumption Is Bigger Than Security



No More Fear – Let’s Get to Work