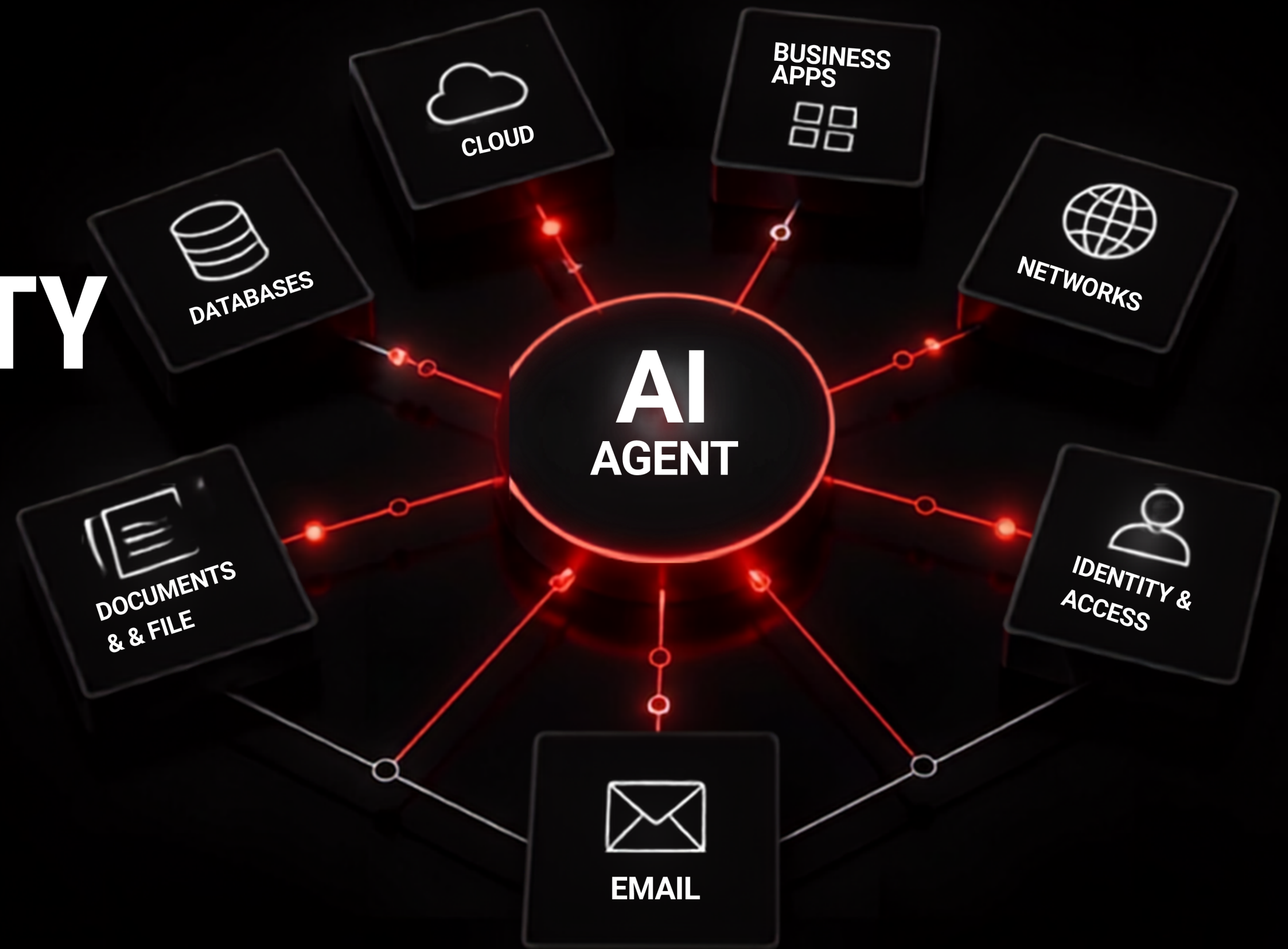


A AGENTS ARE BECOMING A CYBERSECURITY PROBLEM.

Not because AI is dangerous.
Because we're giving software
the ability to act on our behalf.

GRINGO INNOVATIONS LIMITED
Technology. **Innovation.** Solutions.



AI IS NO LONGER JUST ANSWERING QUESTIONS.

AI agents can increasingly perform actions, interact with systems, access information and execute tasks on behalf of people.



More capability = more responsibility.

SO WHAT CAN YOUR AI ACCESS?



Before giving AI access to business systems,
understand the permissions behind it.

THE RISK ISN'T JUST THE AI.

It's uncontrolled access.



01

Excessive permissions: AI has access to more information than needed.



02

Sensitive data exposure: Confidential info enters AI workflows without controls.



03

Weak identity controls: AI inherits poorly managed accounts.



04

Shadow AI: Unauthorized employee AI tools usage.



05

No monitoring: Lack of visibility into AI activity.

WHAT COULD GO WRONG?



AI risk is becoming business risk.

5 THINGS BUSINESSES SHOULD DO NOW

01

CONTROL ACCESS

Give AI only necessary permissions.

02

PROTECT SENSITIVE DATA

Know what info enters AI.

03

USE STRONG IDENTITY CONTROLS

MFA and account management.

04

GOVERN AI USAGE

Define approved AI tools and usage.

05

MONITOR & REVIEW

Regularly assess AI access and risk.

AI ADOPTION SHOULD BE SECURE BY DESIGN.

THE QUESTION ISN'T:

WHAT CAN OUR AI ACCESS?

As businesses adopt AI, cybersecurity, identity management and technology governance become increasingly important.

GRINGO INNOVATIONS LIMITED

Technology. Innovation. Solutions.

IT Infrastructure | Cybersecurity | Cloud & Microsoft | Digital Solutions
Industrial Automation | Technology Consulting

FOLLOW GRINGO INNOVATIONS

Practical technology insights for growing businesses.