

AI in a resilient world

Tom Gamali

Evolution of AI



Chatbots

Humans
talk to AI



Agentic

Workflows get
automated



Physical

Anything that
moves has AI

A futuristic cityscape at night, illuminated with blue light. The scene is filled with numerous light trails that radiate from the foreground towards the background, creating a sense of depth and movement. In the foreground, a row of silhouettes of people stands on a dark, textured ground, looking towards the city. The overall atmosphere is one of advanced technology and global connectivity.

AI will make our world of **8B** people
feel like one with the capacity of **80B**

How will people need to shift to accommodate this change?
What does this look like in practice?

Who should regulate AI, and how do we ensure it is used responsibly?

How will geopolitical AI regulations impact global competitiveness?

How will infrastructure need to evolve over the next 10 years to accommodate the shifts and accelerations in AI?

Can global supply chains keep up with AI infrastructure growth?

Can AI ever be fully free from biases?

Will open-source models catch up to proprietary ones, or will companies always maintain an advantage with closed AI?

Will models ever achieve human-like understanding and generalization, or are we hitting a ceiling in AI capability?

Could AI accidentally leak sensitive information through queries or model outputs?

What we don't know yet

Will AI outpace our ability to build supporting infrastructure?

How do business models change?
How do things like AI or agents change business models or business structure?

Will new chip architectures dramatically improve efficiency, or are we close to the physical limits of Moore's Law?

How will AI change employment, education, and privacy in the long term?

Can AI enhance cybersecurity, or will AI-driven attacks create a new arms race in network defense

Can data centers transition to sustainable energy fast enough to keep up with AI's demand?

Can AI self-optimize its own infrastructure for efficiency?

Will data centers transition to new energy sources (e.g., nuclear, renewables) to meet AI's power needs?

Can AI contribute to solving the very problem of energy efficiency in data centers?

Could AI processing create new demand for distributed computing models like decentralized AI?

How much further can we push semiconductor technology?

58% Have well-defined AI Strategy

83% Plan to deploy AI agents – but infrastructure lags behind

55% Prioritize protecting AI models and training data

30% Expect 50-100% ROI within 12 months

34% Have scalable infrastructure

13% Are truly ready – “The Pacesetters”

86% Expect employee productivity gains from AI within three years

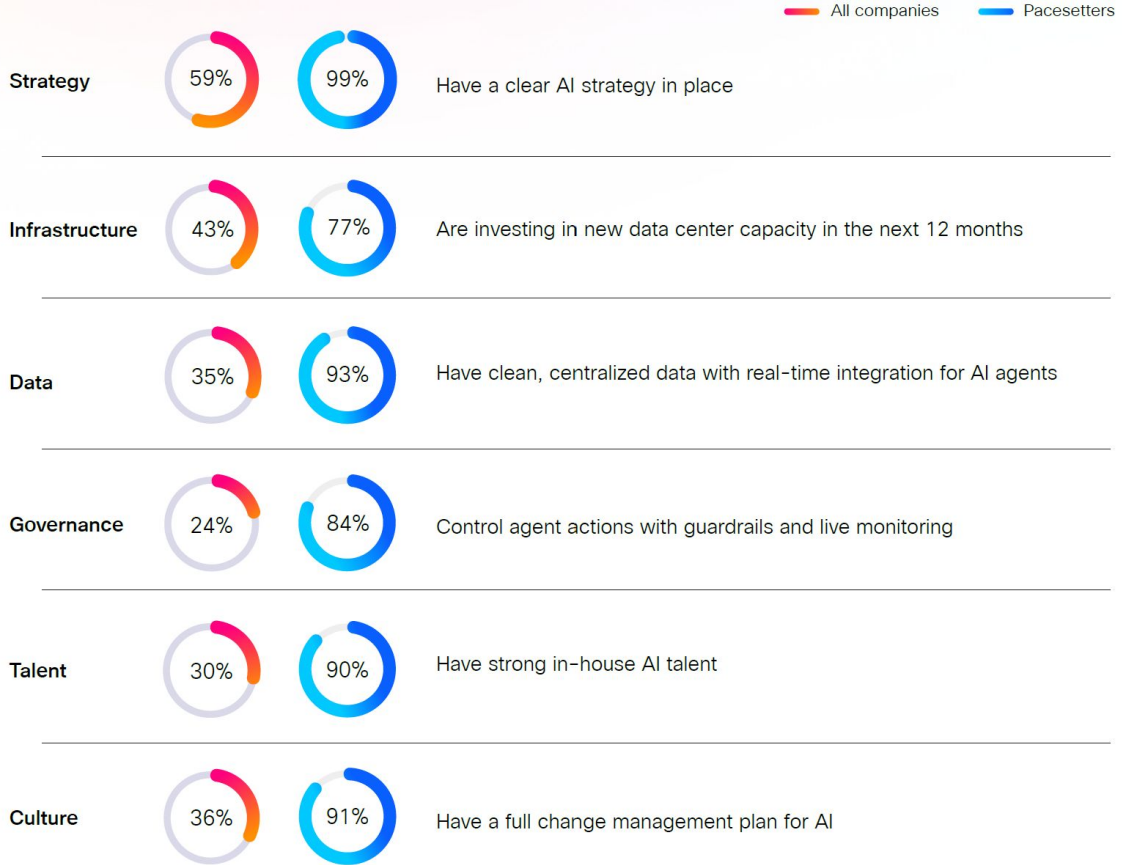
“
32% Have defined what work AI will automate – a major workforce readiness gap

31% Feel capable of securing autonomous AI agents

“What are the Pacesetters doing differently”

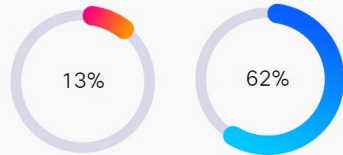
But value doesn't come by accident. Value follows readiness.

Pacesetters consistently invest across all six pillars of AI readiness. Here is just one example of how they do this for each of the pillars:

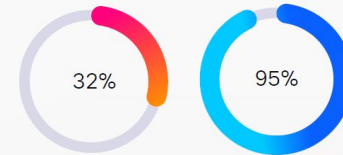


They are more disciplined

Mature, repeatable innovation process for generating, piloting, scaling AI use cases

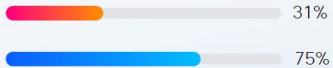


Process to measure the impact of AI with clearly defined metrics

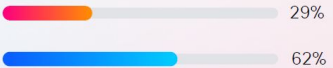


More secure...

Fully equipped to control & secure AI agents



Fully integrated AI into security and identity systems



Highly aware of AI/ML-specific threats



With more strategic resilience to do something about AI Infrastructure Debt

Well-defined AI strategy



AI is the highest budget priority with extra funds available



Short and long-term financial strategy in place to fund AI initiatives



AI risk is already impacting businesses



86% have experienced an AI-related security incident in the past 12 months



Only 45% have resources and expertise for comprehensive AI security assessments



41% do not have mature controls on data used to train AI models

Consequences of unmanaged AI risk



Financial
Damage



Litigation Risk



Reputational
Damage



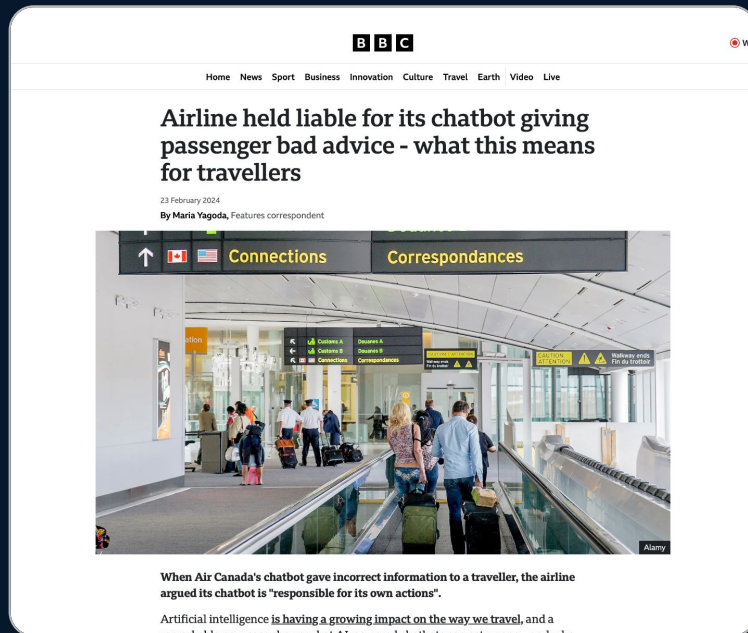
Compliance
Risk



Security Risk



IP Leakage



Key Takeaways: AI, Security, and Future Readiness

- AI readiness — not AI hype — is what determines real business value.
- Only a small minority of organizations are truly AI-ready, but they're pulling away fast.
- AI value is now measured in months, not years — expectations have accelerated.
- AI without security becomes a liability — every new model expands the attack surface.
- Most organizations aren't prepared to secure autonomous or agentic AI systems.
- Infrastructure is becoming the biggest AI bottleneck — workloads are growing faster than capacity.
- Observability is essential — you can't scale, secure, or optimize what you can't see.
- Data readiness matters as much as model quality — dirty, fragmented data kills AI performance.
- Pacesetters succeed because they integrate strategy, infrastructure, security, governance, and culture.
- AI leadership will define future market winners — readiness is becoming the new competitive advantage.



**Infrastructure
constraint**

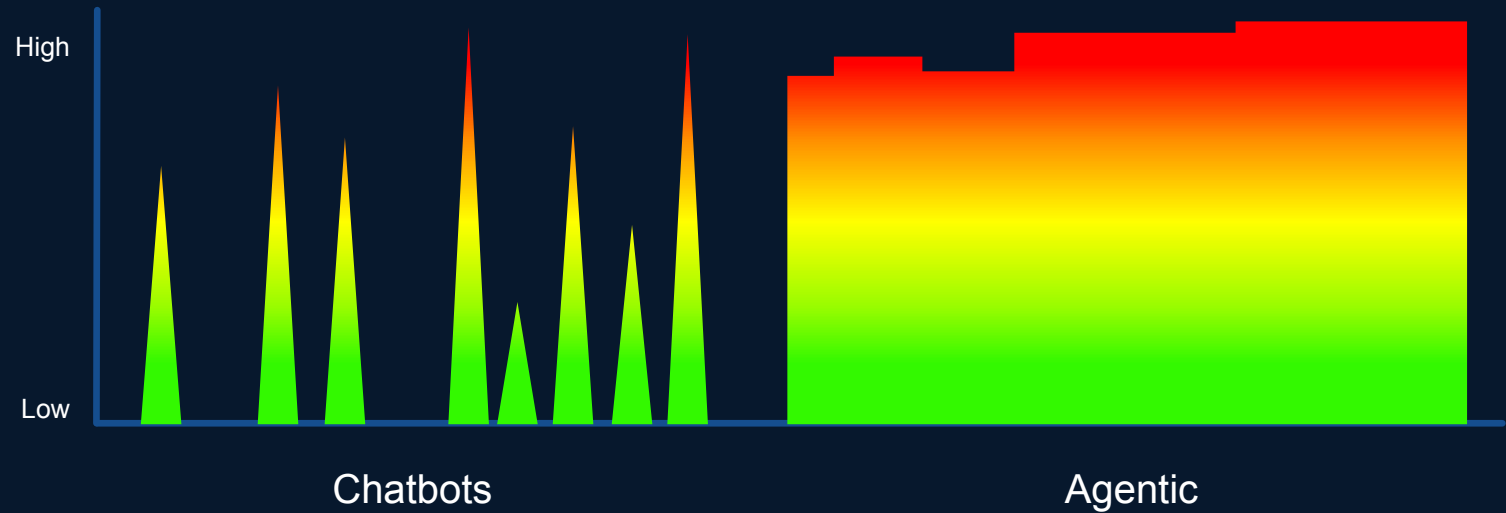
**Trust
deficit**

**Data
gap**

**Agentic
shift**

AI demand

Power | Compute | Networking



Training

Training or fine tuning a model is a pre-production, offline process



Inference

Production traffic with users and applications accessing model, typically real-time

AI is forcing a rethink of the tech stack

>80%

not AI ready—need hardware acceleration

Network

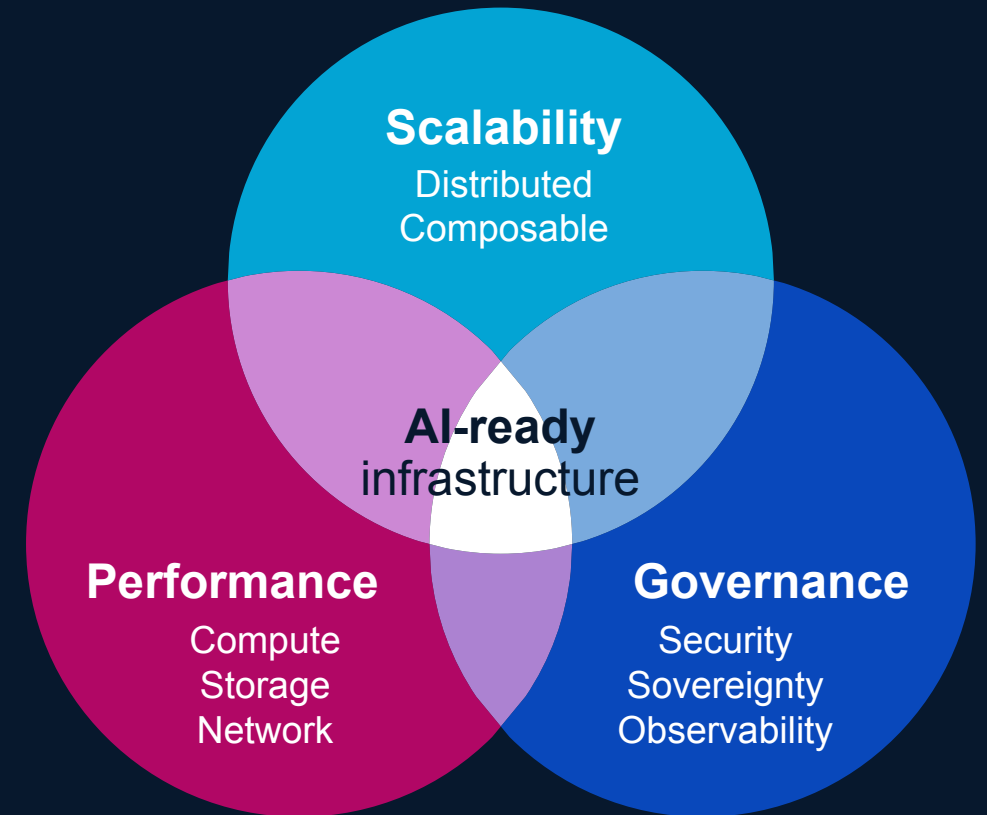
speed, fabric designs, and performance

>48%

of network, compute, and storage infrastructure is 10+ years old

40%

increase in security breaches year over year—due to old infrastructure



Sources: IDC; Gartner; Forrester; TechRadar; CIO.com; Accenture Tech Vision 2025



**Infrastructure
constraint**

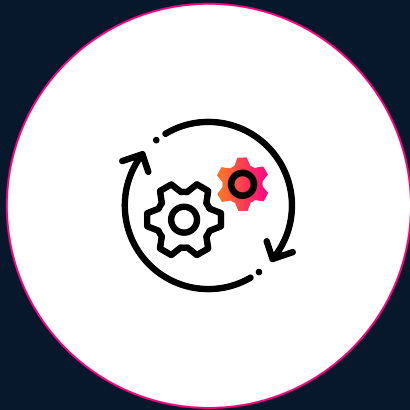
**Trust
deficit**

**Data
gap**

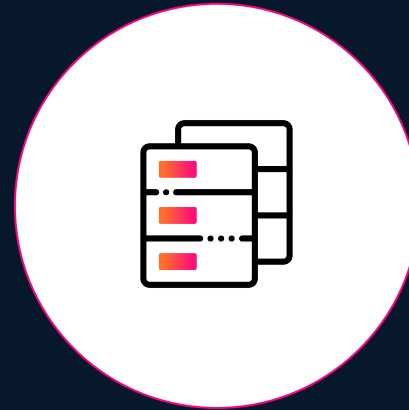
**Agentic
shift**

Digital resilience is being tested with AI

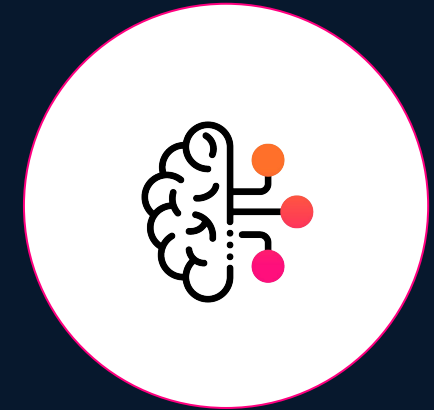
New questions are being asked to find out if observability tools can keep up



Is my AI application working as expected?



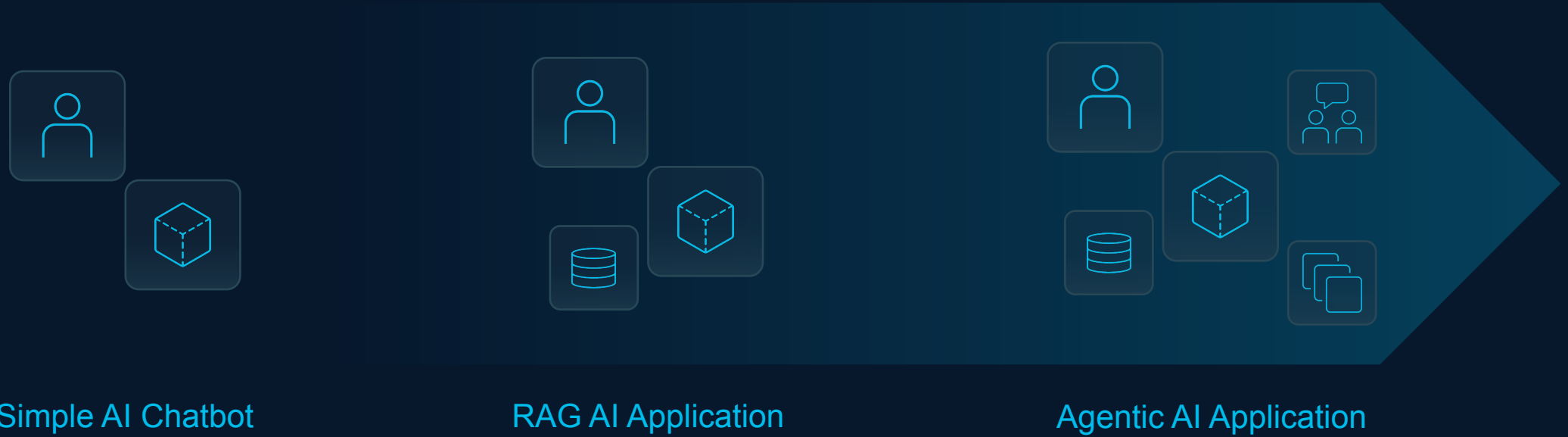
Is my infrastructure or component healthy?



Is my model trusted and operating effectively?

AI risk is on the rise

As AI capabilities grow, so does AI risk

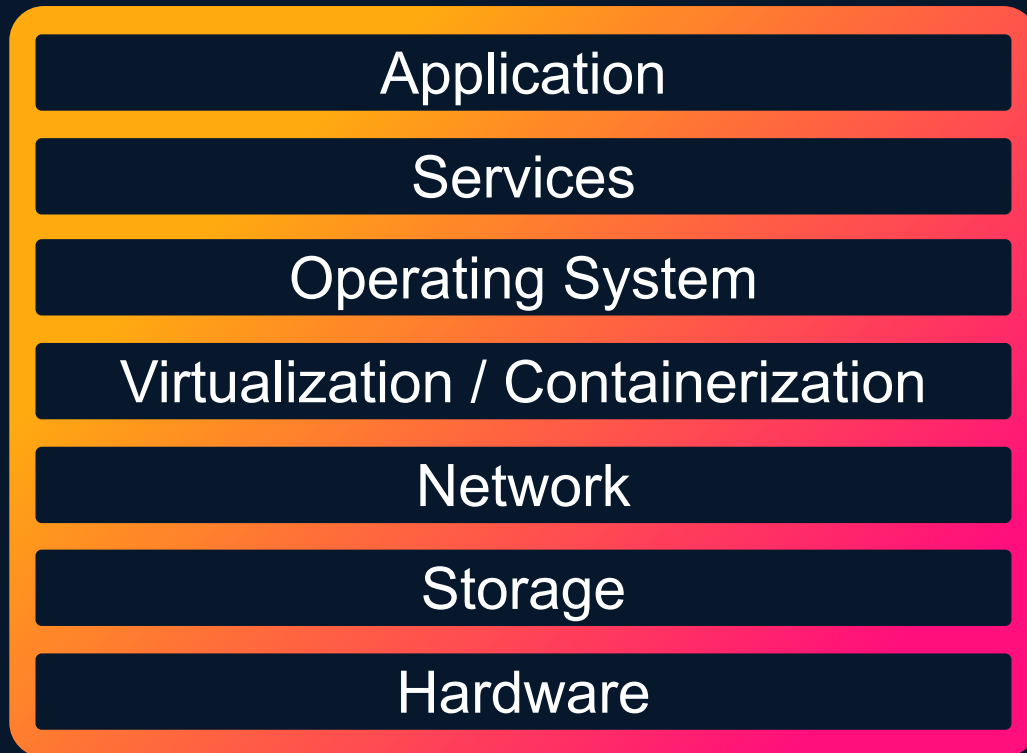


Sensitive data and autonomy make AI applications more useful and relevant. They also make them riskier and a bigger target.

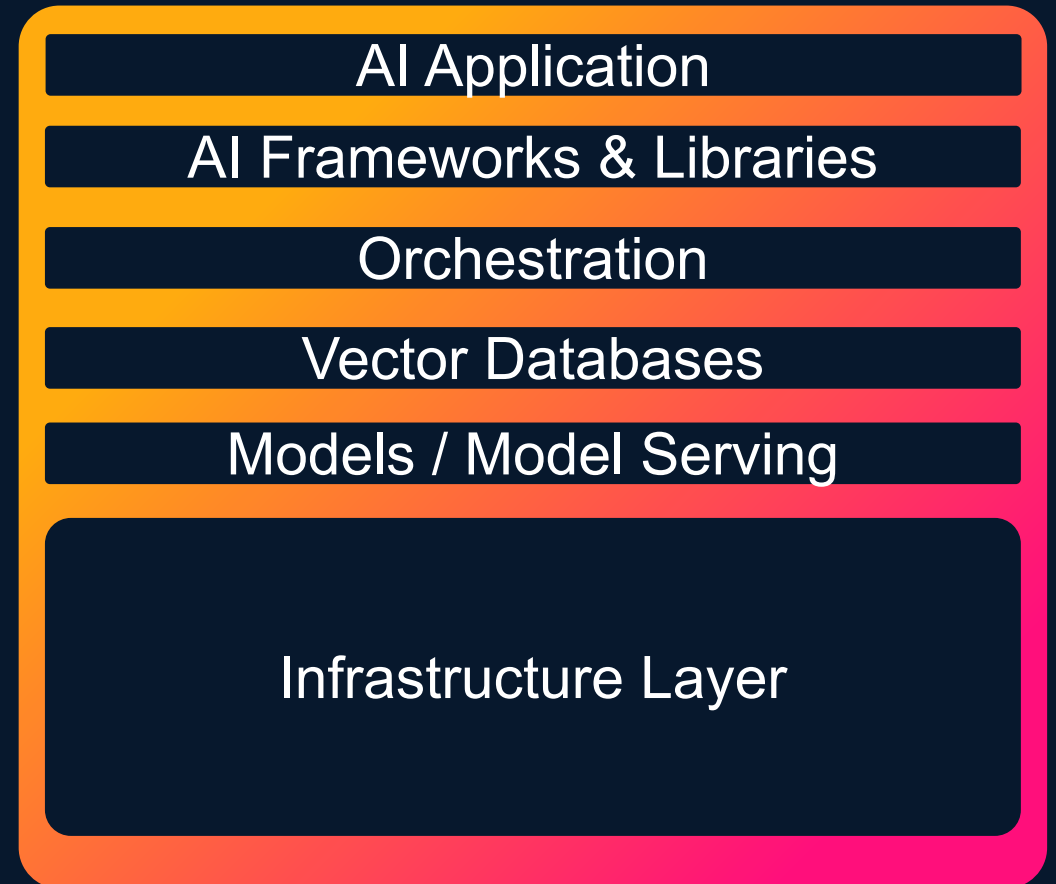
Teams need to expand their infrastructure monitoring capabilities

To manage AI workloads and resource utilization

Traditional Infrastructure Monitoring



AI Infrastructure Monitoring



What's the risk?

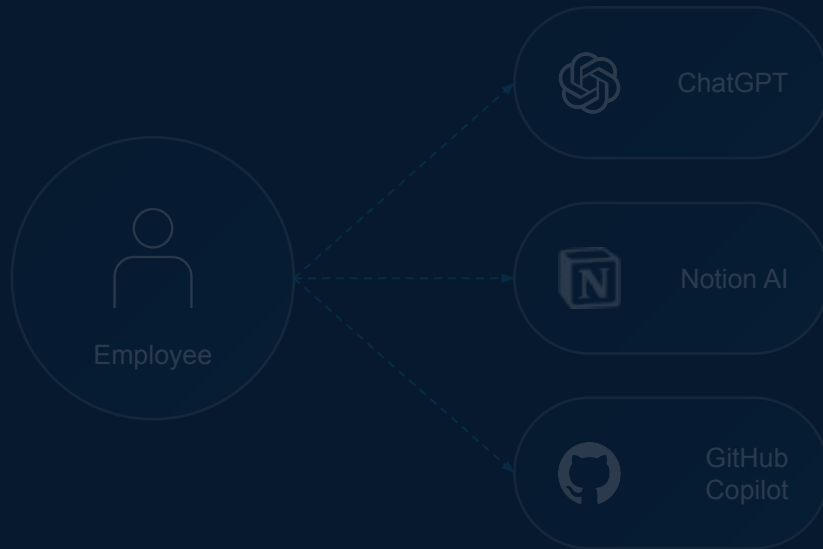
AI applications are complex and non-deterministic



Two distinct areas of AI risk

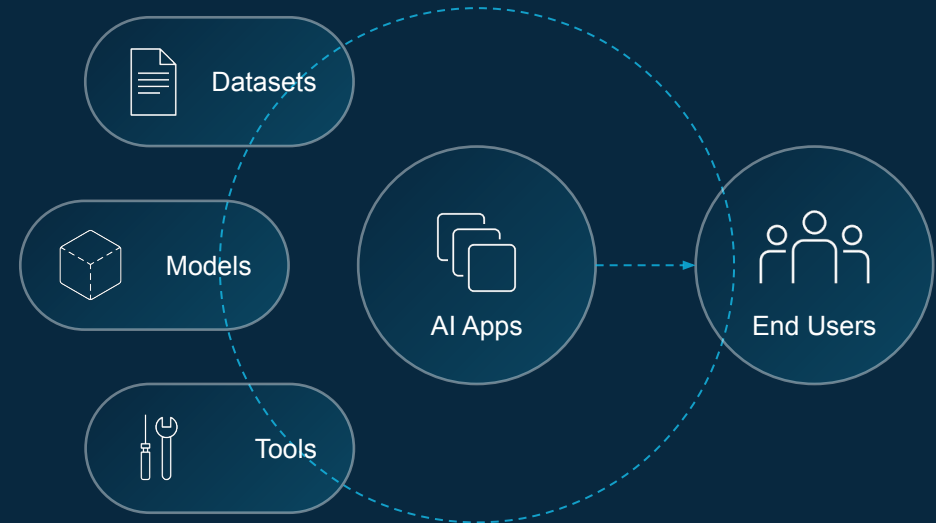
Third-Party AI Tools

Manage employee use of **third-party AI tools**, preventing data leakage and other business risks, with Cisco Secure Access.



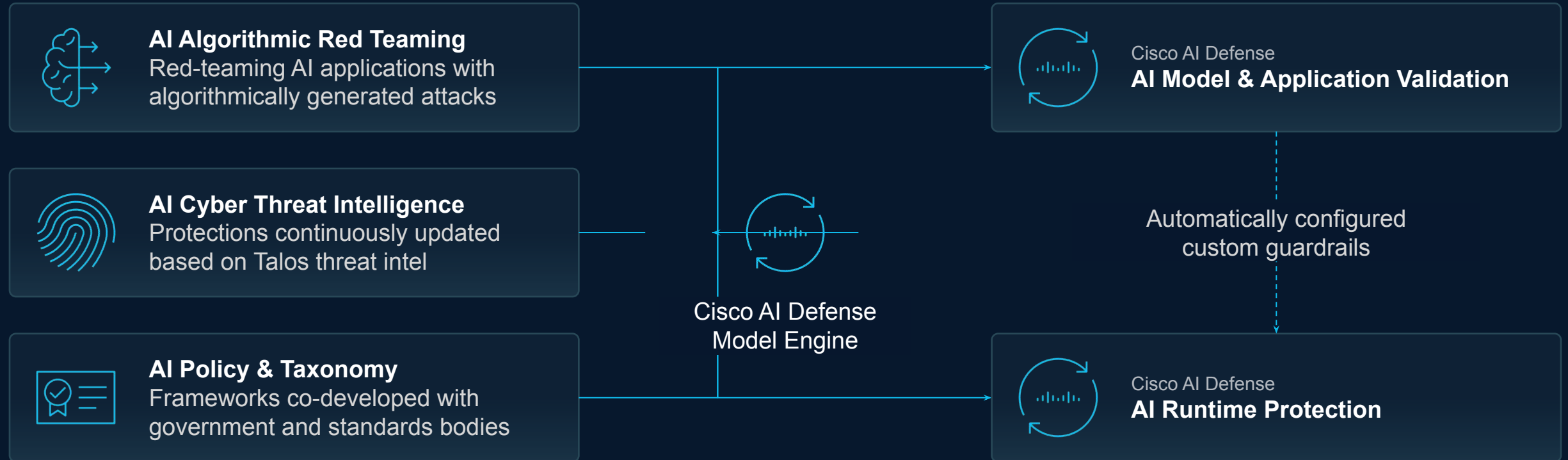
First-Party AI Applications

Enable end-to-end secure development of **first-party AI applications** across your business with Cisco AI Defense.

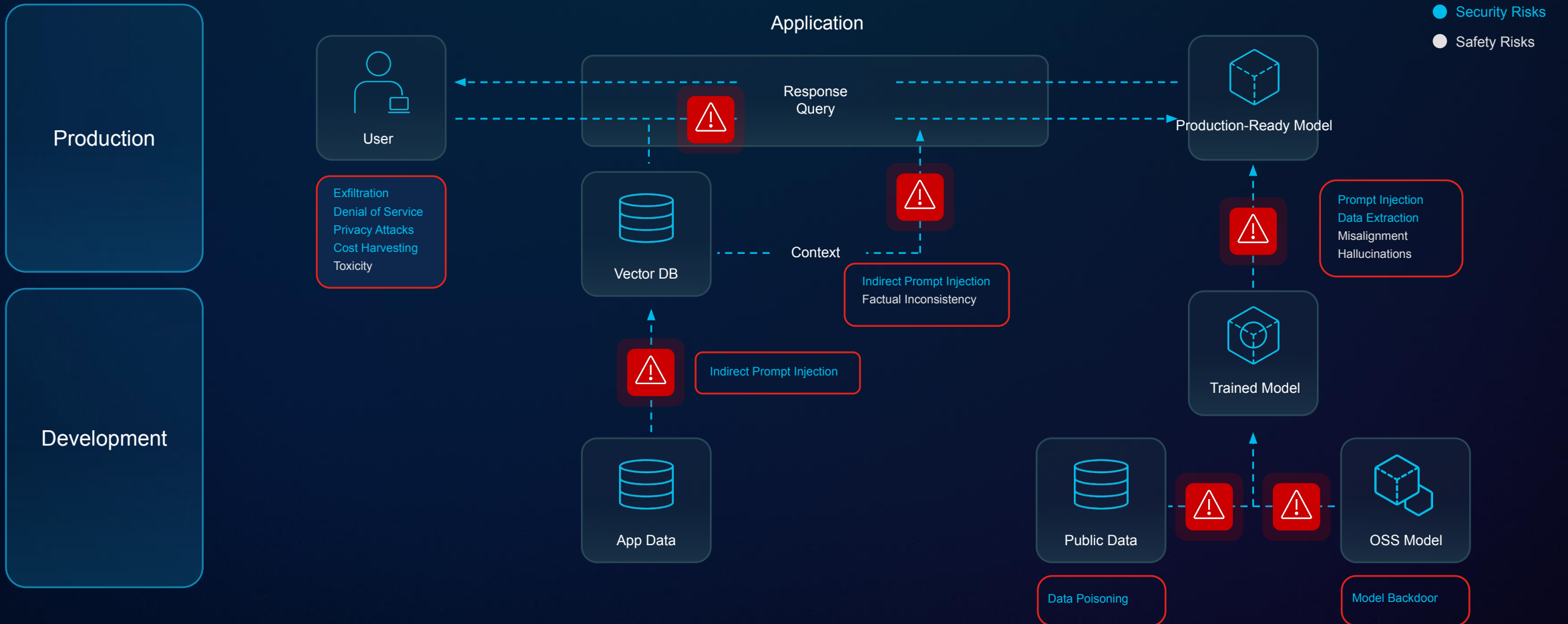


The engine behind Cisco AI Defense

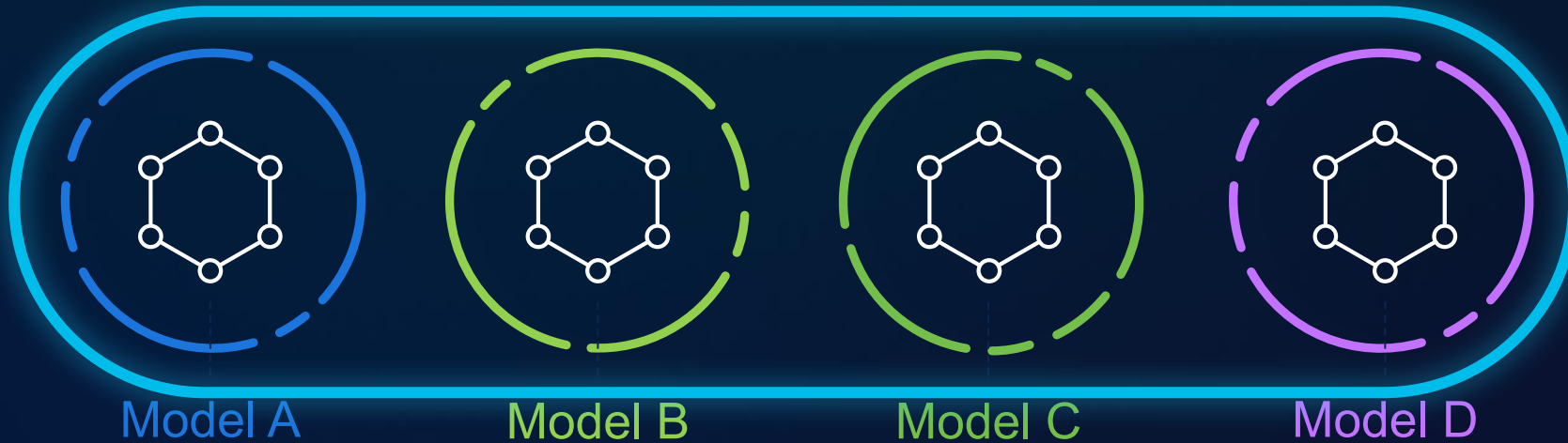
Learn what powers our proprietary model engine, which automatically generates inputs that expose AI vulnerabilities



Risk are present across the GenAI lifecycle



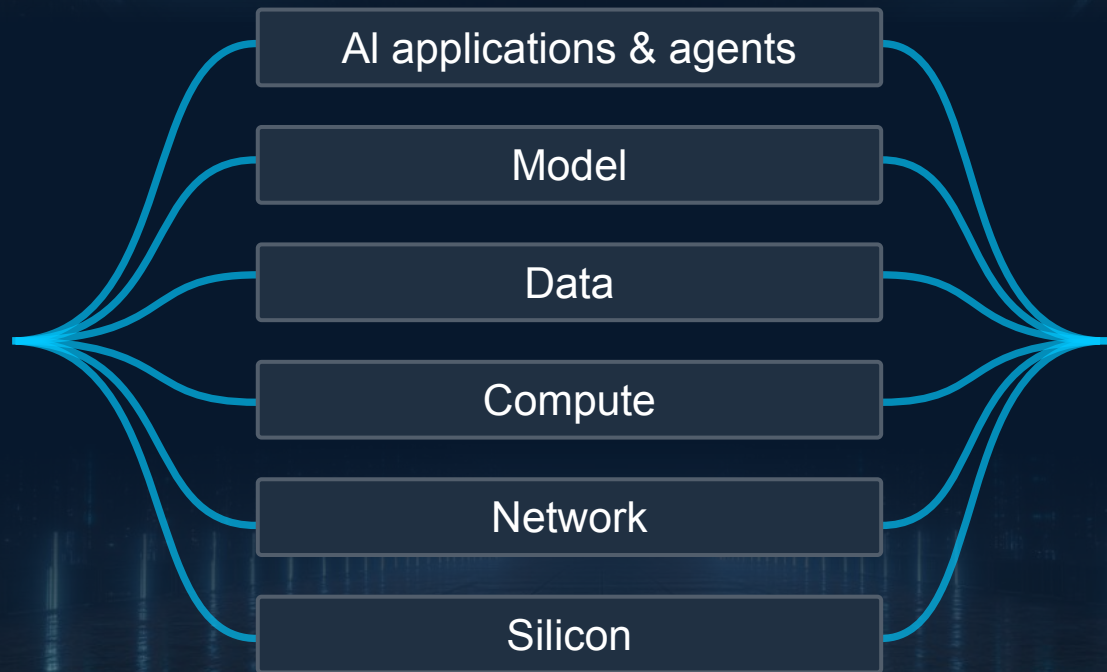
Model security is inconsistent



Enterprise vendors provide a form of optimization for each model, but not across models, allowing AI teams to focus fully on developing that model.



Observability
for AI



Safety & security
for AI



**Infrastructure
constraint**

**Trust
deficit**

**Data
gap**

**Agentic
shift**



ANNOUNCING

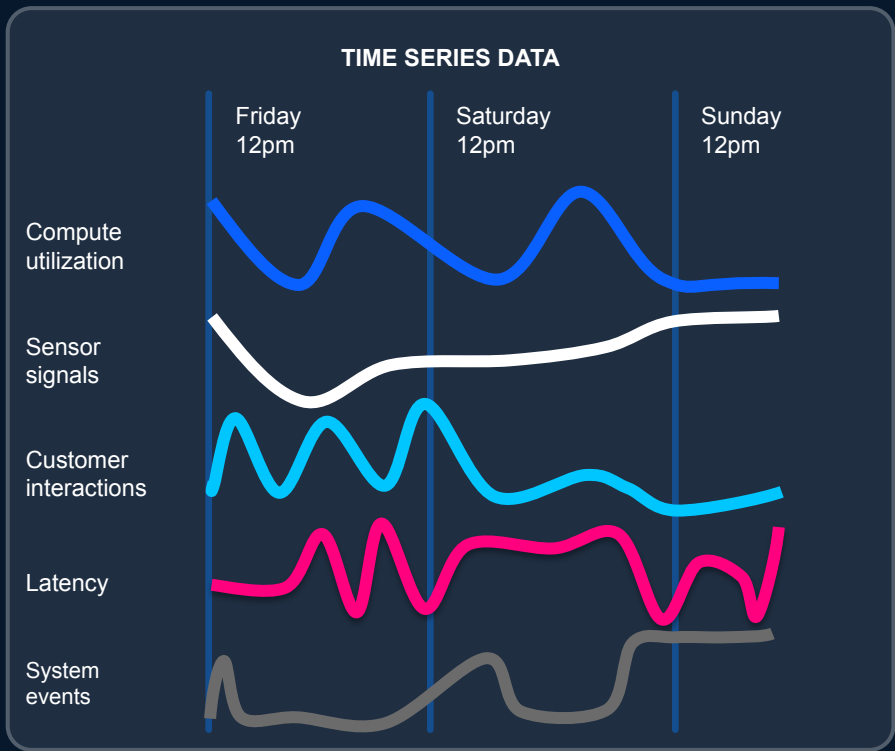
Time Series Foundation Model

OPEN-SOURCE | ON HUGGING FACE NOVEMBER 2025

Optimized for machine data

Accurate and scalable

Adaptable to your domain



UNSTRUCTURED DATA

IT INCIDENT TICKET

User reports intermittent unresponsiveness when running reports


Saturday 08:31 AM


Saturday 12:11 PM

Saturday 1:18 PM

Saturday 1:38 PM

STRUCTURED DATA

 Sales transactions



Degradation in customer experience predicted

There's a **60% chance of a network outage in the next 18 hours** that will impact approximately 8,000 customers, resulting in \$500K missed revenue opportunity.

See suggested remediation...



**Infrastructure
constraint**

**Trust
deficit**

**Data
gap**

**Agentic
shift**

AI is rewriting the rules

Apps can now be written
with little
human involvement

AI agents will perform
basic troubleshooting and
fixes, autonomously

AI apps require
new forms
of telemetry

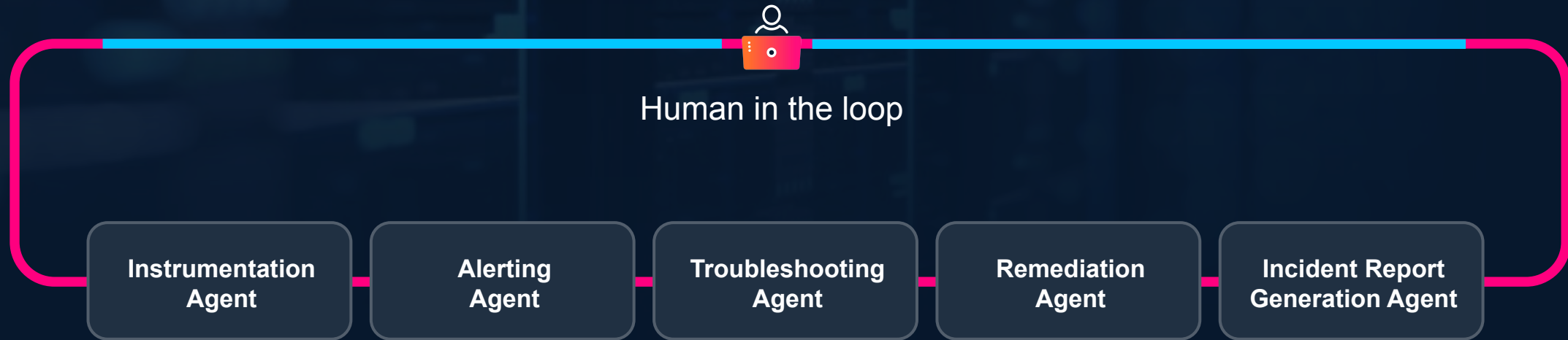
Observability must evolve

Fix and prevent with AI agents

Observe AI agents and infrastructure

Unify observability and show business impact

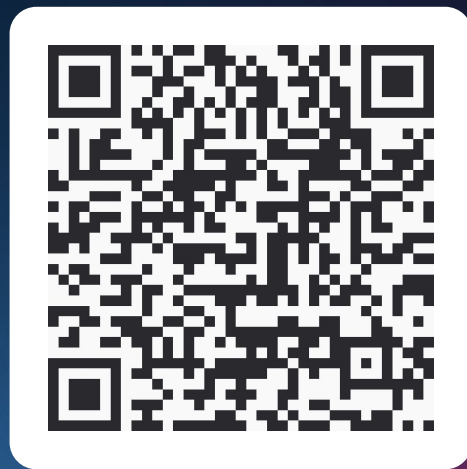
Fix and prevent with AI agents



Learn more about Cisco AI Defense



Request a demo of AI Defense



Read the State of AI Security 2025

THE RISE OF SOVEREIGN AI



Read my article on Sovereign AI