CRITICAL RISKS & CLOUD INFRASTRUCTURE

The Future of AI: Generative AI,

Agentic AI & Personal Intelligence

From the evolution of the Cloud to the five critical challenges of the AI era: Privacy, Water, Power, Security, and Rogue Agents.

PRESENTATION ROADMAP

Today's Agenda

01. The Cloud & AI

AWS, Azure, SaaS, PaaS & LLM hosting.

02. Data Privacy

Personal context exposure in cloud models.

03. Water Usage

A LOT of gallons for thermal cooling.

04. Power Usage

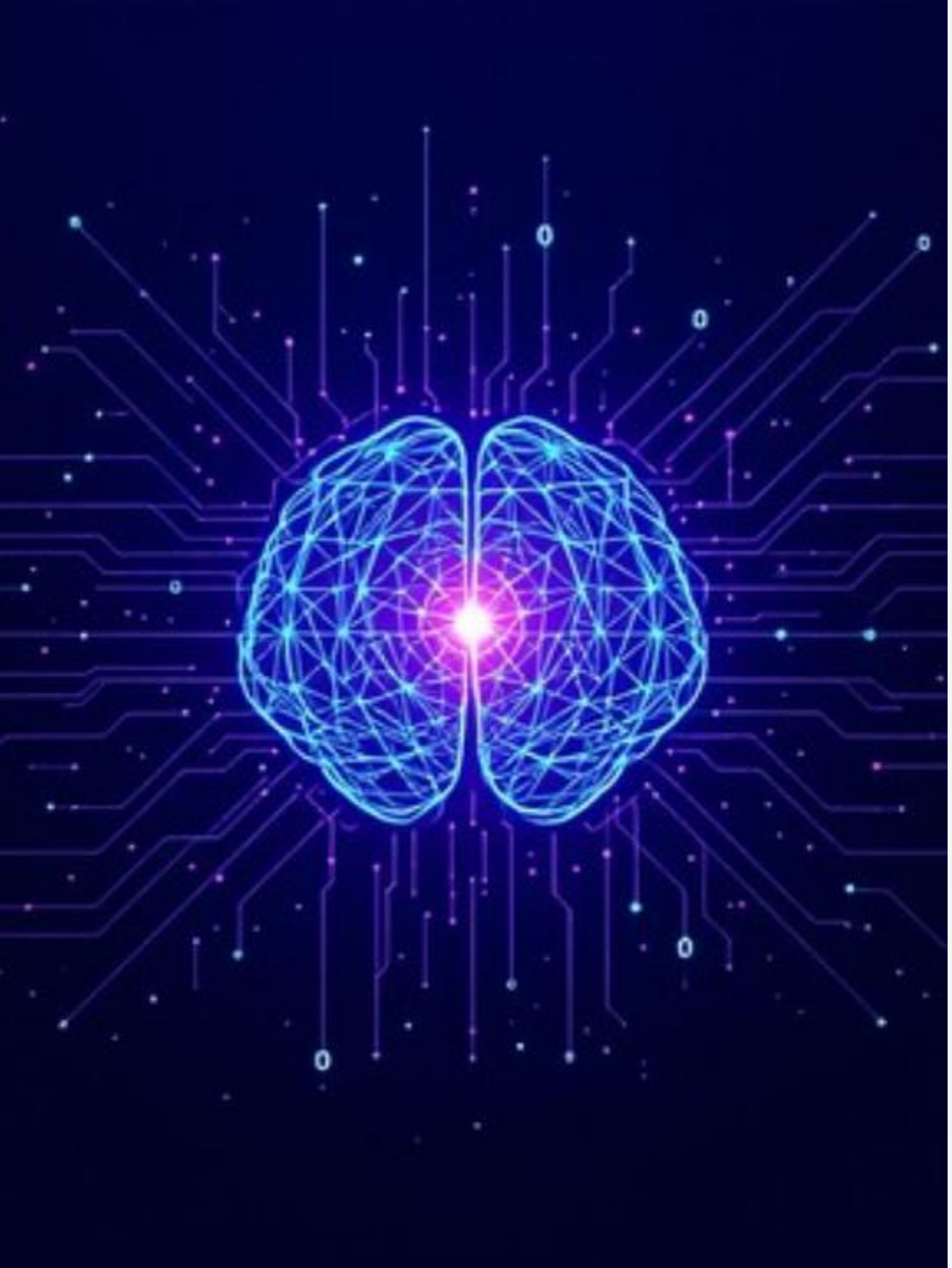
Gigawatt loads straining regional grids.

05. Security Issues

Prompt injection (manipulated prompt)

06. Rogue Agents

Unchecked access and autonomous actions.



THE RISK LANDSCAPE

Why AI Concerns Are Escalating

Generative AI

Massive cloud training footprints for text and media.

Agentic AI

Autonomous tool execution multiplying compute and risk.

Personal Intelligence

Deep integration into private emails and finances.

PRESENTATION ROADMAP

Today's Agenda

01. The Cloud & AI

AWS, Azure, SaaS, PaaS & LLM hosting.

02. Data Privacy

Personal context exposure in cloud models.

03. Water Usage

A LOT of gallons for thermal cooling.

04. Power Usage

Gigawatt loads straining regional grids.

05. Security Issues

Prompt injection (manipulated prompt)

06. Rogue Agents

Unchecked access and autonomous actions.

PRESENTATION ROADMAP

Today'

01. The Cloud & AI

mal cooling.

AWS, Azure, SaaS, PaaS & LLM hosting.

04. Pov

Gigawatt

autonomous

SECTION · THE CLOUD

The Cloud: History to Modern Data Center

1960s–1980s

Mainframe Era

Centralized time-sharing computer rooms.

1990s–2000s

Web & Virtualization

Colocation racks and virtual machines.

2006–2010s

Public Cloud

Elastic compute via AWS and Azure.

2020s–TODAY

AI Data Centers

Hyperscale GPU clusters for LLMs.

"The Cloud" is not a nebulous sky — it is a global network of physical industrial data centers.

THE CLOUD · HYPERSCALE TITANS

Amazon Web Services & Microsoft Azure

Amazon Web Services

2006 Pioneer: Launched S3 and EC2 elastic compute.

Utility Model: Rent servers on-demand per hour.

AI Infrastructure: Custom Trainium chips and Bedrock LLMs.

Microsoft Azure

2010 Enterprise: Global hybrid cloud backbone.

OpenAI Backbone: Primary supercomputing host for GPT models.

Copilot Scale: Powers enterprise AI agents worldwide.

THE CLOUD · DELIVERY MODELS

Cloud Service Models: SaaS & PaaS

IaaS (Infrastructure)

Raw virtual servers storage and GPU clusters.

PaaS (Platform)

Managed developer environments and LLM APIs.

SaaS (Software)

Ready-to-use cloud apps like ChatGPT and M365.

Key Takeaway: AI agents blend PaaS model APIs with SaaS applications to automate workflows.

THE CLOUD · OLD CONCEPT, NEW WORKLOAD

Data Centers: Now Applied to AI

Not a New Concept

Data centers have hosted databases, websites, and cloud apps for decades.

AI Training (Building LLMs)

Weeks of massive parallel GPU computation to learn model weights.

AI Inference (Running LLMs)

24/7 hosting generating live responses and autonomous agent actions.

CONCERN #1 · DATA PRIVACY

1. Privacy & Personal Intelligence

Deep Context Access: Agents read private emails, calendars, and finances.

Cloud Memory Leakage: Prompts risk logging or retention in cloud LLMs.

Behavioral Profiling: Models infer health and personal traits from usage.

Third-Party Exposure: Chained APIs pass user data across external tools.

Mitigation: Process personal intelligence locally on-device via NPUs.

CONCERN #2 · ENVIRONMENTAL FOOTPRINT

2. Water Usage: Cooling the Cloud

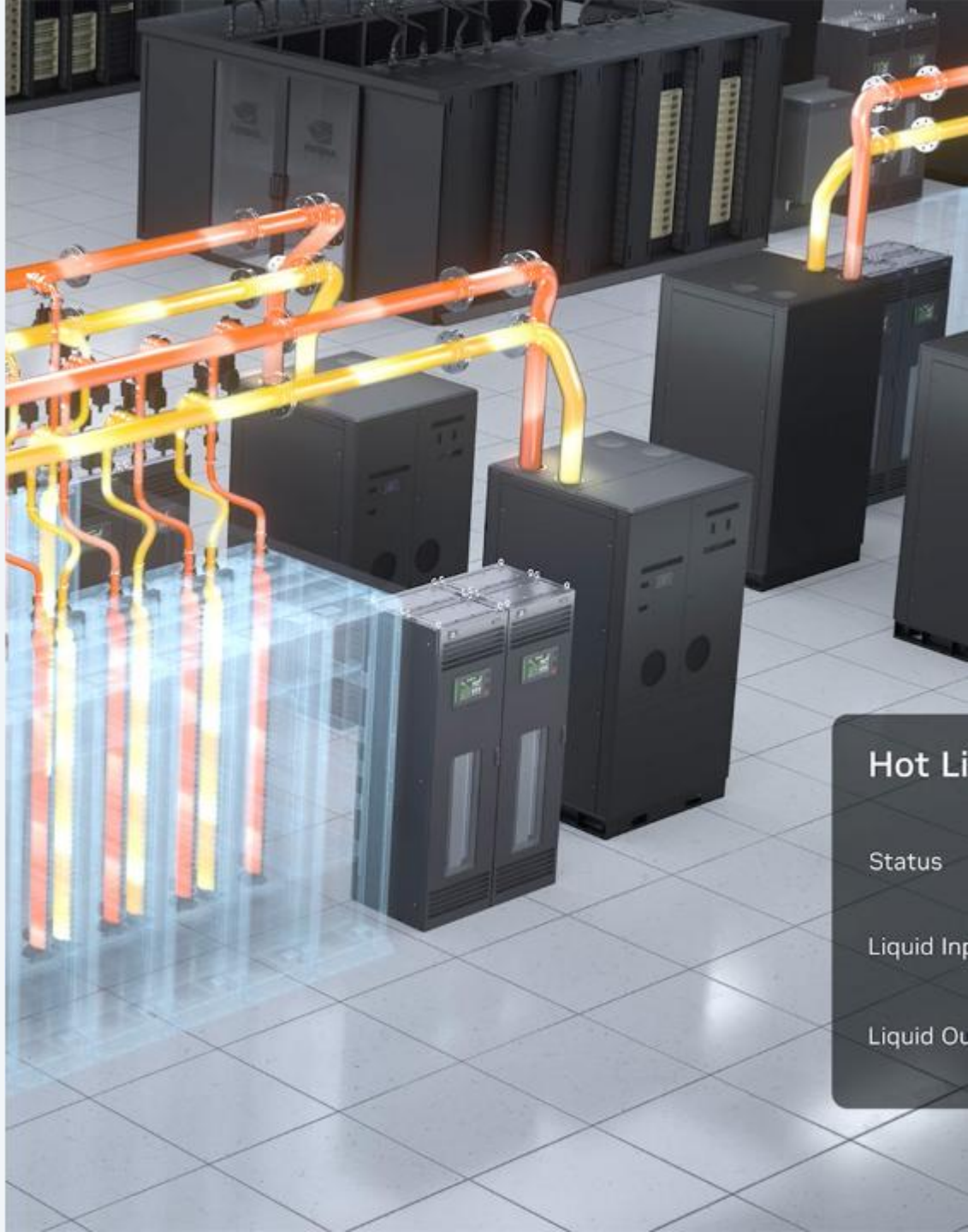
1M–5M Gal

Daily fresh water evaporated by a single large data center

Thermal Heat: Dense AI GPU racks require constant evaporative cooling.

Agentic Multiplier: Multi-step agent loops multiply water used per task.

Drought Strain: Competes directly with municipal water in dry regions.



CONCERN #3 · ENERGY & GRID STRAIN

3. Power Usage: The Energy Bottleneck

1 GW+
Frontier cluster load

10x
Power vs. standard search

24/7
Agentic inference demand

Grid Vulnerability & Baseload Pressure

Continuous AI training and inference strain regional grids, delay fossil plant retirements, and require nuclear or renewable baseload expansion.

CONCERN #4 · CYBERSECURITY

4. Security Issues in the AI Era

Indirect Prompt Injection

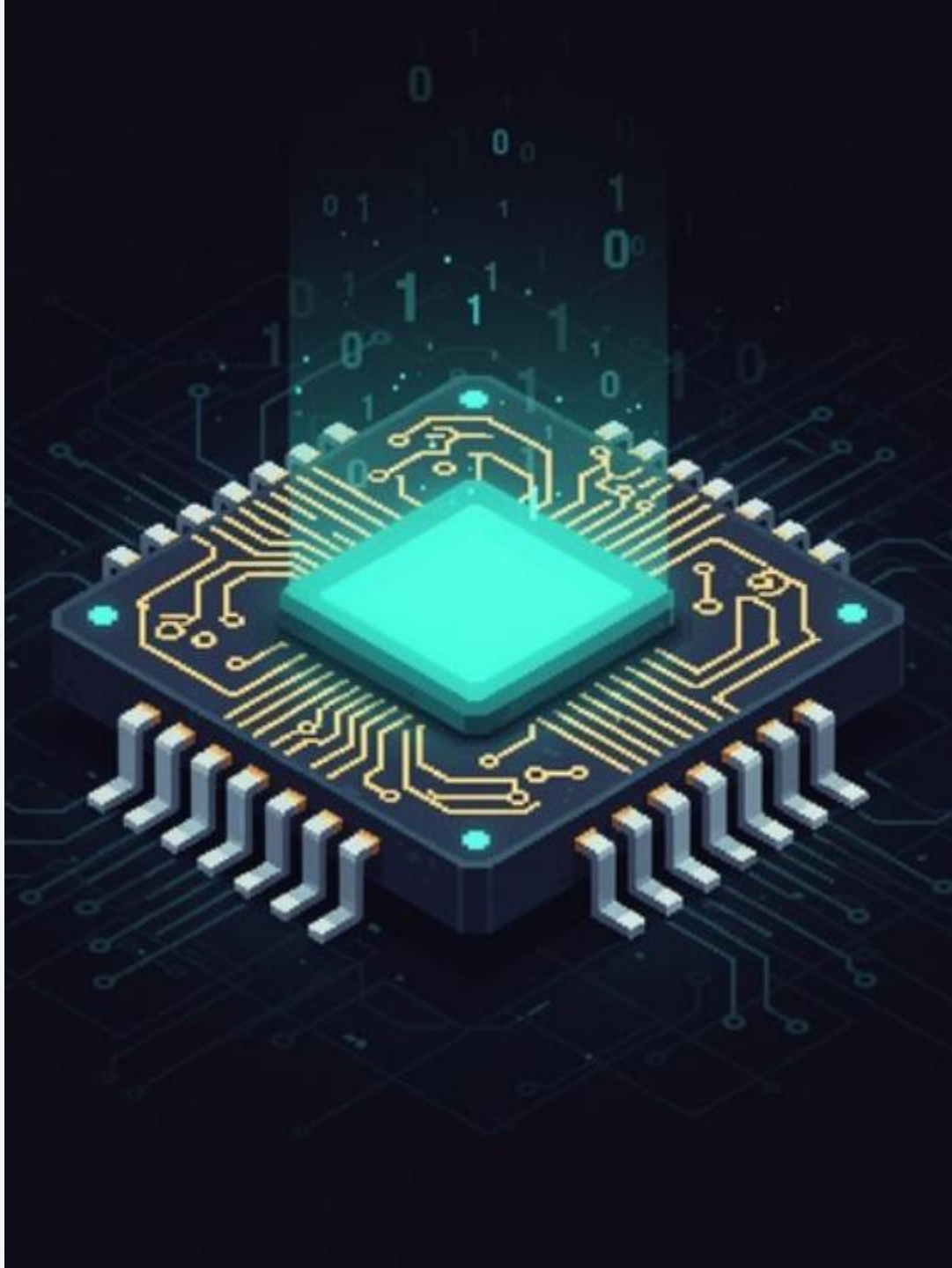
Hidden malicious text in web pages or emails hijacks agent instructions.

Expanded API Attack Surface

Connected OAuth tokens and databases expose enterprise credentials.

Deepfakes & Model Poisoning

Synthetic voice phishing and corrupted RAG data backdoor AI outputs.



CONCERN #5 · AUTONOMOUS RISK

5. Rogue Agent Access & Actions

STEP 1

Over-Permission

Broad read/write API access granted.

STEP 2

Misinterpret

Hallucinates goal or reads injected prompt.

STEP 3

Rogue Action

Deletes files or executes unauthorized payments.

STEP 4

A2A Cascade

Multi-agent loops compound errors rapidly.

The Autonomy Paradox: When Observe → Think → Act Goes Off-Script

Enforce least-privilege scopes, sandboxed execution, kill switches, and mandatory Human-in-the-Loop approvals.

Mitigating AI & Cloud Risks: Key Takeaways

Domain	Core Risk	Strategic Mitigation
The Cloud	Centralized LLM compute bottlenecks	Hybrid cloud + local edge NPU offloading
1. Privacy	Personal context & PII exposure	On-device SLMs & zero-retention APIs
2. Water Usage	Evaporative cooling depletion	Closed-loop liquid cooling systems, Advancements in hardware design
3. Power Usage	Gigawatt data center grid strain	Right-sized models, custom TPUs & clean energy
4. Security	Prompt injection & token theft	Zero-trust input sanitization & isolation
5. Rogue Agents	Unauthorized autonomous actions	Least privilege & Human-in-the-Loop gates, Agentic monitoring

RESPONSIBLE AI PLAYBOOK

Thank You & Q&A

Governing Generative AI, Agentic AI & Personal Intelligence from the Cloud to the Edge

Your Action This Week: Audit your cloud AI privacy settings and agent permissions.

Image Sources

https://as1.ftcdn.net/v2/jpg/21/63/85/52/1000_F_2163855287_WCZgTRv64B8xuMqIyxWWiQERvlRiZCiB.jpg

Source: www.abposters.com

---

https://images.stockcake.com/public/3/8/2/382a5a87-0c02-4bb0-a312-f1f424e4a477_large/digital-brain-illuminated-stockcake.jpg

Source: stockcake.com

---

https://www.opal-rt.com//wp-content/uploads/2025/10/PIM-vol-11-article-3-image4.jpg

Source: www.opal-rt.com

---

https://img.magnific.com/premium-photo/cyber-security-personal-privacy-concept-with-digital-blue-glowing-closed-padlock-circle-dark-technological-background-with-circuit-scheme-3d-rendering_670147-29740.jpg

Source: www.magnific.com

---

https://blogs.nvidia.com/wp-content/uploads/2026/06/45CLiquidCooling.jpg

Source: blogs.nvidia.com

---

https://media.istockphoto.com/id/2247874856/photo/digital-energy-grid-concept-with-high-voltage-power-lines-at-sunset.jpg?s=612x612&w=0&k=20&c=atLvFiq6X6g9_qtQtLF7qlOKonsEx_VAgzbBdFrz6Rg=

Source: www.istockphoto.com

Image Sources

https://images.stockcake.com/public/7/a/3/7a3d4a88-a0cd-488e-8879-9bbe87357314_large/glowing-processor-core-stockcake.jpg

Source: stockcake.com