Balancing the Edge: Cybersecurity and AI in the Era of Risk and Opportunity

Christian Koch (NTT DATA)
Senior Vice President Cybersecurity – IoT/OT-Security, Innovations & Business Development

November 2025

NTT DATA is unique in its ability to deliver success. What sets us apart?

Recognized as a global leader in generative AI services and guiding the industry with landmark insight

Through our Global GenAI Office, AI Center of Excellence, 7 Innovation Centers and nearly 200,000 skilled professionals - including 15.000 data and AI experts - in 50 countries, our clients have benefited from 50% faster application modernization with our GenAI coding solutions, 30% savings when scaling solutions on our GenAI platform solutions and 320% ROI when implementing Copilot adoption programs.

Global, multidisciplinary expertise with localized delivery

Full-stack transformation portfolio and end-to-end capabilities

Demonstrable impact and benefit

R&D heritage and ongoing dedication to innovation

Our differentiation: Why NTT DATA?

NTT DATA offers comprehensive GenAI services for implementing industry-specific use cases.

End-to-end value: Guiding clients through all phases of GenAI transformation from strategy to implementation

Innovation: Advancing GenAI research and building next-generation photonic data centers

Full-stack solutions: Offering data sovereignty, security and various commercial models

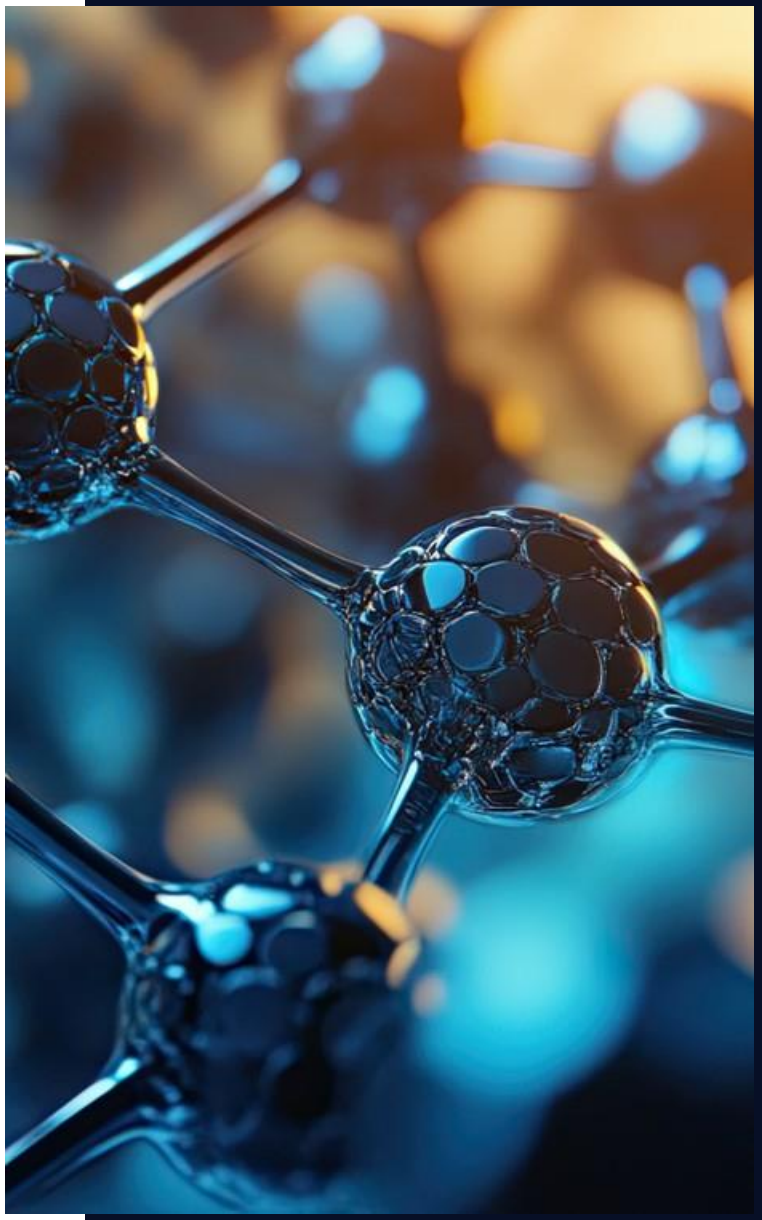
Partner network: Collaborating with hyperscalers and high-performance computing manufacturers

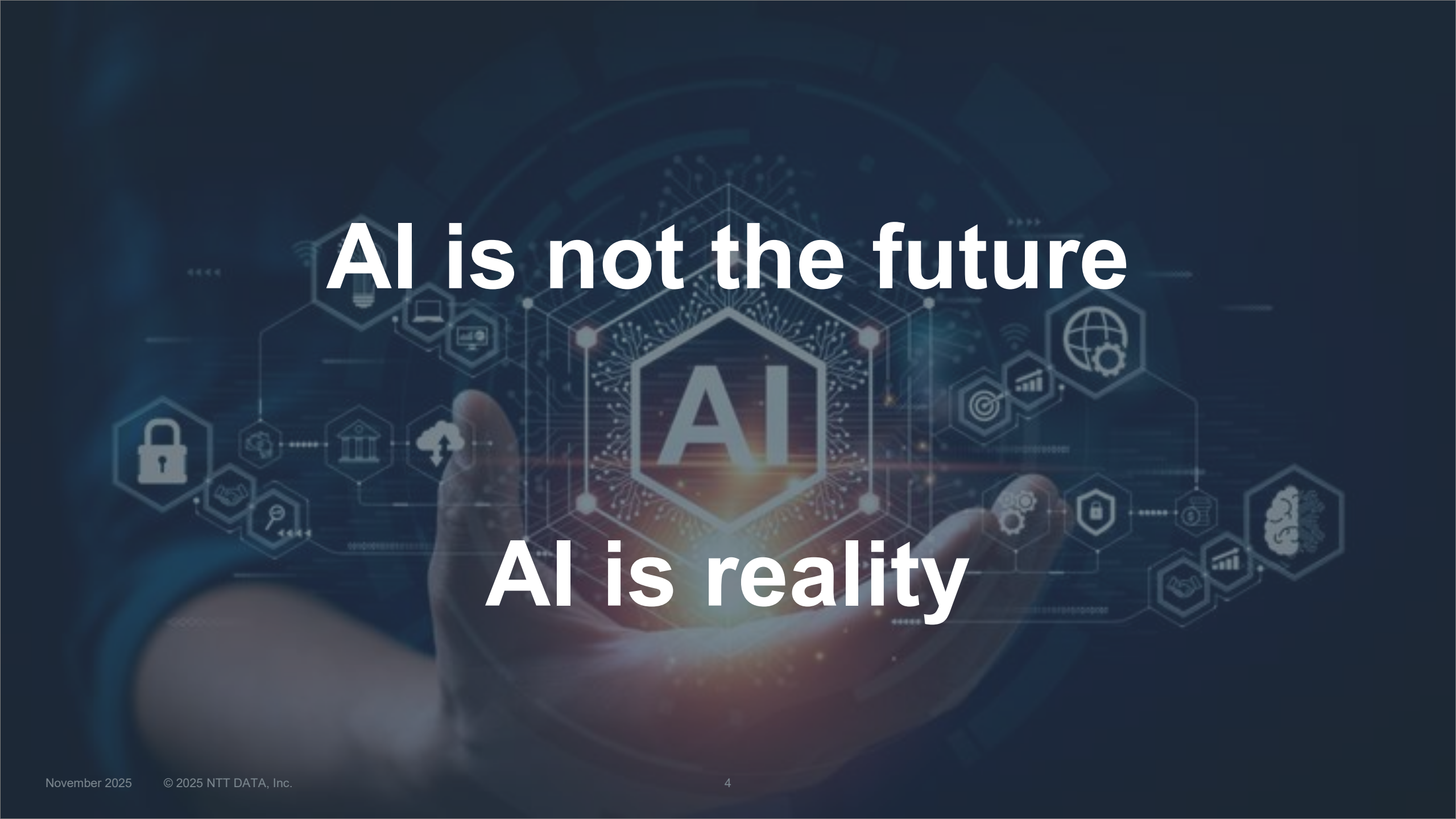
Industry solutions: Addressing core challenges across industry-specific value chains

Talent combination: Cross-functional teams with industry and GenAI expertise

Proven assets: Delivering scalable, efficient and tailored GenAI solutions

Global scale: Providing global coverage and talent sourcing for scalable delivery





Top challenges faced by enterprises in GenAI adoption

Lack of strategy

Lack of strategic vision and roadmap detailing the solutions and resources needed to deliver business value

Time to value

Lack of use case prioritization approach and standard **ROI mode**l results in unclear investment priorities

Complexity in scaling

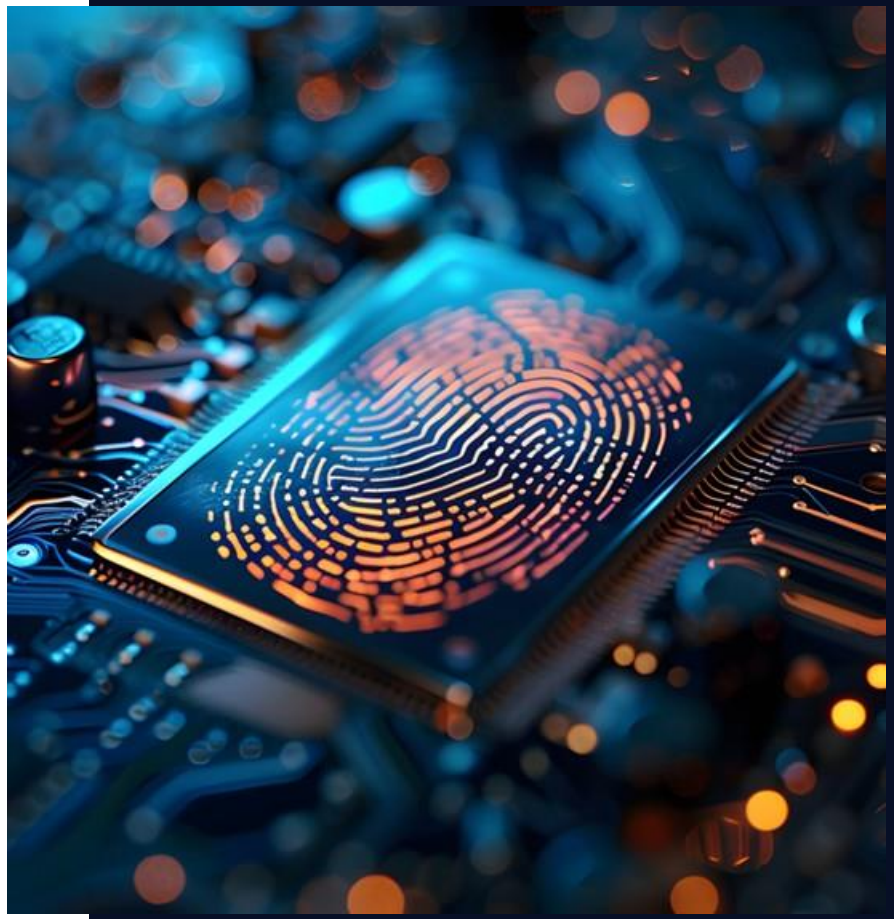
Complexity around model fine-tuning and lack of curated use cases slow down deployment, increasing timelines and cost

Security and responsibility

Data security and privacy, IP infringement concerns, coupled with **quality of output** concerning **erroneous facts and hallucinations**

Too many choices

Thousands of public AI and open-source private AI models make it difficult to choose the right platform and model that is future-proofed for their requirements



Challenges faced by enterprises depend on the phase of the AI journey they are currently in.

Cybersecurity for AI

- Services to secure customer developed systems

Cybersecurity with AI

- Included in cybersecurity products

Is AI creating new challenges?

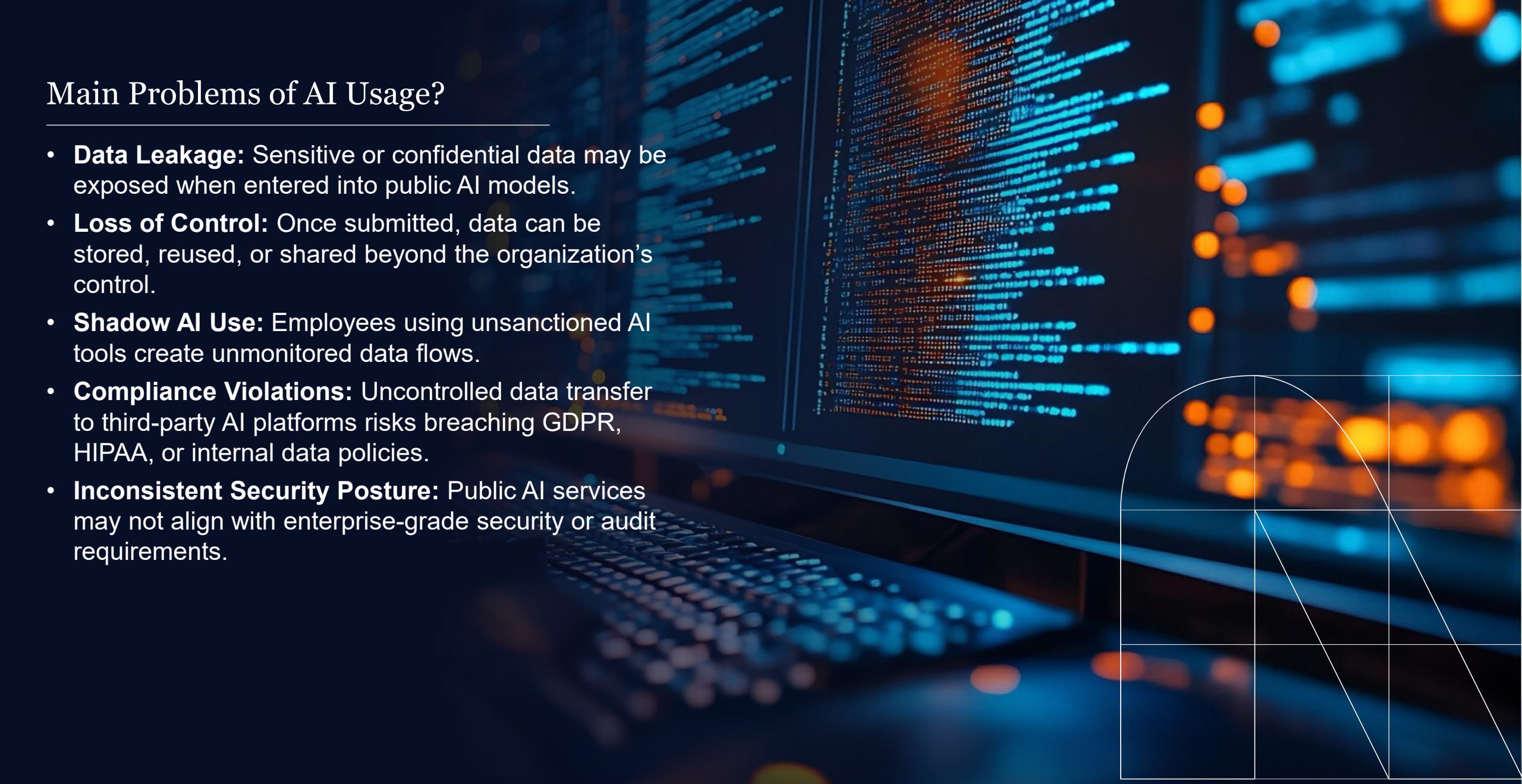
Threats

Governance

Risk Management
for used LLMs

Main Problems of AI Usage?

- **Data Leakage:** Sensitive or confidential data may be exposed when entered into public AI models.
- **Loss of Control:** Once submitted, data can be stored, reused, or shared beyond the organization's control.
- **Shadow AI Use:** Employees using unsanctioned AI tools create unmonitored data flows.
- **Compliance Violations:** Uncontrolled data transfer to third-party AI platforms risks breaching GDPR, HIPAA, or internal data policies.
- **Inconsistent Security Posture:** Public AI services may not align with enterprise-grade security or audit requirements.



How to protect your AI assets

AI model security

- Ensure model integrity and prevent shadow logic
- Ensure validity of pretrained models
- Gain insights into model vulnerabilities

Detection & Response

- Continuous monitoring of input and output of AI algorithms
- Prevent attacks to hijack or manipulate behavior

AI Assets are

- **not secured** and
- models are **not trusted**

by default

https://atlas.mitre.org/matrices/ATLAS

NTT DATA's Security for AI

Accelerate AI adoption and innovation safely and manage risks effectively with our comprehensive Security for AI services

Our full-stack and full lifecycle managed services

AI Risk and Compliance Service	AI Protection Service	AI Assurance Service
Ensure regulatory compliance and mitigate risks in AI systems throughout their lifecycle	Safeguard AI workloads and data with advanced security measures and threat detection	Guarantee the reliability and integrity of AI solutions through rigorous security validation and monitoring
• AI Risk Assessment • AI controls mapping and validation	• AI asset discovery and shadow AI • AI guardrails • AI model, data and app security	• AI threat modeling • AI vulnerability assessment • AI red team/offensive security

Protection covering every layer of AI systems, from models, data and infrastructure to applications and user interactions, ensuring security and compliance throughout development, deployment and ongoing usage.

Value differentiators

- Security for AI center of excellence
- NTT DATA Compliance Acceleration Platform
- AI red teaming

Services

- Readiness engagement
- Implementation services
- Managed support

Innovation demands

Secure by Design

November 2025

NTT DATA

Cybersecurity for AI

- Services to secure customer developed systems

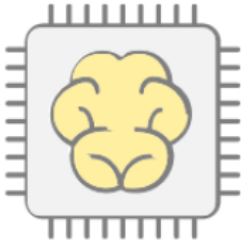
Cybersecurity with AI

- Included in cybersecurity products

Increase efficiency with AI in security operations

November 2025

Assisted SOC



Automation with basic rule-based workflows to automate repetitive tasks.

Hyper-automated SOCs that combine ML, RPA, and orchestration for end-to-end automation.

AI/ML speeds up research on Indicators of Compromise (IoC), Indicators of Attack (IoA), and Tactics, Techniques, and Procedures (TTPs) and provides contextual insights.

Manual SOC

Operated manually, limited automation through hard-coded deterministic scripts.

Human analysts solely responsible for threat life cycle.

Overwhelmed workforce.

AI Powered SOC

Autonomous SOC

AI independently assesses threats, makes decisions, and executes responses.

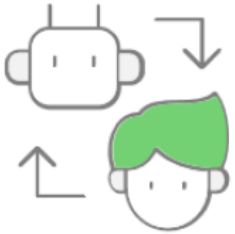
Minimal human intervention.

Human oversight for ethical considerations, focusing on strategic initiatives.

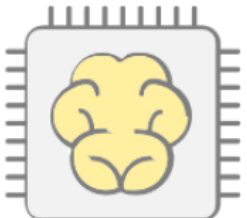
Semi-autonomous SOC

AI drives most of the tasks on behalf of the analysts, handles predefined workflows.

Human oversight retained for critical decisions, balancing automation and expertise.



Assisted SOC



Automation with basic rule-based workflows to automate repetitive tasks.

Hyper-automated SOCs that combine ML, RPA, and orchestration for end-to-end automation.

AI/ML speeds up research on Indicators of Compromise (IoC), Indicators of Attack (IoA), and Tactics, Techniques, and Procedures (TTPs) and

Cybersecurity with AI

Natural language interface

Advanced data analytics in real time

Zero day threat detection

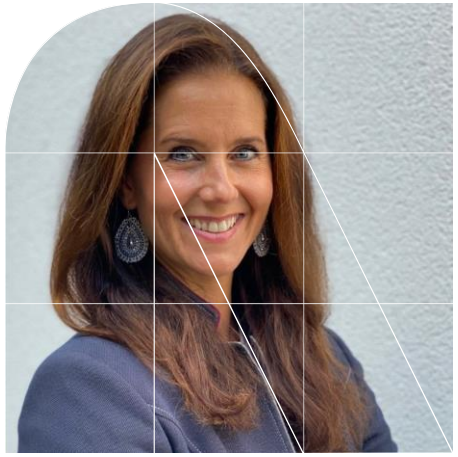
Usecase/Playbook optimization and reduction of false positive alerts

Advanced phishing detection

Shadow data detection (hidden or unexpected data activities)

November 2025

Your Contact in Austria



Eva Heralic

Vice President Cybersecurity AT

Eva.Heralic@nttdata.com
M: +43 660 574 37 27

Christian Koch

SVP Cybersecurity – IoT/OT, Innovations & Business Development

c.koch@nttdata.com
M: +49 151 20945797


NTT DATA