AI and ML Solutions | Cybersecurity Consulting

Use AI and ML technologies safely in your business

Our consultants have broad experience in automation, AI/ML solutions and risk management frameworks. We can assist you with identifying and managing risk in ML and AI solutions, enabling you to use these technologies safely in your business.

New technologies bring new risks

Organizations worldwide are adopting technologies like neural networks, machine learning (ML) and generative AI (GenAI) to enable various business outcomes.

But, as with any technological transformation that's built on existing frameworks and compute, network and cloud solutions, they bring novel cybersecurity risks to be managed.

When developing new systems based on ML models, it is crucial to address unique risks, including:

- Safeguarding privacy and intellectual property when data is used in model training and model prompts
- Ensuring the accuracy of the training data and the reliability of the output produced by the model
- Implementing web/API security, system-hardening measures, network defenses, and robust access and authorization controls to protect ML systems
- Addressing ethical concerns, such as hidden biases, and ensuring fairness in decision-making processes
- Ensuring transparency throughout the entire process, from gathering training data to generating model outputs

Comprehensive services for your AI/ML journey

Our portfolio of services will help you manage challenges and risks in your AI/ML journey, from design to governance.

AI Security Governance

- Build processes and frameworks that will ensure appropriate security controls are in place for systems that use ML models.
- Define the parties responsible for risk assessment and mitigation.

AI Assets Discovery

- Gain visibility of all ML and GenAI services being used in your organization.

AI Threat Modelling

- Map adversarial attack techniques and tactics that intentionally deceive, compromise or manipulate AI models to make incorrect, unintended predictions or decisions.
- Assess cross-tenant data leakage in a multitenant environment, where applicable.

AI Risk Assessment

- Identify and mitigate risks to systems and services that use or will use ML models.
- Evaluate risks of ML models in development or in production, taking into account tools, processes and people risks.

ML System Security Solution Design

- Assess security risks and embed security controls in the design of a system that uses ML or GenAI components.
- This service covers controls relevant to both ML models and the underlying compute, network and cloud infrastructure.

ML Systems Offensive Assessment

- We look for and attempt to exploit vulnerabilities in a system that uses ML models.
- This service can cover attacks on the ML model itself and on the underlying system infrastructure.

> By 2026, 75% of businesses will use generative AI to create synthetic customer data, up from less than 5% in 2023.
>
> **Gartner, Inc.** (Apr 2024)[1]

Understand and manage the risks

With our services, you benefit from:

- **Visibility** of the security risks that AI/ML present to your business
- **Transparency** in data-handling
- **Ongoing assurance** that systems using AI/ML are secure

Our highly skilled team has extensive experience in application and network security. We stay up to date with the threat environment for ML models and GenAI systems.

Use AI and ML effectively

Working with us, you can control your organization's exposure to the risks inherent in these models and systems and manage these risks effectively.

- Implement appropriate governance and controls.
- Reduce the risk of data breaches and attacks.
- Provide assurance that systems which use ML models can withstand both well-known and emerging threats.
- Maintain high ethical standards.

Key service features

- Highly skilled, experienced and trained testers
- Based on recognized frameworks such as NIST AI RMF, ISO 42001, OWASP Top 10 for LLM, Google SAIF, and MITRE ATLAS
- Ability to deliver globally
- Expertise in ML and GenAI, data, network and systems security
- Globally consistent methodology and reporting
- Industry-recognized cybersecurity offensive certifications (OSCP, CREST) and data privacy certifications (CIPP)
- Automated and manual testing techniques for breadth and depth of findings

Why NTT DATA

Global experience

More than 15,000 security engagements with clients spanning 49 countries across multiple industries.

Track record

Decades of experience in providing professional, support, managed and fully outsourced security services to over 6,000 clients.

Expert skills

Highly certified security consultants with expertise across various infrastructures, systems and application technologies including Gen AI. We even have our own developed and supported lightweight large-language model, tsuzumi[2].

Proven approach

Client-centric, pragmatic approach using proven assessments, methodologies, frameworks and best practices to deliver consistent, high-quality engagements.

[1] Gartner, April 12, 2024. 3 Bold and Actionable Predictions for the Future of GenAI. https://www.gartner.com/en/articles/3-bold-and-actionable-predictions-for-the-future-of-genai

[2] https://group.ntt/en/magazine/blog/tsuzumi/

If you'd like to find out more about our Cybersecurity Services, speak to your NTT DATA Client Manager or Security Sales Specialist, or email us directly at **ap.ntt.apac-cybersecurity@global.ntt**

NTT DATA

