# Accelerate AI adoption securely and responsibly

## Security for AI

 

# Compliance, assurance and security throughout your AI lifecycle

**By managing emerging risks and threats to AI models, data, infrastructure and applications, we help you comply with global standards and provide assurance across the entire AI lifecycle, from design to deployment and ongoing monitoring.**

As AI adoption accelerates, organizations are exposed to risks such as data poisoning, adversarial attacks, model inversion and bias amplification. Globally, regulations and frameworks are coming into play to address this — the EU AI Act, ISO/IEC 42001 and NIST AI Risk Management Framework (RMF) are some examples.

> “Without proper controls, shadow AI and ungoverned GenAI usage can lead to legal, financial and reputational damage.”

**Read more:** The AI security balancing act: From risk to innovation shares our in-depth insights on the AI risks that organizations face today and how they can manage those without holding back on innovation.

## Detect and mitigate risk while supporting responsible AI practices

Security for AI is a complete suite of services that facilitate safe and responsible AI adoption. They span the full AI lifecycle and stack, from employee GenAI usage to model protection, application security, infrastructure safeguards and compliance.

### AI Risk and Compliance Service

Risk assessments aligned with ISO 42001, NIST AI RMF and regulatory frameworks

- **01.** Maturity roadmaps
- **02.** AI Risk and Regulatory Assessment
- **03.** Shadow AI discovery
- **04.** Responsible AI policy enforcement.

### AI Protection Service

The identification and defense of AI assets across models, data, applications and APIs

- **01.** Guardrails
- **02.** Sensitive-data detection
- **03.** Vulnerability scans
- **04.** AI firewall
- **05.** GenAI-specific controls like prompt injection protection

### AI Assurance Service

Continuous testing and red teaming to identify and remediate threats across model runtime, APIs, applications and pipelines

- **01.** Adversarial scenario simulation
- **02.** Structured large language model (LLM) testing

**Together,** these services offer layered protection, governance and real-time security controls to help secure your AI-led innovation journey.

**Secure AI Lab**

This center of excellence (CoE) service is a turnkey GenAI security lab available as a hosted or client-deployed environment. With built-in partner integrations and automation capabilities, it's the ideal setting in which to experiment, test your proofs of concept (PoCs) and further develop your AI strategy.

## Evaluate use cases quickly and effectively

We help you accelerate the evaluation of GenAI use cases through potential multivendor solutions and PoCs, and maintain nonproduction setup for secure AI innovations.

  

# Choose your engagement model

**Our engagement models are tailored to your current state and future ambitions. Choose one, more or all, depending on your AI ambitions.**

**Readiness Engagement**

Risk assessment and validation

**Adoption Engagement**

AI usage and workload protection and governance

**Support Engagement**

Managed security for AI services

**On-demand Engagement**

Risk assessment, threat modeling, vulnerability assessment, red teaming and penetration testing for AI, offered as on-demand services

> “Our global Security for AI center of excellence includes threat modelers, red teamers and compliance specialists.”

## Our approach is simple, systematized, dynamic — and built around your needs

**We lead through consulting-led discovery and risk assessments, followed by structured implementation and managed services.**

Our global Security for AI center of excellence includes threat modelers, red teamers and compliance specialists.

Your organization can also benefit from our Cybersecurity Assurance Platform for risk tracking and a dedicated Secure AI Lab environment to test strategies before deployment.

Our services are backed by strategic partnerships with leading AI security vendors, supporting the integration of best-in-class technologies across your AI security stack.

## Achieve your AI goals using our deep expertise and holistic approach to AI security

**From uncovering shadow AI to implementing red teaming AI systems, we provide complete AI lifecycle protection for your organization.**

Our dedicated center of excellence gives you access to best-in-class experts in AI risk, compliance and adversarial threat management, while our proprietary Cybersecurity Assurance Platform helps you align with leading standards such as ISO 42001, NIST AI RMF and the EU AI Act.

To find out more, contact your NTT DATA account representative to schedule an AI Readiness Engagement or Secure AI Lab walkthrough.

**Together, we can help you achieve your innovation goals and scale AI safely and confidently.**

**Learn more about our Cybersecurity solutions and services, visit:**
http://www.nttdata.com/global/en/services/cybersecurity

**Visit nttdata.com to learn more.**

NTT DATA is a global innovator of digital business and technology services, helping clients innovate, optimize and transform for success. As a Global Top Employer, we have experts in more than 50 countries and a robust partner ecosystem. NTT DATA is part of NTT Group.

  