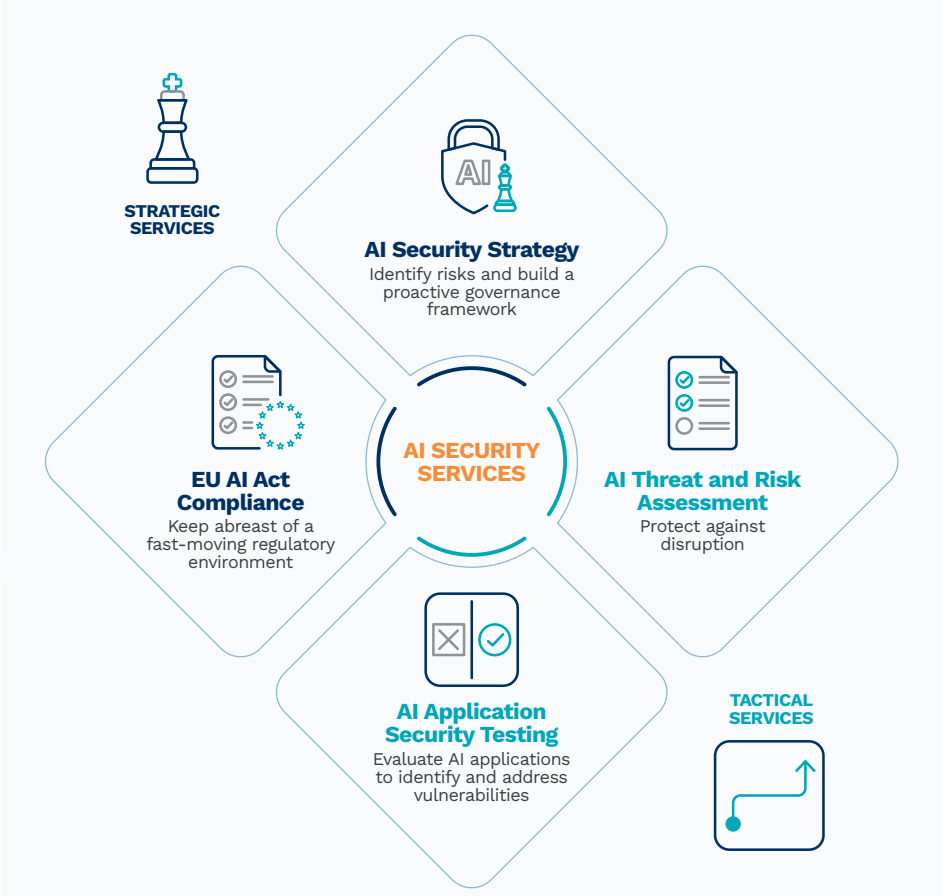
KUDELSKI SECURITY

AI Security Services

Kudelski Security offers comprehensive protection for your AI applications and ecosystems. In an ever-evolving threat landscape, we can help you stay one step ahead with a proactive approach that ensures your operations remain resilient and secure. Our security services blend strategic and tactical solutions to help businesses prepare for and mitigate the growing threats associated with AI-powered systems and applications, and in compliance with emerging regulations.

AI technologies are transforming businesses around the world, but the work to secure these innovative new solutions is often one step behind. It presents unique security challenges due to the technology's complexity and interconnectedness, which can lead to everything from reputational damage, to financial losses, legal liabilities, and operational disruptions.

SECURITY FOR YOUR AI-POWERED ECOSYSTEM



Proactively protect your critical AI solutions in a fast-evolving threat landscape.

- **82%** of executives surveyed believe secure and trustworthy AI is essential for success
- **76%** of executives surveyed have no security component for their generative AI projects
- By 2026, enterprises that invest in AI Trust, Risk and Security Management controls will achieve **35%** more revenue growth than those that don't

Source: IBM Institute for Business Value and Gartner, 2024

AI SECURITY – PROTECT YOUR NEXT FRONTIER

Kudelski Security's AI Security Services proactively protect your AI systems against evolving threats, ensuring your operations remain resilient and secure. With tailored strategies we can help you address specific threat models, and ensure comprehensive protection for your AI systems.

1. **Protect Against Attacks**
   Mitigate the risks of AI adoption with protection against attacks like data poisoning and manipulation.
2. **Ensure Trustworthy AI**
   Implement robust security measures to make sure your AI deployment works reliably.
3. **Comply with New AI Regulations**
   Get ahead of a fast-evolving regulatory landscape to not just comply with regulations, but use them to gain a competitive advantage.
4. **Build Stakeholder Trust**
   Get stakeholders onside by fostering trust thanks to a more secure AI environment.
5. **Strengthen Competitive Edge**
   Gain a key advantage over your competitors through robust AI security measures.

WHAT SETS US APART

Over five years pioneering novel approaches in the AI security space

Broad range of services which integrate strategy, risk management, compliance, and tailored security assessments

We co-build strategies and procedures that focus on your unique threat model, ensuring proactive comprehensive protection for your AI-powered systems

With extensive regulatory experience, we have a deep understanding of compliance requirements including the EU AI Act.

OUR AI EXPERTISE IS RECOGNIZED, OUR CYBERSECURITY SKILLS CERTIFIED:

FORRESTER®

Twice recognized in the cybersecurity consulting services landscape in Europe, 2021-2023.

CISSP

Our advisors hold the CISSP certification, showcasing expertise in cybersecurity management, compliance, and leadership.

NIST

Member of the AI Safety Consortium at NIST, contributing expert insights and shaping AI safety standards.

OWASP®

Contributor to the OWASP Top 10 for Large Language Model Applications, helping identify and mitigate critical web application security risks.

OffSec OSCP | OffSec OSCE³ | OffSec OSWE

Offensive Security certifications demonstrate a range of expertise, from penetration testing (OSCP) to exploit development (OSCE) and web application vulnerability discovery (OSWE).

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, with operations in countries around the world.

info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY

Find out more about Kudelski Security's lineup of AI security services