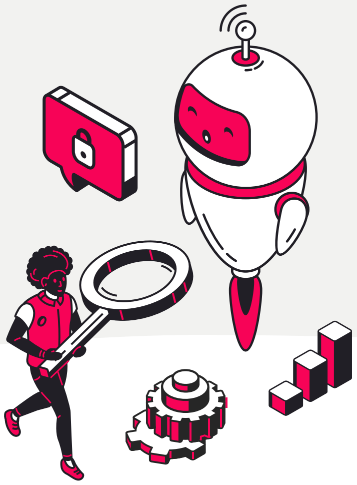
In partnership with

Connect AI Risk Assessment Service.



Enabling secure and confident AI adoption for your organisation.

Artificial Intelligence (AI) and Machine Learning (ML) are transforming industries today, delivering unparalleled opportunities for innovation and efficiency. However, these transformative technologies also introduce new and complex risks.

Connect's AI Risk Assessment Service empowers organisations to address these challenges head-on, ensuring secure, compliant, and resilient AI systems.

Our tailored approach identifies vulnerabilities, mitigates risks, and builds confidence in AI adoption, helping organisations scale their AI capabilities safely while reducing operational, financial, and reputational risks.

The value we deliver.

Through Connect's AI Risk Assessment Service, we deliver meaningful and measurable value by enabling organisations to confidently adopt AI technologies while maintaining robust defences against emerging threats. Here's how we help:

Proactive threat management
Stay ahead of emerging AI-related security threats with Connect's proactive approach. By identifying vulnerabilities in AI systems before they can be exploited, we can help reduce the risk of costly breaches, data loss, or operational disruptions, protecting your organisation from potential crises.

Tailored security enhancements

Every organisation's use of AI is unique, and so are the risks. We deliver **customised insights and strategies** to address vulnerabilities specific to your AI models and use cases. The tailored recommendations we make ensure practical and effective security measures aligned with your operational environment.

Regulatory confidence

Navigating complex regulations such as GDPR and the AI Act is critical. Connect ensures your AI systems meet these evolving standards, helping you avoid penalties, reduce legal risks, and maintain the trust of your customers and stakeholders.

Enhanced resilience and reliability

Connect reinforces your AI systems, ensuring **resilience against adversarial attacks and operational errors** while maintaining continuity of critical business operations.

Increased stakeholder trust

Enhance your reputation as a **responsible adopter of AI.** By demonstrating a commitment to AI safety and compliance, Connect helps you build trust with customers, investors, and partners, solidifying your position as a forward-thinking organisation.

Cost-effective risk management

Proactively addressing AI risks is significantly more cost-effective than dealing with breaches or failures. We help to identify vulnerabilities early and propose robust security measures, avoiding unnecessary financial and operational costs.

Competitive advantage

Adopting AI securely and in compliance with regulations can set you apart in the marketplace. Connect helps you showcase ethical and responsible AI practices, providing your organisation with a distinct competitive advantage.

Future-ready strategy

AI technologies and threats are evolving rapidly. Connect provides not only immediate solutions but also **long-term strategies** that scale with your ambitions, ensuring your systems remain secure as your capabilities grow.

Key deliverables.

As part of our service, Connect provides a comprehensive AI Risk Assessment Report, which includes:

- **Identified vulnerabilities** such as data poisoning, adversarial attacks, and model inversion risks.
- **Risk prioritisation matrix** to help you focus on the most critical vulnerabilities.
- **Recommendations for mitigation strategies** tailored to your systems and use cases.
- **Strategic roadmap** outlining the steps to address AI-related risks effectively.
- **Executive summary** designed to communicate key findings and actions to stakeholders.

Our approach: A comprehensive four-step framework.

1. **Discover**
   We conduct a detailed review of your AI systems, workflows, and deployment practices to map out vulnerabilities.

2. **Diagnose**
   Our experts identify risks unique to your AI use cases, such as adversarial attacks or model theft.

3. **Benchmark**
   We evaluate compliance with relevant legal and industry frameworks, such as GDPR and the AI Act.

4. **Deliver**
   A prioritised action plan with tailored recommendations is provided to strengthen your AI security posture.

Why choose Connect?

We understand that every organisation's AI journey is unique. That's why we're committed to providing a personalised and professional approach to AI security.

With expert guidance, our team of highly skilled security advisors bring specialised expertise in AI and ML risk management, working closely with you to navigate the complexities of AI security.

With Connect's tailored recommendations, we address your organisation's specific needs and challenges, ensuring relevance and practicality.

Our strategies are prioritised and results-driven, designed to deliver measurable improvements in both security and compliance.

Secure the future of AI in your business with confidence.

As AI reshapes industries, don’t let security and compliance challenges hold your organisation back. Partner with Connect to safeguard your AI investments and ensure they deliver measurable, secure outcomes for your business.

BLOCKPHISH - Trusted experts in security solutions

BLOCKPHISH, an NCSC Assured Service Provider, brings together a team of seasoned security professionals with expertise spanning commercial CISOs, ex-Special Forces, intelligence services, and senior advisors to central Government. They are passionate about keeping organisations secure, and provide insightful, proven solutions to tackle complex security challenges. BLOCKPHISH provide a tailored service based on their deep understanding and years of experience in building robust security postures that mitigate the most prevalent cyber and physical security threats. They have proudly supported organisations across diverse global industries, including Government, Defence, Healthcare, Legal, Energy, Critical National Infrastructure, Not-for-Profit, Financial Services, and Telecommunications sectors.

nqa. ISO 9001 QUALITY MANAGEMENT UKAS MANAGEMENT SYSTEMS 0015

nqa. ISO 27001 INFORMATION SECURITY MANAGEMENT UKAS MANAGEMENT SYSTEMS 0015

HM Government G-Cloud Supplier

CYBER ESSENTIALS PLUS

CYBER ESSENTIALS

ARMED FORCES COVENANT

Cyber First

CISM Certified Information Security Manager. An ISACA Certification

Crown Commercial Service Supplier

Chartered Institute of Information Security MEMBER 2025

National Cyber Security Centre

Connect with us.

Confidently adopt AI with robust defences.

☎ +44 2070 751450 (UK) +27 10 476 0300 (SA)

info@weconnect.tech

weconnect.tech