Modern AI

AI Security, Risk & Resilience

Secure AI systems, data, and agents with enterprise-grade controls, governance, and resilience.

Secure AI by Design

Embed security controls across models, apps, data, and workflows.

Proactive Risk Reduction

Identify threats early and reduce exposure across the AI lifecycle.

Enterprise Readiness

Prepare AI initiatives for scale, oversight, and stakeholder trust.

What We Deliver

AI threat modeling

Assess models, agents, pipelines, and trust boundaries.

GenAI / LLM security

Address prompt injection, jailbreaks, misuse, and leakage.

Secure AI architecture

Design secure cloud, hybrid, on-prem, and API-connected environments.

AI red teaming

Simulate adversarial attacks and validate control effectiveness.

Data and model protection

Protect sensitive data, RAG systems, embeddings, and model access.

Incident readiness

Create monitoring, escalation, and response playbooks for AI misuse events.

Ideal Client Outcomes

- Reduce AI risk before production
- Build stakeholder and regulator confidence
- Protect models, data, and users
- Launch AI with stronger resilience

Why Modern AI

We help organizations operationalize AI securely by combining cybersecurity expertise, governance thinking, and practical delivery experience.

Strengthen AI Security from Day One

Modern AI helps clients secure their AI roadmap, architecture, and operating model before risk becomes exposure.