

AI Security Services

Operationalize AI securely with trusted architecture and controls

Why it matters?

AI adoption is accelerating, but so are the risks. AI Security Services help organizations embed security, governance, and compliance into every phase of the AI lifecycle – so they can innovate responsibly and build trust from the start

Core capabilities include:

- Security for AI solutions, aligned with enterprise architecture and compliance standards
- Integrated controls for identity, data, and model governance
- Operational assurance across MLOps, DevOps, and SecOps pipelines

Outcomes



Secure AI Architecture

A defensible, compliant foundation for AI systems



Identity & Data Controls

Enterprise-grade controls to safeguard sensitive data and enforce access boundaries



Operational Resilience

Secure MLOps, DevOps, and SecOps practices to support scalable AI deployment



Governed AI Lifecycle

AI development aligned with governance, risk, and compliance frameworks to build trust

What your organization gains from secure, governed AI

Capabilities and Offer Overview

AI Security Services provides a modular, end-to-end framework for securing AI systems. It spans advisory services, architecture design, identity and data protection, threat modeling, and secure deployment practices. Choose from foundational packages or tailor engagements based on use cases, regulatory needs, and operational maturity.



AI Security Foundation

Advisory and governance services to ensure a tailored AI security strategy integrated with enterprise architecture and digital transformation initiatives. Advise and educate executive, legal, and technical stakeholders to ensure shared accountability.



Threat Modelling

Proactively identify, assess, and mitigate potential security threats (both legacy and emerging) targeting AI solutions.



Security Controls Enablement

Assess hosting environment against Cloud Security Framework and regulatory compliance requirements and build security controls backlog. Design and implement, as a code, Azure policies and controls.



Data Security

Prevent data acquisition risks by implementing encryption, data segregation and AI-aware DLP controls—minimizing exposure to data leakage, misuse, and model exploitation.



Logging, Monitoring and Threat Detection

Design and implement enterprise-level logging, monitoring and threat detection for all interactions with AI models to mitigate harmful use of the models and help ensure that security and compliance standards are met.



Tools & Methodologies



To mitigate identified threats, we onboard specialists and support enabling Microsoft solutions and capabilities.

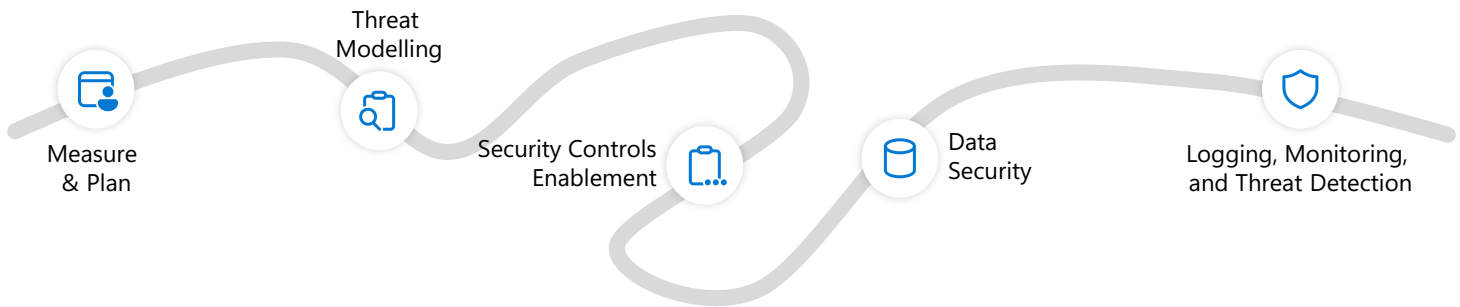


Our Threat Modelling approach is backed by the MITRE Atlas® and OWASP® frameworks for identifying risks across all AI workloads.



Scope

From 16 to 28 weeks



Benefits



Why Microsoft Industry Solutions Delivery (ISD)

Industry Solutions Delivery (ISD): The what and why?

Mission

AI-first consulting capability to ensure acceleration of commercial cloud growth by deploying outcome-based, complex solutions where the customer wants Microsoft to take accountability for end-to-end project delivery.

ISD's world-class skills provides customers...

Tailored Expertise

We listen closely, applying our deep Microsoft knowledge to **develop and deliver solutions** that address each customer's unique challenges.

Consultative Solutions

We specialize in **Microsoft platforms and leading AI solutions** to connect customer needs with the right products, ensuring impactful results.

Swift, Tangible Impact

We accelerate success with **innovative IP** and AI technical depth to drive measurable results while **embedding security** across every step.

Trusted Orchestration

We take ownership, **blending Microsoft's ecosystem of proven partners** to reduce risk and deliver comprehensive solutions on time.

Next steps

Contact your Microsoft Services representative to learn how to best secure your AI environment and ensure responsible adoption.