

# Adopt agentic AI with confidence with our Security for AI solutions

Unlock the full potential of artificial intelligence while improving the security and trustworthiness of your AI solutions.

### Partner with Confidence—Secure AI from Strategy to Execution

Closing the AI security gap requires more than just technology—it demands a trusted partner. IBM Consulting Cybersecurity Services provides end-to-end support to help you secure AI at every stage:

#### 1. **AI Security Strategy & Governance**

Assess your enterprise AI agents and application landscape to identify risks and develop a strategy to remediate and deploy a strategic AI security solution.

#### 2. **AI Security Posture Management**

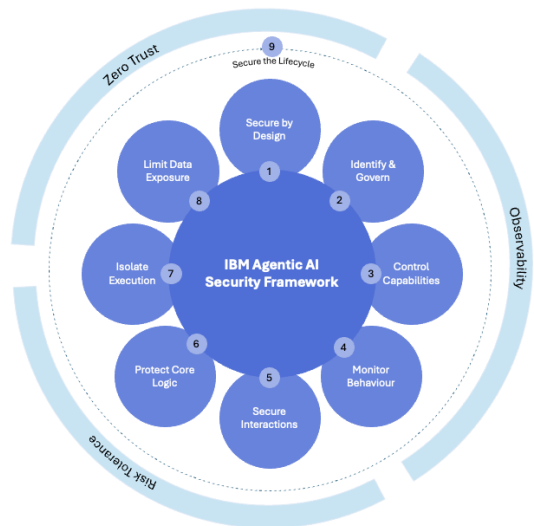
Identify and govern shadow AI and AI agents at enterprise scale and sustain desirable AI security posture.

#### 3. **AI Secure Integration & Operations**

Design and deploy best in class security for bespoke and platform agentic AI applications.

#### 4. **Security Testing**

Penetration testing and scenario-based assessments for GenAI and Agentic AI systems.



IBM Agentic AI security framework

With IBM Security for AI Transformation Services, organizations like yours can build, deploy, and manage more secure, reliable, and compliant AI solutions. Our comprehensive approach will:

- Build trust in your Agentic AI solutions, helping to ensure the confidentiality, integrity, and availability of sensitive data
- Proactively address Agentic AI-related risks and vulnerabilities to mitigate costly breaches and reputational damage
- Drive business innovation while supporting regulatory compliance and reducing the burden of AI risk management

With our expertise, you can unlock the full potential of AI, accelerate your digital transformation and drive sustainable business growth.

Contact your IBM Sales rep for further information



© Copyright IBM Corporation 2025. IBM and the IBM logo are trademarks or registered trademarks of IBM Corp., in the U.S. and/or other countries.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.