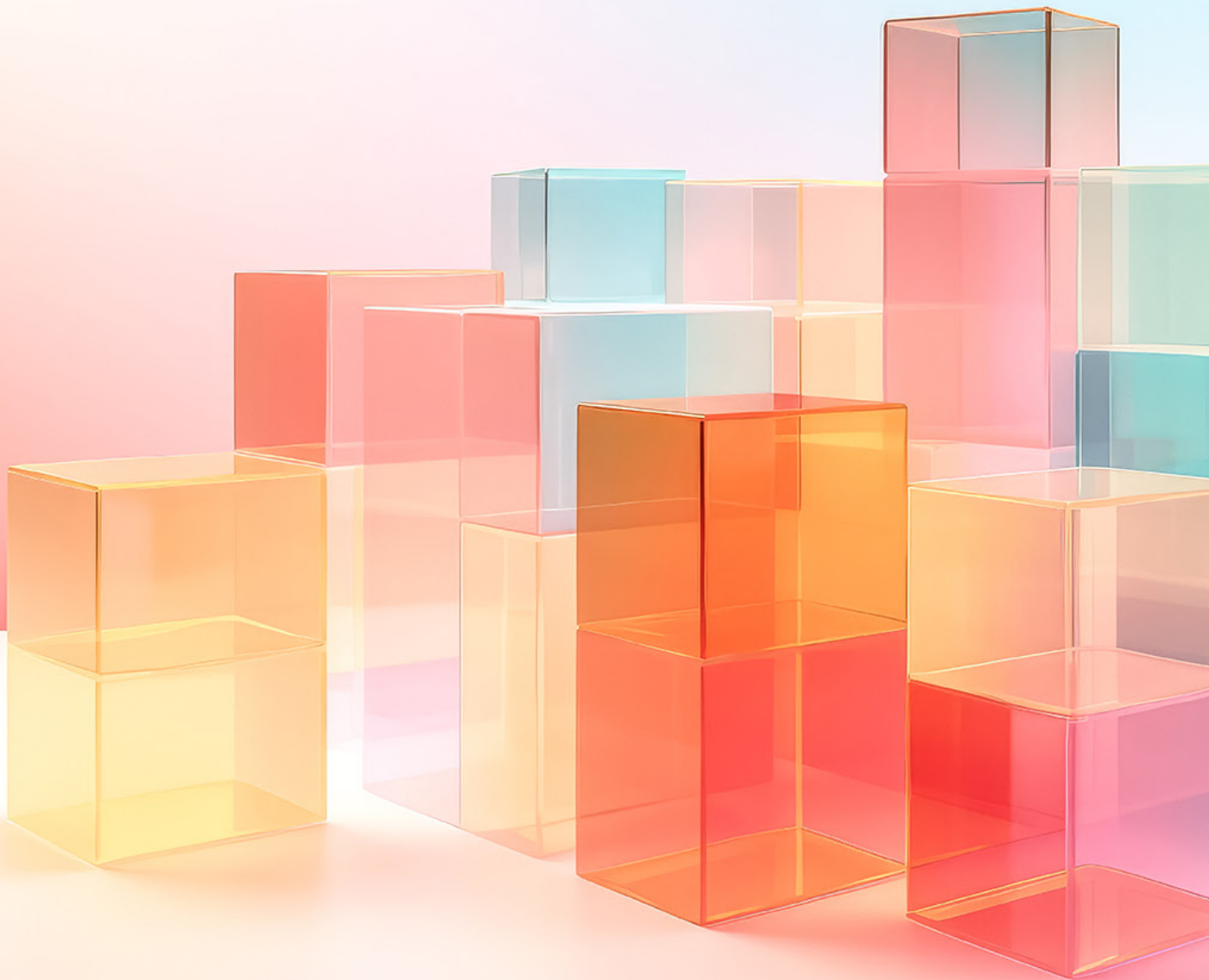


AI Assurance Services

Enabling safe, reliable and accountable
AI adoption across the enterprise



Overview

Artificial intelligence (AI) is quickly changing the way businesses work, bringing new ideas, efficiency and opportunities. As enterprises start using AI in critical systems and daily operations, it becomes crucial to make sure these technologies are safe, reliable and used responsibly. Because AI works with large amounts of data, uses complex algorithms and can sometimes carry hidden biases, it also creates new risks that traditional security methods can't fully handle. This white paper introduces HCLTech AI Assurance, a comprehensive set of services that help organizations adopt AI with confidence while reducing risks and promoting responsible use.

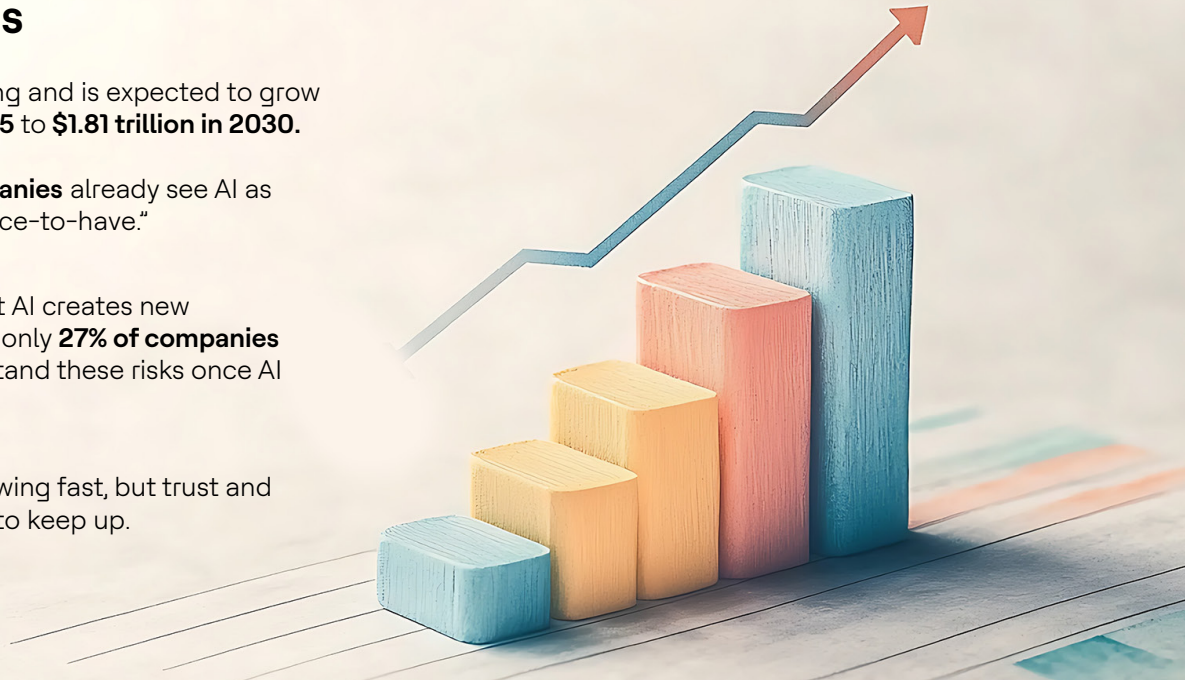
Market trends

The AI market is booming and is expected to grow from **\$391 billion in 2025** to **\$1.81 trillion in 2030**.

91% of mid-sized companies already see AI as a "must-have," not a "nice-to-have."

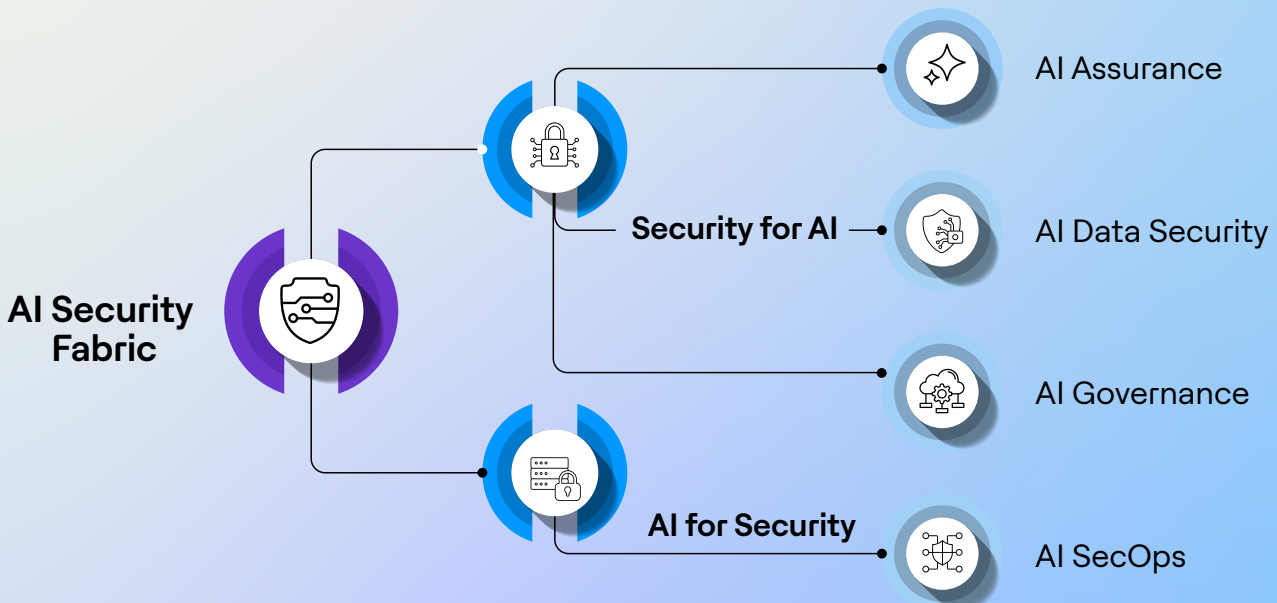
81% of CISOs worry that AI creates new cybersecurity risks, but only **27% of companies** say they clearly understand these risks once AI is in production.

The takeaway: AI is growing fast, but trust and security are struggling to keep up.



HCLTech in AI and Security

HCLTech delivers scalable AI cybersecurity that secures AI systems as well as leverages AI to enhance enterprise security. By treating AI as core infrastructure, we embed governance, compliance and threat intelligence into every layer enabling organizations to operationalize AI securely while using AI-driven insights to strengthen cyber resilience across the enterprise.



We see the connection between AI and Security in two ways: how we secure AI itself and how we use AI to make security stronger.

Security for AI: Protecting AI systems



Governance: We help organizations set-up the right policies, frameworks and checks to make sure AI is used responsibly and in-line with regulations.



Data security: Since AI depends heavily on data, we focus on protecting training and inference data from leaks, tampering or misuse. This helps reduce risks like data poisoning or exposure of sensitive information.



AI Assurance: We ensure AI systems are trustworthy by rigorously testing their reliability, resilience, fairness and ethical compliance.

AI for Security – Using AI to defend smarter

AI-driven Security Operations (SecOps): We use AI to transform security operations by analyzing massive amounts of data in real time, detecting advanced threats that traditional tools often miss and automating routine tasks. This speeds up incident response, strengthens defenses and allows security teams to focus on critical, high-value priorities

This two-pronged approach ensures that we are not only making AI safe for businesses but also using AI to create stronger security for the enterprise as a whole.

Introducing HCLTech AI Assurance: A comprehensive offering

HCLTech AI Assurance helps organizations adopt AI with confidence by embedding security, reliability and governance at every stage of the AI lifecycle. Our approach ensures trusted, responsible and scalable AI adoption.

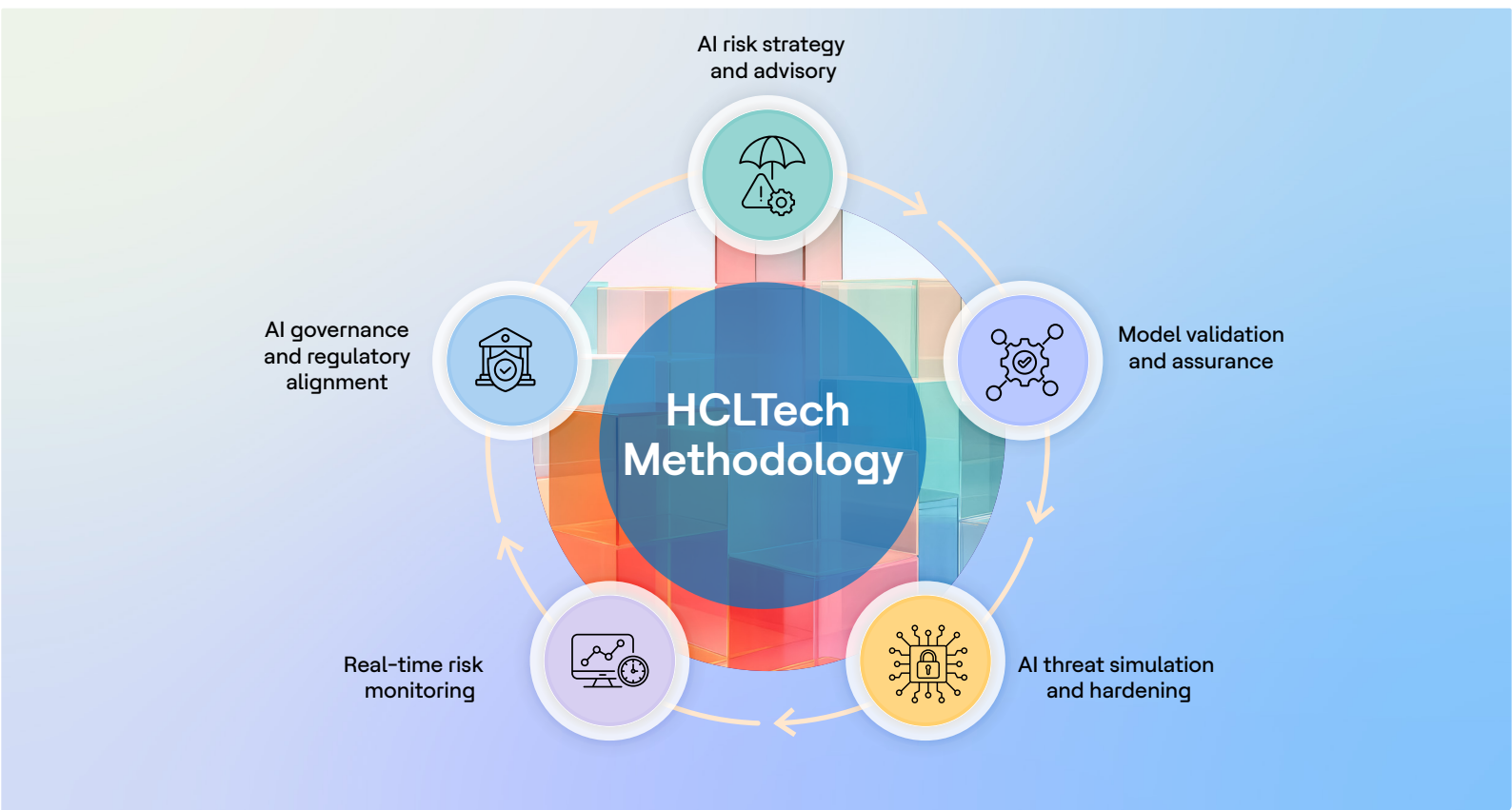
We follow a secure-by-design approach, meaning we add security right from the start of AI development to reduce risks early. Our AI SecOps and DevSecOps practices make security a continuous part of the development and operations process, encouraging close teamwork between data scientists, developers and security experts. We also use adversarial testing and validation to carefully test AI models against potential attacks, making sure they remain strong and reliable. Along with this, we create a comprehensive AI security posture that protects data, models, infrastructure and access controls. Finally, our governance framework- NIST AI RMF, AI-TRISM, AI-MAESTRO and accelerators like VERITY for AI ensure that AI is built and deployed in line with industry standards, regulations and ethical practices



Key elements of the HCLTech AI Assurance framework

Our comprehensive framework is structured around several key elements, ensuring a layered and proactive approach to AI assurance:

AI platform management Securing the underlying infrastructure and platforms used for AI development and deployment.	AI app security Protecting AI-powered applications and their integrations from security threats.	AI security posture management Continuously assessing and improving the overall security posture of AI systems.
Model and agent testing Thoroughly evaluating the security, reliability and performance of AI models and intelligent agents.	AI pen testing Simulating real-world attacks to identify and exploit vulnerabilities in AI systems.	AI red teaming Deploying skilled security experts to emulate sophisticated attackers and uncover hidden weaknesses.



Delivering tangible business outcomes

By partnering with HCLTech for AI Assurance, organizations can achieve significant business outcomes, including:

Secure model usage Mitigating prompt injections, jailbreaks and data leakage across model and app layers.	Reliable AI Developing AI models that behave as intended, reducing hallucinations, unfair outputs and biased decisions.	Accelerated AI adoption Enabling faster and safer innovation by embedding trust and compliance from day zero.
Actionable posture reporting Providing accountable reporting on vulnerabilities, threat models, asset inventory, and remediation steps.	Shift left assurance Integrating security and testing early in the AI lifecycle, reducing downstream risk and costs.	

Our methodology: Supporting your end-to-end journey

HCLTech's AI Assurance methodology is designed to support clients across their entire AI journey, from building the right strategy to maintaining strong governance over time. We start with **AI risk strategy and advisory**, where we define the security roadmap, profile risks and guide organizations through security-by-design practices. Next, **our model validation and assurance** process tests custom AI and large language model workloads, including adversarial checks, jailbreak testing and fairness assessments.

We then move to **AI threat simulation and hardening**, running red team exercises, fixing misconfiguration and strengthening the security of AI applications and APIs. To stay ahead of risks, we enable **real-time monitoring**, which includes prompt tracing, hallucination detection, drift analysis and SOC integration for visibility. Finally, our **AI governance and regulatory alignment** ensures ongoing compliance with regulations, strong privacy safeguards, controlled model access and readiness for audits.

Conclusion: Partnering for a secure AI future

As organizations navigate the transformative potential of AI, ensuring its security and reliability is no longer an option but a necessity. HCLTech AI Assurance offers a comprehensive and pragmatic solution to address the unique challenges of AI security across the entire lifecycle. By partnering with HCLTech, you can confidently accelerate your AI adoption journey, mitigate emerging threats, build trust in your AI systems and unlock the full potential of AI innovation. Connect with HCLTech to explore how AI Assurance can accelerate your secure AI journey.



HCLTech | Supercharging
Progress™

hcltech.com