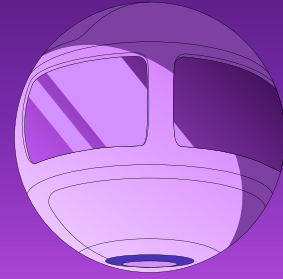


AI Security Risk Assessment

Unlock AI Innovation - Securely

Pair our experts with yours to build the confidence, visibility, and control needed to accelerate high-value AI initiatives – without compromising on security.



Build a Secure Foundation for AI Success

The AI security landscape is evolving rapidly, creating an urgent need for organizations, like yours, to establish a robust security posture before risks materialize. Regulatory scrutiny is intensifying, new attack surfaces are emerging, AI adoption is accelerating, and board-level pressure is increasing. All leading to the need to be ready today.

Establish a solid foundation.

Create a comprehensive, strategic security-first framework to deploy AI safely.

Enable faster, safer scaling.

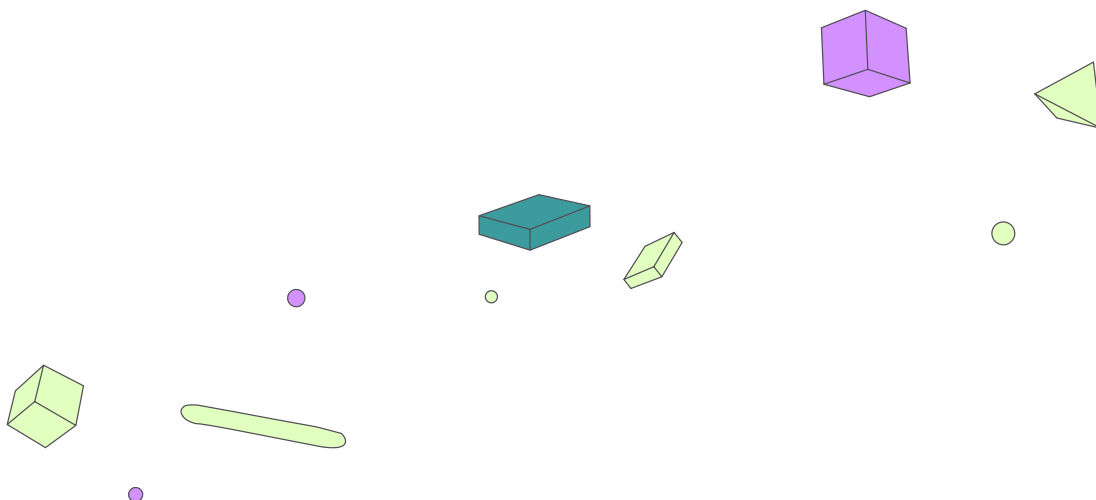
Accelerate deployment of high-value AI use cases, specific to your organization.

Know where to go next.

Establish a detailed baseline of AI security maturity and develop a clear, actionable roadmap on how to move forward.

Proactively mitigate risk.

Manage emerging vulnerabilities and threats across the entire AI ecosystem.



Comprehensive Security Evaluation

Cyera experts will examine your AI program, evaluating security and governance controls across the complete AI lifecycle. We'll focus on eight critical, and interconnected, domains that collectively determine your organization's ability to deploy AI safely and responsibly. And that no blind spots - from data models to operations - exist.

AI Governance Policies, oversight structures, and responsible AI frameworks.	Data Security Training data protection, provenance, and privacy controls.	Infrastructure Network, compute, and cloud security for AI workloads.	Agent & Model Security Development, deployment, and runtime protections.
Interface Security API, plugin, and integration security controls.	Application Security Input validation, output filtering, and guardrails.	Identity & Access Authentication, authorization, and privilege management.	Detection & Response Monitoring, threat detection, and incident handling.

Examine your AI program through a holistic lens

The Assessment will determine true operational maturity, along with detailed evidence and specific recommendations. The assessment produces actionable deliverables designed to support immediate decision-making, drive AI security improvements, and enable ongoing program management.

Policy & Standards.	Documented requirements, guidelines, and governance frameworks.
Implementation.	Technical capabilities and controls, processes, and tooling deployed in practice.
Monitoring & Measurement.	Visibility, metrics, testing, and compliance validation mechanisms.
Improvement.	Feedback loops, optimization programs, and proactive risk management.

Ready to get started? Let's talk. Contact us at cyera.com/ai-security-risk-assessment