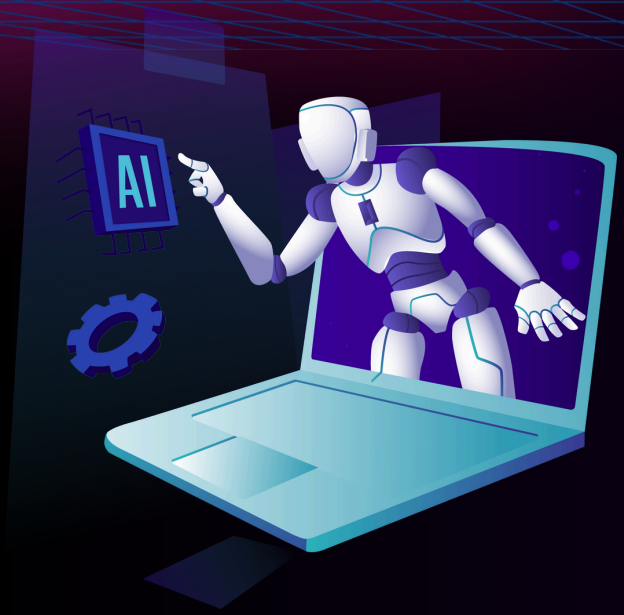

ENTERSOFT | AI -AST™

ENTERSOFT

WHAT IS AI-AST™

Securing systems that think, decide, and act

AI-AST™ (AI Application Security Testing) is Entersoft's proprietary framework to test AI behavior, not just applications.

AI-AST™ Coverage (Big Picture)

Any System That Thinks, Decides, or Acts

It evaluates:

- How AI systems respond under attack
- How decisions can be manipulated
- How autonomy and intelligence can be abused

Think of it as:

Pen-testing for AI reasoning and decision-making.

CONTACT US

+91 8885462220

hari@entersoftsecurity.com

2nd Floor Skyview 10 Hitech City Hyderabad

https://entersoftsecurity.com/

ENTERSOFT | AI -AST ™

WHY AI CHANGES SECURITY:

Security Has Changed. AI Changed It.

- **Traditional apps follow rules**
- **AI systems learn, reason, retrieve, and act**
- **Attacks no longer target just code — they target decisions**

Key Message:

SAST & DAST were never designed to test intelligence.

WHAT AI-AST™ COVERS:

One framework. Multiple AI realities.

- LLM-powered applications
- RAG (Retrieval-Augmented Generation) systems
- Classical Machine Learning models
- Autonomous & agentic AI
- AI exposed via APIs
- AI governance & compliance readiness

ENTERSOFT

WHAT CUSTOMERS GET

Clear, Actionable Outcomes

- AI Threat Model & Attack Surface Map
- CVSS-rated findings with business impact
- Proof-of-Concept attack evidence
- Remediation & hardening guidance
- 30-day validation / retest option
- Compliance mapping (OWASP, NIST, ISO)
- Executive & technical reports

Not theory. Not checklists. Real outcomes.

Powered by Entersoft Security | 13+ Years of Offensive Security Excellence

INDICATIVE AI-AST RATE CARD (USD)

Pricing adjusted using AI Gravity.

RAG AST: $5k – $10k

LLM AST: $5k – $12k

ML AST: $6k – $12k

Agent AST: $7k – $15k

AI API AST: $5k – $9k

AI Governance Audit: $6k – $15k

ENTERSOFT | AI-AST™

PRICING MODEL

Designed in alignment with global AI security and governance standards trusted by enterprises and regulators.

OWASP Top 10 LLM

Artificial Intelligence Risk Management ISO/IEC 23894 FOUNDATION ITCERTS CERTIFIED

NIST AI RMF

Digital Personal Data Protection Act (DPDP) 2023 INDIA

Not All AI Systems Carry the Same Risk

ENTERSOFT

THE AI GRAVITY CONCEPT

Entersoft uses AI Gravity to size security effort fairly.

We assess:

- LLM usage
- RAG & data size
- Autonomous actions
- Public exposure
- Regulatory impact
- Production criticality

Higher AI Gravity = Higher risk = Deeper testing