## WHAT WE OFFER

END-TO-END, INTEROPERABLE, EASY TO DEPLOY & MANAGE, Designed for the Enterprise.
Enhance, Optimize, Manage security of GenAI applications and workflows in your Organization.

1. Discover, Track, Lineage of AI assets.
   Trace back to single point-of-origin with AI lineage. 360 view command, control, reconnaissance, lateral movements.

2. Detect Adversarial attacks on LLM applications, Models, Poison, Evasion, Exfiltration, Infiltration, Feature corruption attacks etc,using IOC, IOA's, and AI Threat intelligence.

3. Automate LLM and model Vulnerability scan. Domain specific security guardrails, integrations. Recommendations, Reviews ,Issues, Model, LLM, Prompt, RAG, Vulnerability database.

## WHY CHOOSE US?

Generative AI is New Attack Vector endangering Enterprises. Elevate Security for high-value use cases. Ensure the reliability and trustworthiness of LLMs.

1. Training, Evaluation, Inference analytics, Model behavior analytics, Prompt usage analytics.
   Detect Rogue Models, Risky pipelines, Harmful Prompts.

2. Zero-Trust LLM applications.
   Ensure Integrity, Reliability of LLM applications.
   Integrity verification's at runtime.
   Enhanced domain-specific security guardrails.

3. Ensure security controls to LLM's ready for enterprise infrastructure.
   Assign the AI service roles on the AI resource's to Managed identities.
   Spot and Stop Attacks on AI compute, gpu, external,internal traffic, denial attacks.

ALERT AI

## #1 GEN AI SECURITY PLATFORM

**Alert AI** is interoperable, end-to-end security platform for Generative AI applications and workflows across Industries.

With over 100+ Integrations, 1000's of detections, Easy to deploy and manage services **Alert AI** seamlessly integrates to provide 360 degrees Visibility, Vulnerability management, Adversarial threat detection, Data Privacy, Integrity Monitoring, AI Forensics domain-specific security guardrails in GenAI applications and workflows.

## WHAT WE OFFER:

Generative AI opens up all kinds of opportunities to obtain sensitive data. Generative AI pose the greatest risk yet with a variety of concerns around.

1. Detect, Redact, Alert Sensitive information disclosures, Data privacy violations, PII, PHI, Copyright Legal exposures in all Generative AI applications in environment

2. Interoperable with your GenAI stack integrations with top providers, platforms, tools.

3. Enriched ADR(AI Detection & Response) events with Alert data and forward to SIEM.

## GET IN TOUCH

We are seeking to work with exceptional people who adopt, drive AI transformation.
We want to know from you to better understand GenAI in business to secure GenAI applications better.

### VISIT US

www.alertai.com

### GET STARTED

@ contact@alertai.com

ALERT AI

## OUR ADVANTAGES:

With over 100+ integrations and 1000+ detections, domain-specific security guardrails, easy-to-deploy & manage security platform seamlessly integrates AI workflows and applications.

1. AI Visibility and AI Asset Access Usage Analytics.
   Tracking and Lineage Analysis.
   Adversarial ML detections in AI Footprint.

2. Detetion & Respose Engine Data leakage AI Incidents.
   LLM & Model Vulnerability Management.
   Pipeline, Data leakage, Integrity monitoring.
   Model Risk analysis.

3. Privacy, Sensitive Information Filtering.
   Domain-specific security guardrails.
   Security posture, Recommendations.
   AI Forensics, AI Incident Response to SIEM.
   AI Audits, Complaince, Governance Reports.