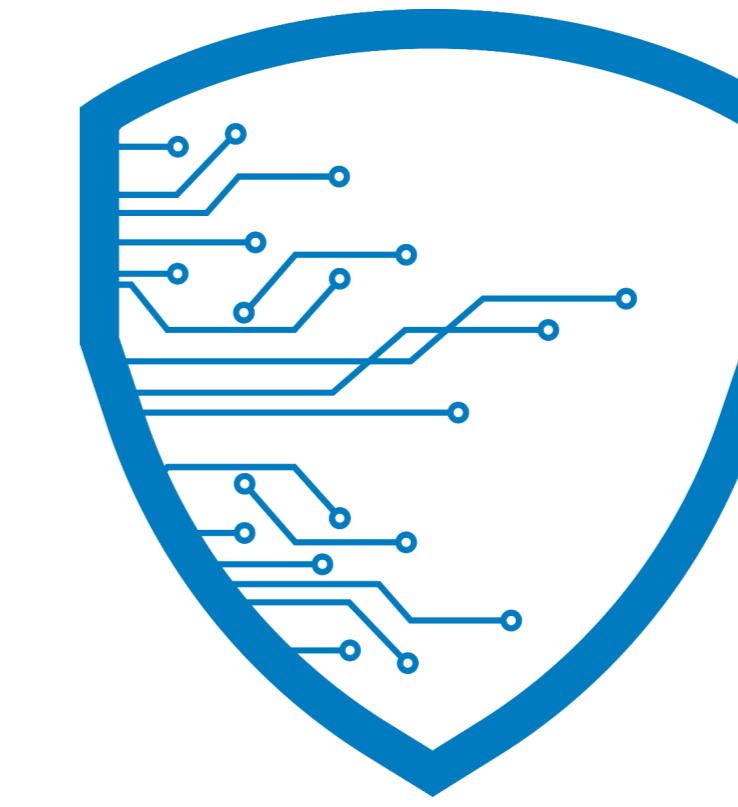


Join the frontier of AI Security

Ready to elevate your AI's defense?
Contact us today.



AIShield

Powered by Bosch

About AIShield

AIShield, a Gartner-recognized AI Application Security company backed by Bosch, is at the forefront of AI security across the globe. AIShield's enterprise-grade products and solutions are strongly supported by an extensive portfolio of 40+ patents.

Founded in 2022, AIShield proudly serves 40+ customers across diverse industry verticals, including healthcare, banking, telecom, automotive, manufacturing, and cyber-defense, across the US, APAC, and EMEA regions.

AIShield's strategic collaborations with prominent players in technology, IT consulting, cloud, MLOps, and cybersecurity position us as an integral part of the AI/ML ecosystem.



Location
Bengaluru, India



Email
AIShield.Contact@bosch.com



Website
www.boschaishield.com

FULL STACK AI APPLICATION SECURITY

Protecting AI models and Generative AI applications across the lifecycle:
Any Model. Any Framework. Any Deployment.



Connect with AIShield: Every Link, One Scan



AIShield Watchtower

AI Unveiled. Risks Revealed.

An open-source tool for automated AI Model Discovery and Vulnerability Assessment

- Automated Model Discovery**
Discovers AI models and related artifacts in repositories
- Comprehensive Vulnerability Assessment**
Auto-assesses vulnerabilities related to model and its artifacts
- Dynamic Monitoring**
Monitors and evaluates model changes and triggers relevant assessments
- Risk Identification**
Assesses risks: hardcoded secrets, PII, outdated/unsafe libraries, model serialization attacks, custom unsafe operations etc.
- Alignment with Industry Standards**
Aligns with OWASP, MITRE, NIST AI RMF MAP function and CWE standards

Benefits

- Zero cost AI/ML asset discovery and risk identification
- Actionable reports for securing models
- Developer-friendly integration for efficiency
- Empirically validated in real time

AIShield Platform

Assess. Detect. Defend.

An enterprise-grade, AI AppSec SaaS Product, safeguarding AI systems from adversarial ML threats

- Vulnerability Scanning**
Analyzes AI/ML models against theft, poisoning, evasion, and inference
- End-Point Protection**
Generates threat-informed defenses and provides attack data for model hardening
- Intrusion Detection**
Monitors and prevents real-time attacks, both in the cloud and on devices
- Threat Intelligence / Telemetry SIEM**
Pursues active threat hunting with incident alerting
- Comprehensive Reporting**
Real-time AI Security posture and dashboards for organization leaders

Benefits

- More than 90% OWASP Top 10 ML risks coverage
- 7x to 15x ROI via Holistic AI Risk Mitigation
- Reduce critical vulnerabilities by up to 90%
- Accelerated time to value with brand & IP protection
- Regulatory preparedness in line with MITRE ATLAS, NIST AI RMF with full ZTA

AIShield GuArdlan

Defy Risks. Harness GenAI's scale.

Robust guardrails for safe and compliant enterprise adoption of Generative AI

- I/O Filtering**
Filters content while preventing and logging enterprise policy violations
- Cybersecurity Risk Management**
Mitigate cybersecurity risks associated with prompt injections, jailbreaks & evasion attacks
- Ease-of-Use & Observability**
Seamless application integration via Python SDK and dashboard
- Role-Based Policy Enforcement**
User and role-based dynamic policy enforcement
- LLM Agnostic**
Compatible with all LLMs and deployment scenarios

Benefits

- More than 70% OWASP Top 10 LLM risks coverage
- Protection against the loss of valuable IP, PII and trade secrets
- Facilitates responsible and careful experimentation
- Safety & compliance automation

AI/ML Development

AI/ML Operations

Lifecycle of AI/ML Application development