
AIShield
AIShield
Powered by Bosch

The need to secure AI with a case in point (pedestrian detection)

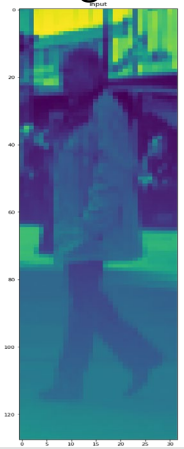
Impact across Individuals, Organizations & Society

Developed over months with large proprietary datasets

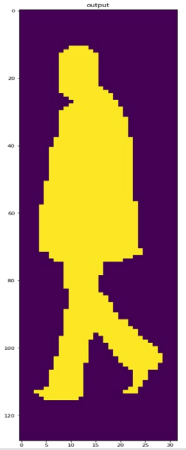
Investment:

~Euro 2mn

Original

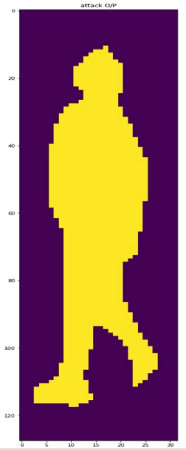


Human labeled



Original Model

Stolen Model



Stolen in <2 hours at Fraction of cost & less than 4% delta to original model accuracy

Autonomous Vehicles
- Algorithm stealing
- Vehicle malfunction

Industry 4.0
- State sponsored attacks
- Compromised Predictive maintenance algorithms

BFSI
- Fraud detection failure
- Compromised credit scoring

Healthcare
- Personal Identifiable Information disclosure
- Medical misdiagnosis

Video Surveillance
- Misidentification
- Perimeter security breach

AI models are **highly invested** and most **valuable assets** of an AI system.

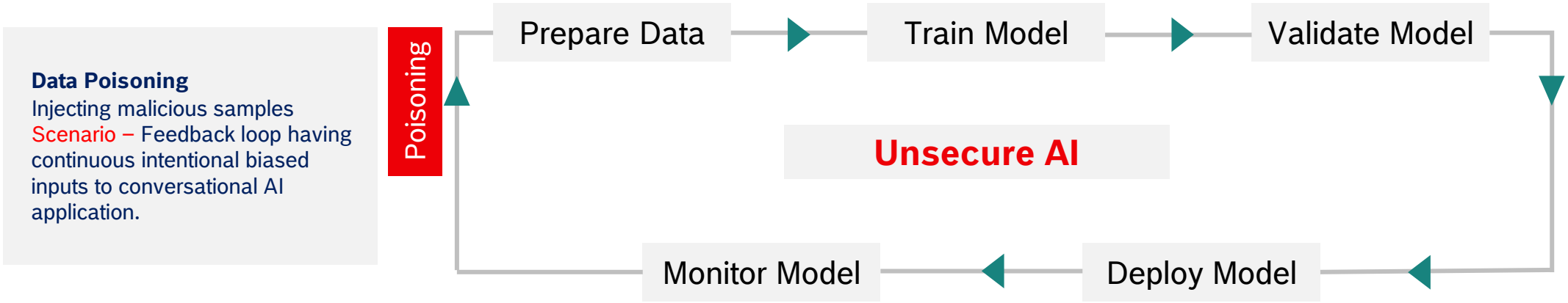
AI models **can be hacked** to cause **financial loss, brand reputation damage, loss of competitive advantage & loss of intellectual property** to an organization.

AI model and system security needs to be included in the existing Cybersecurity measures.

AIShield Powered by Bosch

Understanding the attacks across the model lifecycle

Adversarial threats to AI/ML models



Data Poisoning
Injecting malicious samples
Scenario – Feedback loop having continuous intentional biased inputs to conversational AI application.

Extraction

Model Extraction
Steal/replicate IP
Scenario – Software stealing followed by unlicensed usage, malfunction and further attacks.

Evasion

Model Evasion
Evade AI application analysis
Scenario - Camouflage from video surveillance or fraud detection applications leveraging adversarial examples.

Inference

Membership Inference
Access data record information
Scenario – Compromised personal data when hackers infer the AI/ML model and associated data.

AIShield Powered by Bosch

How common are AI attacks?

“2 in 5 organizations had an AI privacy breach or security incident, of which 1 in 4 were malicious attacks. Conventional controls ARE NOT enough.”

41%

Organizations experienced AI Attacks

Organizations surveyed by Gartner had experienced an AI privacy breach or security incident

60%

Faced data compromised by internal party

Insider attacks

27%

Malicious attacks on organizations AI Assets

Malicious attacks on the organization’s AI infrastructure by adversaries

Gartner®

Managing AI Risks Pays off

For better business outcomes and also for regulatory compliance

Source: Gartner Blog: AI Models under Attack; Conventional Controls are not Enough *By Avivah Litan| August 05, 2022*
https://blogs.gartner.com/avivah-litan/2022/08/05/ai-models-under-attack-conventional-controls-are-not-enough/

The global market for AI security is expected to be $35 billion by 2028.

Bloomberg

AIShield Powered by Bosch

AI Security to be driven by regulations as well

Proposed Regulations, Guidelines and Research

Sectoral

Healthcare

FDA U.S. FOOD & DRUG ADMINISTRATION

IMDRF International Medical Device Regulators Forum

Proposed regulatory framework for AI based Software as a Medical Device

Banking

New proposed cybersecrity risk management riles to improve the resilience of investment advisers and investment ; Algorithmic Accountability Act

Telecom

ETSI

ETSI SAI (Securing Artificial Intelligence) for: Securing AI from attacks, Mitigating against malicious AI, Using AI to enhance security measures

Automotive

ISO UNECE

UNECE WP.29/UN Regulation No. 155 - Cyber security and cyber security management system – applicable for managing AI risks in vehicles

Horizontal

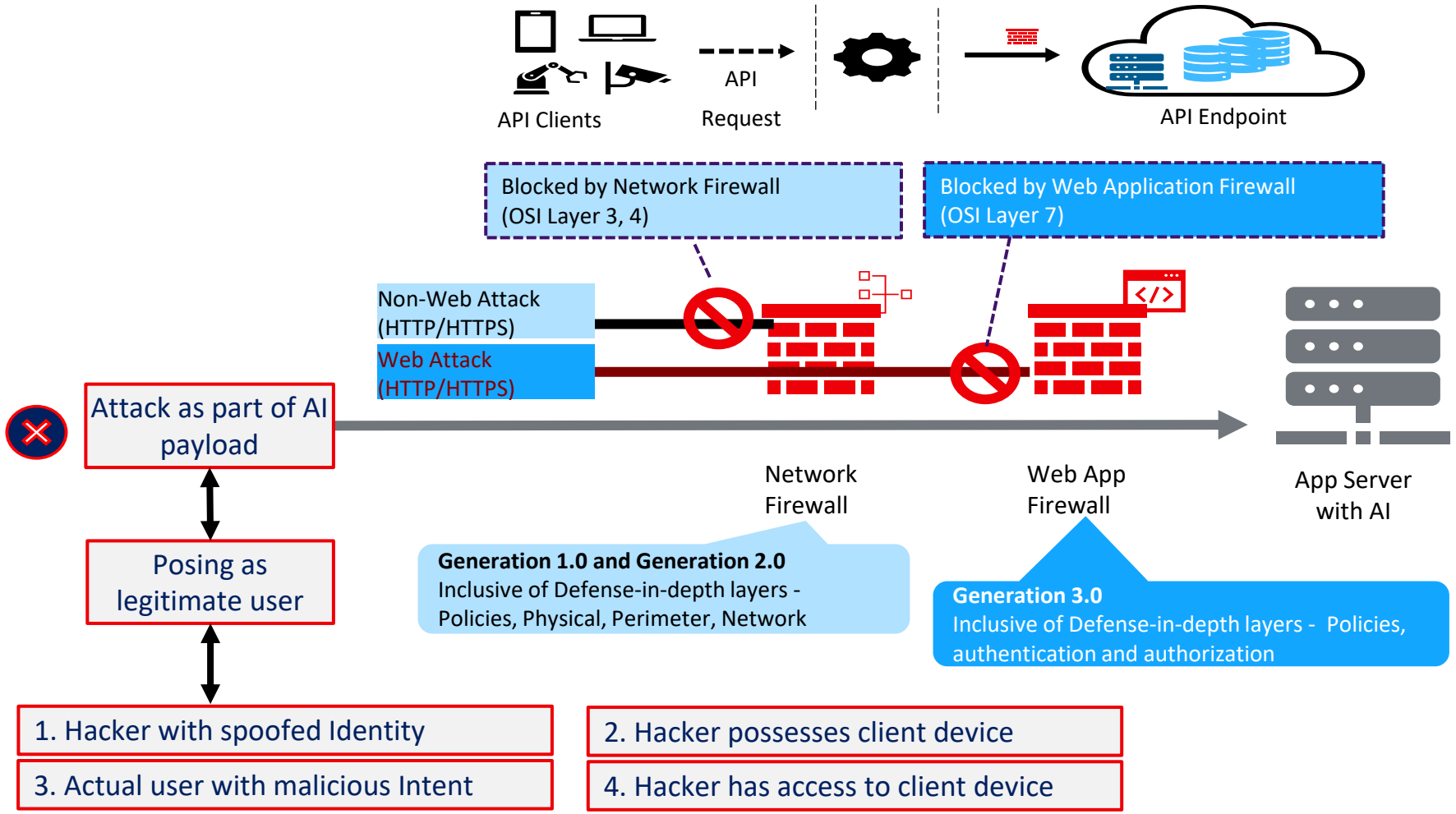
EU AI Act - Proposed regulation laying down harmonized rules on artificial intelligence

New proposed cybersecrity risk management riles to improve the resilience of companies against cybersecurity threats and attacks

NIST National Institute of Standards and Technology

AI Risk Management Framework to better manage risks to individuals, organizations, and society associated with AI

Can AI assets be compromised despite existing measures?
YES



Introducing AIShield
Solution Overview

One stop solution to secure AI across:

Lifecycle | Use cases | Models

AI Security solution offered as:

Product - API | Enterprise Solutions

Implementation Partners:

Industry Associations:

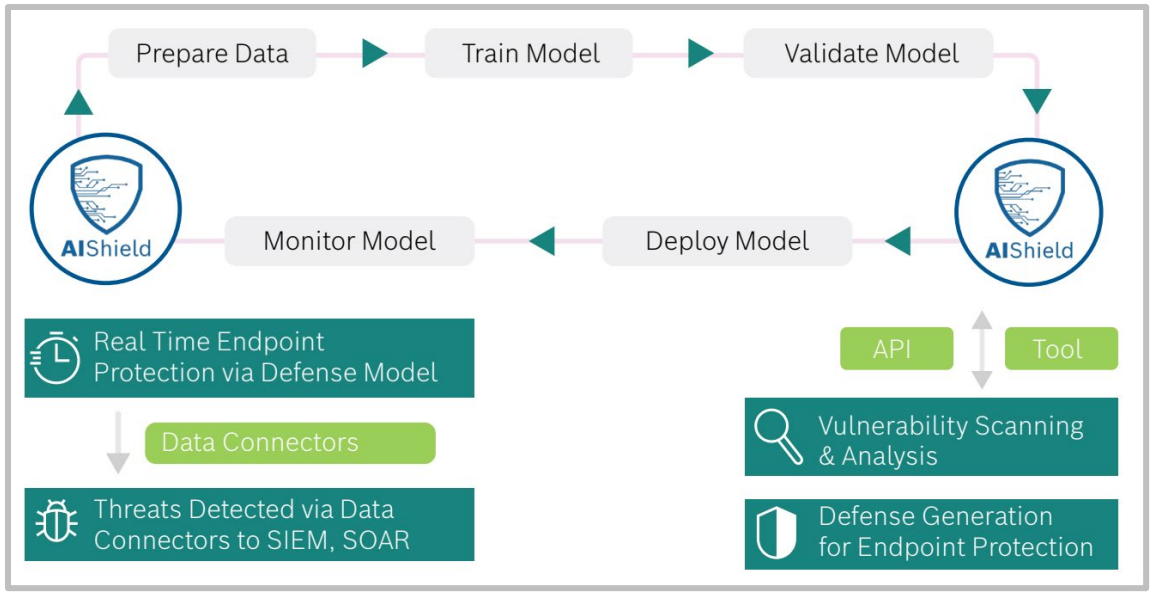
Deployment flexibility:

On prem | Edge | Cloud

Input:
- AI/ML model file (encrypted or via endpoint)
- Validation data subset (optional)

AIShield

- Vulnerability assessment & Defense Mechanism
- Threat-Informed EDR (End Point Defense and Response)
- MLOps and SIEM Integration

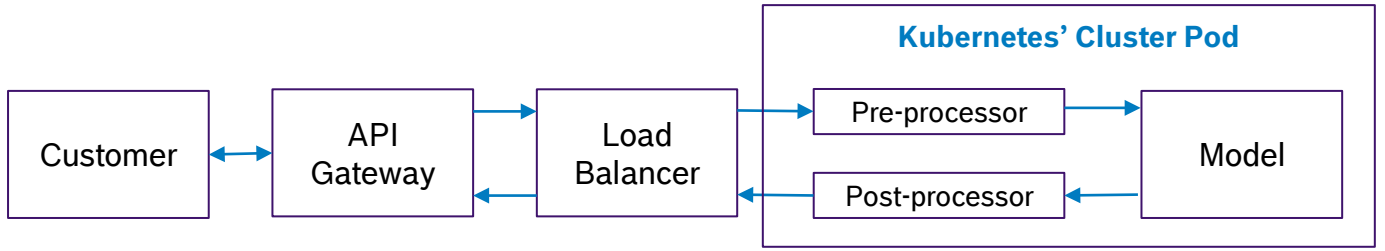


AIShield Powered by Bosch

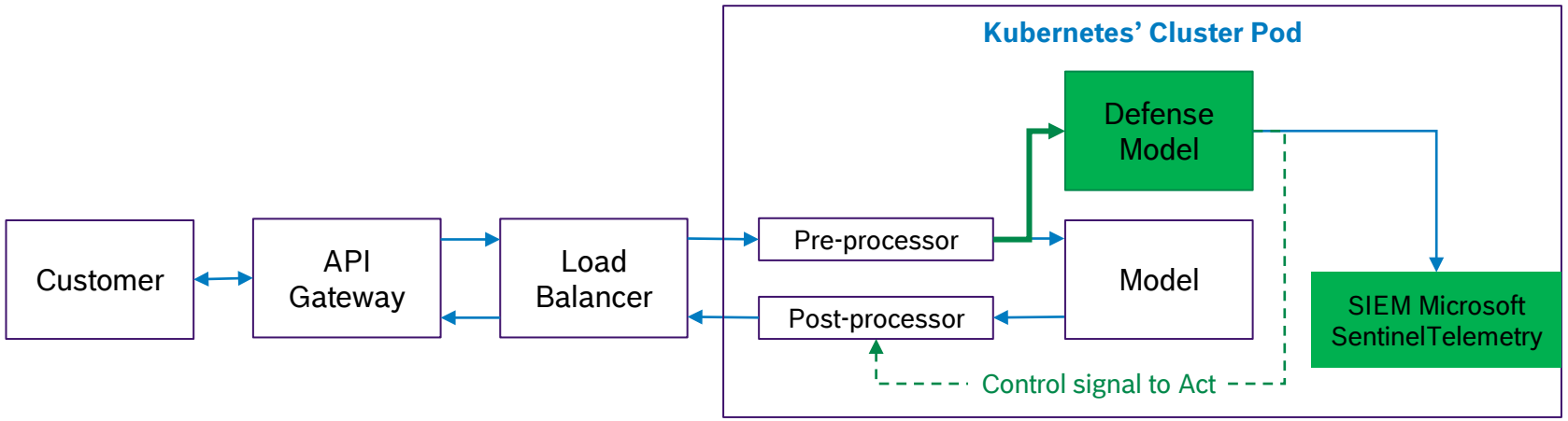
AIShield Solution Architecture – Block Level Overview

Cloud Based Workload | Parallel Detection | System-dependent Action

Without AIShield



With AIShield



AIShield Powered by Bosch

AIShield Offerings – Customer View

Vision: Securing any AI Systems of organisation across lifecycle at scale

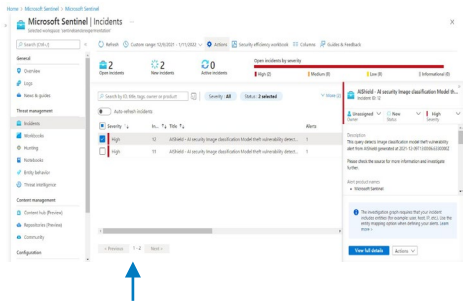
Offering	PRODUCT	SOLUTIONS
Description	API based AI Security Vulnerability assessment and defense	Customized industry specific solution

Features	Technical:
	▪ Enterprise-class AI Model Security Vulnerability assessment and Threat informed defense mechanism
	  ▪ Extraction and Poisoning attacks for Image classification, Sentiment Analysis, Timeseries forecasting/classification, Tabular classification
	  ▪ Direct support for Tensor flow, indirect support for other ML framework
	Usability:
	▪ Easy to use APIs with ready reference implementations documentation and configuration files
	▪ Developer Reports and dashboard
	▪ Working with encrypted AI/ML models or API end point of AI/ML models
	Support:
	▪ Easy integration with MLOps platform with product API
	▪ SIEM/SOAR connectivity via containerized defense (customer to deploy)
		Consulting & Advisory:
		▪ AI Security Overview (Threats landscape, Regulations)
		▪ AI Security Risk Assessment with Report
		▪ AI GRC (Governance, Risk, Compliance)
		
		AI/ML Model Security
		▪ Vulnerability Assessment for all attack types, across AI/ML models and framework (Report)
		▪ Target optimized and Defense Generation & integration
		▪ SIEM/SOAR connector for Security monitoring
		▪ Enterprise integration with MLOps and other dashboards
		
		Trustworthy AI/ML Services (on demand)
		▪ Explainability | Responsible | Performance Assurance

Pricing	Pay per use , Tier based	Connect with sales for custom pricing

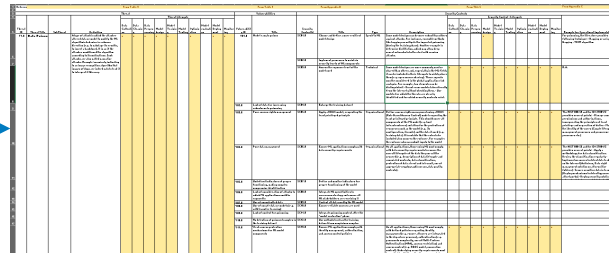
AIShield

AIShield in Development Workflow

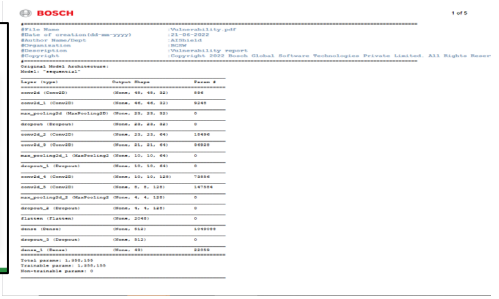


Business Understanding → Data Understanding → Data Preparation → Modelling → Evaluation → Regulatory Compliance → Deployment → Operation → End of Life

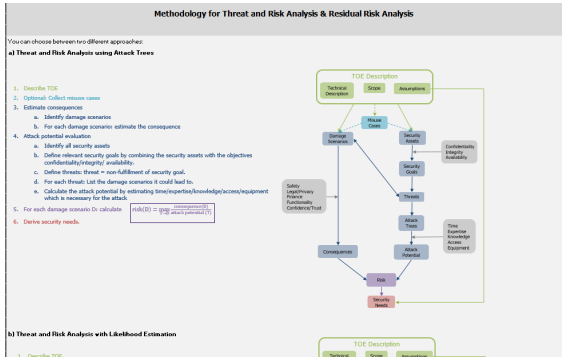
Utilise propreity AI Risk Assessment Framework to Identify Risks



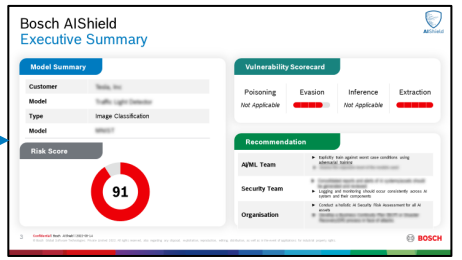
Utilise AIShield Product to provide details and evidence of testing pertaining to known vulnerabilities

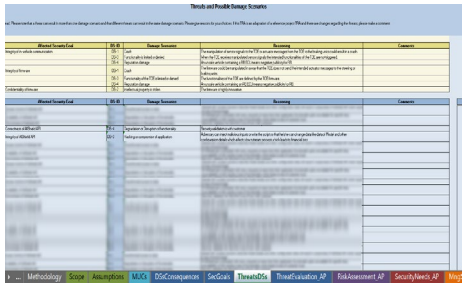


Leverage Threat and Risk Analysis Framework to identify security requirements and threat mitigation measures



Security testing documentation and relevant assessments available for compliance submission purposes





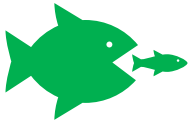
AIShield Powered by Bosch

Why AIShield
Benefits and USP

Trustworthy and secure AI adoption

AI assets intellectual property protection

Prevent brand reputation damage due to AI hacks



Global competitive advantage on AI Security

Unmatched Research
AIShield solution is based on 3 years of unmatched deep technology research

AISecurity Expertise & IP Leadership
AIShield holds 20+ patents in AI Security (Securing AI Systems) space

Product Advantage
An industry-first and production optimized API to secure AI models

Proven Solution
AIShield solution is already deployed across industry use cases

AIShield
Powered by Bosch

Thank You

[AIShield Webpage]

[AIShield Brochure]

[AIShield Intro Video]

[AIShield Product Demo]

[AIShield Linkedin Page]

AIShield

[AIShield at CES 2022]

[AIShield at RSAC]

[AIShield at ET CIO]

[AIShield at AIIA]

[AIShield at AIIA MLOps Summit]

[AIShield at CDMG]

For more information, please contact

Contact AIShield
AIShield.Contact@bosch.com

AIShield
Powered by Bosch