OpsMx

DATASHEET

AI/ML Security with OpsMx Delivery Shield

Secure AI models from prompt attacks and data leaks before they go live

CHALLENGE

AI/ML pipelines face security risks at every stage from ingestion to inference. At **Data Engineering stage,** the vulnerability arises from data poisoning and privacy violations. Risks involved in **Model Engineering stage** are adversarial inputs, model extraction, tampering, and dependency hijacking. Similarly, the **Model Deployment and Runtime stage** expose models to API abuse, DDoS attacks, misconfigurations, and bias exploitation.

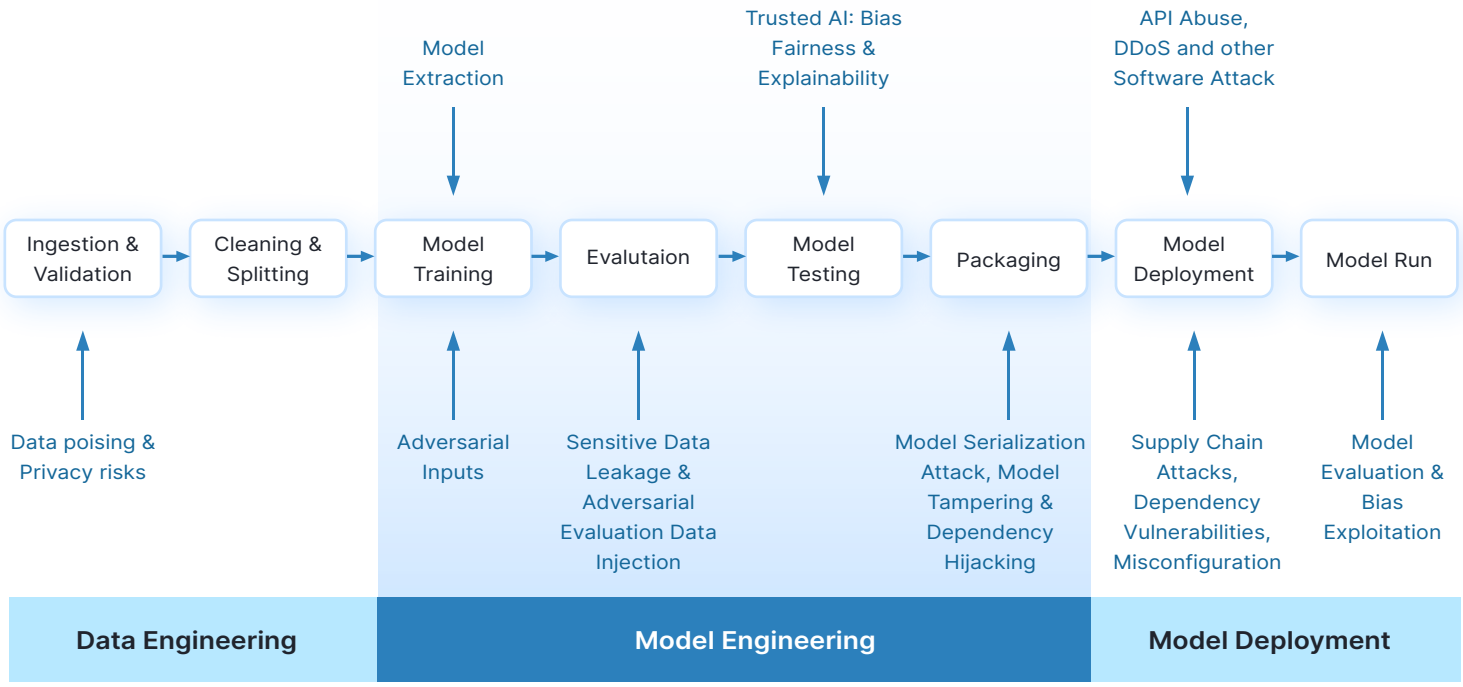

Fig A: Various risks at various stages in the AI/ML Piepeline

Traditional AppSec tools are ill-equipped to handle these evolving threats in the AI context. Manual red-teaming is slow and incomplete, while runtime AI misuse remains largely undetected. What enterprises need is continuous, contextual AI security that spans the entire pipeline without slowing innovation.

AI/ML Security with OpsMx

Secure AI models from prompt attacks and data leaks.

DATASHEET

Solution: End-to-End AI Defense with OpsMx Delivery Shield

OpsMx Delivery Shield embeds security across the ML pipeline by integrating open-source tools like **NBDefense, ModelScan,** and **Garak** to scan code, models, and notebooks at every critical phase—from ingestion and training to packaging and deployment.

These scanners identify risks such as exposed credentials, adversarial prompts, insecure packages, and behavioral drift. Delivery Shield acts as a centralized intelligence layer, aggregating findings, correlating context, and assessing AI risk posture throughout the lifecycle. At the deployment stage, the OpsMx Firewall Agent makes a go/no-go decision based on accumulated evidence—ensuring only safe, compliant, and policy-conformant models are released to production.

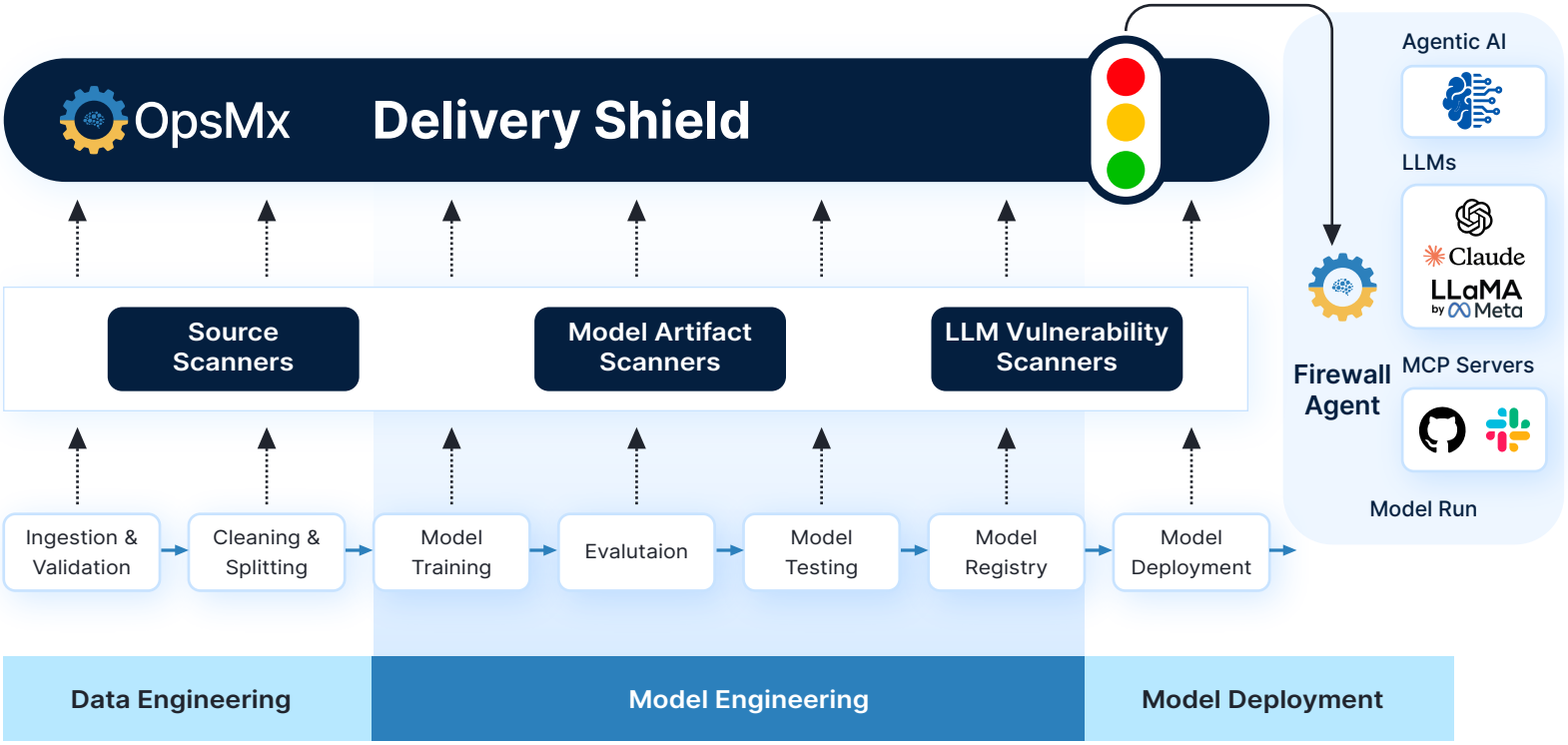

Fig B: OpsMx Delivery Shield embeds security across the ML pipeline

How OpsMx Works

Scans at Every Stage

Integrates tools like Source Scanners, Model-Artifact Scanners, and LLM-Vulnerability Scanners into your ML pipeline.

Contextual AI Intelligence

Collects model metadata, training lineage, usage behavior, and scanner outputs into a unified security graph.

Policy-Driven Decisioning

Applies enterprise-defined policies using contextual insights to determine if a model can safely progress.

Runtime Enforcement

The OpsMx Firewall Agent blocks or allows model promotion or inference based on risk posture and compliance.

OpsMx

AI/ML Security with OpsMx

Secure AI models from prompt attacks and data leaks.

DATASHEET

Core Capabilities

AI Discovery & Shadow AI Detection

- Scans environments to uncover all active AI models, APIs, and tools—including those outside approved pipelines.
- Helps security and compliance teams address unmanaged or rogue AI usage across the enterprise.

AI Security Posture Management (AISPM)

- Aggregates metadata, usage logs, and lineage to assess the risk posture of each AI asset.
- Visual dashboards enable teams to prioritize remediation based on exposure, criticality, and behavior.

Supports AI Red Teaming

- Simulates adversarial prompts and jailbreak attempts to validate model robustness and uncover potential exposures.
- Detects hallucinations, data leakage, and unsafe outputs in pre-production and test environments.

AI Runtime Defense

- Monitors model behavior live during inference to flag abnormal responses, evasion, or misuse.
- Enforces LLM firewalls and dynamic security rules to block prompt-based threats in real time.

Agentic AI Security

- Support proactive, reactive, and detective security controls to safeguard agentic AI systems, LLMs, and ML models.
- Reacts in real time with automated guardrails and remediation to secure agent behavior.

Context Graph & Policy Engine

- Links scanner findings to model versions, datasets, code commits, and deployment metadata.
- Applies policies contextually—deciding promotion or rollback based on cumulative risk across the pipeline.

Automated Remediation

- Suggests risk-informed actions such as rollback, isolation, or retraining—powered by GenAI.
- Streamlines response with auto-generated playbooks tailored to the violation type and impact.

OpsMx

AI/ML Security with OpsMx

Secure AI models from prompt attacks and data leaks.

DATASHEET

KEY BENEFITS

Prevents Attacks Before They Escalate

Detects vulnerabilities and adversarial threats early—across notebooks, models, and ML pipelines.

Delivers Full-Lifecycle AI Security

Protects from data ingestion to runtime inference, ensuring continuous coverage.

Reduces Manual Security Overhead

Automates validation, risk scoring, and policy enforcement—freeing up AppSec and MLOps teams.

Improves Compliance & Audit Readiness

Enforces organizational and regulatory policies (e.g., HIPAA, GDPR) with traceable evidence.

Controls Shadow AI Risk

Prevents unauthorized models and usage patterns from bypassing controls or governance.

Accelerates Safe AI Deployment

Speeds up decision-making with contextual risk insights and go/no-go gates at every stage.

ABOUT US

OpsMx simplifies and accelerates comprehensive application security from developer to deployment building on AI-driven automation, open source security tools, and a deep understanding of the software delivery process. OpsMx enables tens of thousands of developers at both fast moving innovators and global enterprises to deliver more secure software faster.

FOR MORE INFORMATION, CONTACT US:

OPSMX, INC | 350 OAKMEAD PKWY, SUNNYVALE, CA 94085.

info@opsmx.com

www.opsmx.com