Pillar

AI SPM

Security Posture Management

What are the most critical security and privacy risks in our AI development and production environments—right now?

PROBLEM

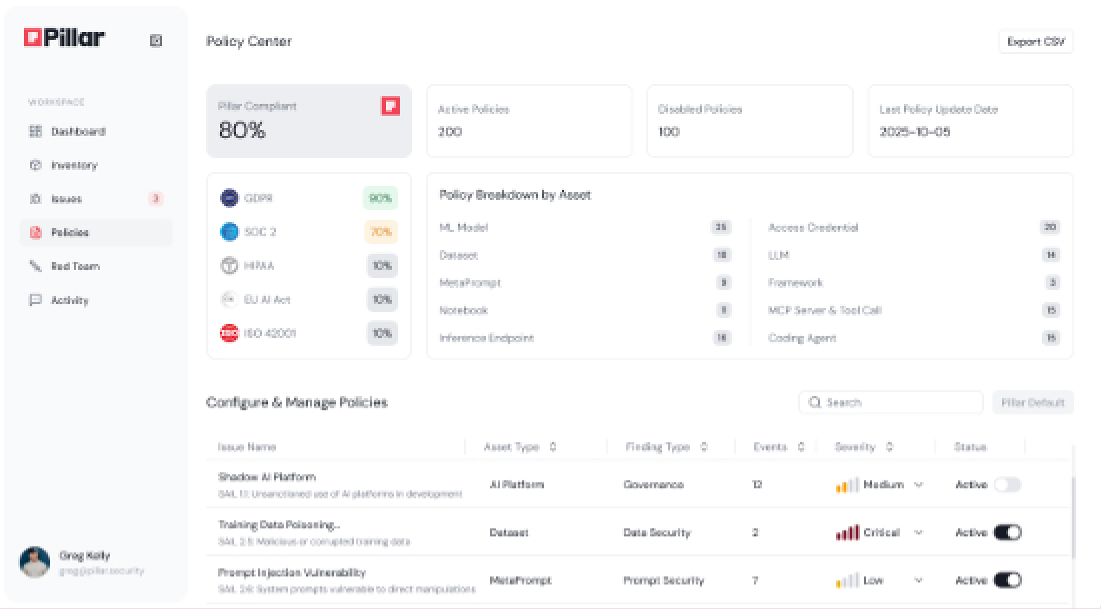
AI systems are exposed to evolving threats—ranging from prompt injection and supply chain attacks to model theft and data leakage. These risks can impact every stage of the AI lifecycle, from development and testing to live deployment.

SOLUTION

Pillar continuously scans for high-impact vulnerabilities and prioritizes risks across your entire AI stack. With dynamic threat modeling, AI fingerprinting, and real-time posture scoring, you get actionable insights on where your biggest exposures are—mapped directly to industry standards like OWASP LLM Top 10 and MITRE ATLAS. This lets you focus resources on what matters most, before attackers do.

> "What impressed us most about Pillar was their holistic approach to AI security."

eleos



Policy Center

Pillar Compliant	Active Policies	Disabled Policies	Last Policy Update Date
80%	200	100	2025-10-05

GDPR	90%
SOC 2	70%
HIPAA	10%
EU AI Act	10%
ISO 42001	10%

Policy Breakdown by Asset

ML Model	25	Access Credential	20
Dataset	18	LLM	14
MetaPrompt	9	Framework	3
Notebook	8	MCP Server & Tool Call	15
Inference Endpoint	18	Coding Agent	15

Configure & Manage Policies

Issue Name	Asset Type	Finding Type	Events	Severity	Status
Shadow AI Platform SAIL 1.1: Unsanctioned use of AI platforms in development	AI Platform	Governance	12	Medium	Active
Training Data Poisoning... SAIL 2.3: Malicious or corrupted training data	Dataset	Data Security	2	Critical	Active
Prompt Injection Vulnerability SAIL 2.6: System prompts vulnerable to direct manipulations	MetaPrompt	Prompt Security	7	Low	Active