



OVERSIGHT

Visibility & Inventory

Do we have complete, real-time visibility into all our AI models, agents, prompts, and datasets—across every cloud and platform?



PROBLEM

Modern organizations often have AI assets—including models, datasets, agents, and prompts—scattered across code bases, MLOps stacks, and shadow IT platforms. Without real-time discovery and inventory, hidden risks, compliance violations, and unapproved deployments can go undetected.



SOLUTION

Pillar provides automated, continuous discovery and full inventory of all AI assets, integrating directly with your code, data, and cloud platforms. This eliminates blind spots, enables compliance with frameworks like ISO 42001, and ensures you always know what's running, where, and who is responsible—empowering proactive risk management from day one.

The screenshot shows the Pillar AI Inventory dashboard. On the left is a sidebar with navigation links: Dashboard, Inventory (selected), Issues, Red Team, Activity, and Compliance. The main area has a top bar with 'AI Inventory' and a 'Discover AI Usage' button. Below this is a table of AI assets. The table has columns: Name, Provider, Creator, Type, Used by, Risk, and Severity. The table lists several assets including GPT-4, GPT-3.5, Stable Diffusion, Azure OpenAI GPT-4, Azure OpenAI Codex, Whisper, and Amazon Nova Micro. Each row shows the asset's name, provider (Open AI, Huggingface, Azure AI, Bedrock), creator (Open AI, Amazon), type (LLM, VLM, Classifier, ADR), and usage (e.g., 18 apps, 3 apps). Risk and severity are indicated by colored icons and bar charts.

Name	Provider	Creator	Type	Used by	Risk	Severity
GPT-4	Open AI	Open AI	LLM	18 apps	High	High
GPT-3.5	Open AI	Open AI	VLM	3 apps	Medium	High
Stable Diffusion	Huggingface	Open AI	Classifier	12 apps	Medium	High
Azure OpenAI GPT-4	Azure AI	Open AI	LLM	18 apps	High	High
Azure OpenAI Codex	Azure AI	Open AI	LLM	18 apps	High	High
Whisper	Open AI	Open AI	ADR	3 apps	Medium	Medium
Amazon Nova Micro	Bedrock	Amazon	LLM	12 apps	High	High

“For the first time, our security team sees every model, dataset, and prompt in a single dashboard—no more chasing blind spots.”

CISO,
GLOBAL E-COMMERCE