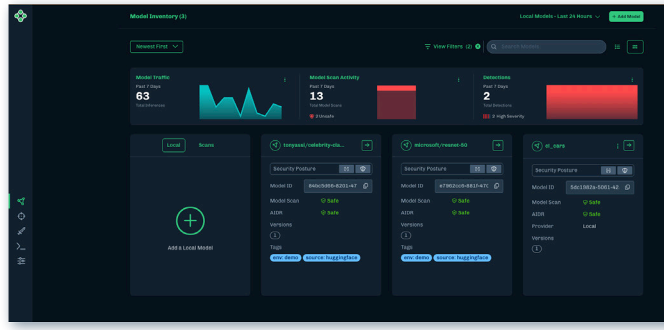
HIDDENLAYER AISEC PLATFORM

HiddenLayer's AISec Platform is a Protection Suite designed to secure AI models across the MLOps pipeline.

It proactively detects and mitigates risks from adversarial AI attacks, prompt injection, IP theft, PII leakage, and supply chain vulnerabilities — ensuring the integrity of your AI ecosystem without accessing private data or models.



AI Detection & Response

Automate and scale the protection of AI models, ensuring their security in real-time. With AIDR integrated into your environment, you can proactively defend against threats to AI unobtrusively.

Model Scanner

Scan AI models to identify hidden cybersecurity risks and threats such as malware, vulnerabilities, and integrity issues. Secure your entire AI lifecycle by protecting training, build, and production files.

Automated Red Teaming

Simulate expert attacks with zero lead time, delivering comprehensive reports to identify, prioritize, remediate, and document security risks—ensuring AI projects stay on track and compliant with security standards.

KEY PRODUCT CAPABILITIES

- **Model Genealogy & Integrity Protection** — Tracks model lineage from training through fine-tuning, identifying unauthorized changes, tampering, or corruption to ensure traceability and compliance
- **AI Bill of Materials (AIBOM)** — Automatically generates a detailed inventory of model components, datasets, and dependencies. Exportable in standard formats to support supply chain audits and licensing enforcement
- **Enhanced Threat Intelligence & Community Insights** — Combines data from public sources like Hugging Face, with expert analysis to surface actionable intelligence on emerging AI threats
- **Adversarial & Prompt Injection Defense** — Detects and mitigates adversarial attacks, model theft, and prompt injection using a blend of behavioral analysis, static inspection, and anomaly detection
- **Telemetry Dashboards & Red Teaming** — Offers advanced dashboards and simulated attack playbooks to visualize misuse patterns, agentic behaviors, and runtime anomalies
- **Security Framework Alignment** — Integrates with MITRE ATLAS and OWASP LLM, mapping over 64 tactics for unified governance and team collaboration

KEY BENEFTIS

- **Supply Chain Transparency** — AIBOM ensures full visibility into model components, enabling licensing checks and regulatory compliance
- **Real-Time Threat Detection** — Continuously scans for malware, model tampering, and CVEs across the AI pipeline, ensuring rapid response to threats
- **Protection Against IP Theft & Misuse** — Stops model extraction and unauthorized agentic behavior, safeguarding IP and backend access
- **Operational Visibility & Control** — Telemetry dashboards and white-glove policy enforcement improve incident response and governance
- **Faster, Safer AI Deployment** — Cuts deployment timelines while embedding security unobtrusively—so you can ship AI products confidently

AVAILABLE ON

Azure Marketplace | AWS Marketplace | Google Cloud Platform

Why HiddenLayer®?

HiddenLayer®, a Gartner recognized Cool Vendor for AI Security, creates security solutions that prevent the latest wave of cybersecurity threats against artificial intelligence assets. Using a patented approach, only HiddenLayer® offers turnkey AI security without requiring increased model complexity, access to sensitive training data, or visibility into the AI assets.

Gartner COOL VENDOR 2024

hiddenlayer.com