PROTECT YOUR GEN AI ASSETS WITH HIDDENLAYER AISEC PLATFORM

WHY NOW?

"AI could contribute up to **$15.7 trillion** to the global economy in **2030**." — pwc

"**President Biden issued an Executive Order** on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (EO 14110)"

"By **2026**, more than **80%** of independent software vendors will have embedded generative AI (GenAI) capabilities in their enterprise applications, up from less than 1% in 2023." — Gartner

ARTIFICIAL INTELLIGENCE ADVERSARIAL ATTACKS ARE EXPLODING

REAL WORLD ATTACKS

AI Models across all industries are being attacked. MITRE ATLAS has identified sixty-four unique AI model attack methods being used by adversaries today. A Zero Trust architecture requires protecting your AI models across your organization just like any other IT platform.

ACCELERATING REGULATIONS

Government & industry recognize the need to protect citizens, employees & all people interacting with AI. The White House has issued an AI BIll of Rights requiring secure models & will require disclosure of adversarial activity. Similarly, GDPR regulations are currently being updated to include AI protection.

WEAPONIZED AAI TOOLS

Over 20 free tools have been developed to make attacking AI easier than ever before. Attacks that took forty days in 2019, today take ten seconds. A security software platform is the only way to protect against such efficient attack tools. A model complexity or robustness approach is simply too costly & ineffective.

SCALABLE & REAL-TIME

CYBERSECURITY PRODUCT SUITE TO PROTECT ARTIFICIAL INTELLIGENCE MODELS IN EVERY STEP OF THE AIOPS PIPELINE

HIDDENLAYER MODEL SCANNER

Ensure model integrity

Guarantee validity of pretrained models

Identify malicious injection

HIDDENLAYER AI DETECTION & RESPONSE

Similar to EDR, but for AI Protection

Monitors inputs & outputs of your artificial intelligence algorithms for malicious activity

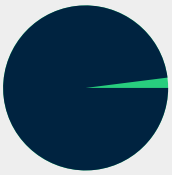
Enables you to respond to attacks

Doesn't require access to private data or models

For further details, access our **Model Scanner** & **AI Detection & Response** datasheets

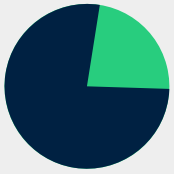
contact@hiddenlayer.com

hiddenlayer.com



98% of IT leaders consider at least some of their AI models crucial to their business success

On average, companies have a staggering **1,689** models in production



77% of companies reported identifying breaches to their AI in the past year. The remaining were uncertain whether their AI models had seen an attack

HiddenLayer commissioned a survey of 150 security and data science leaders to reveal the current state of securing AI.

PROFESSIONAL SERVICES

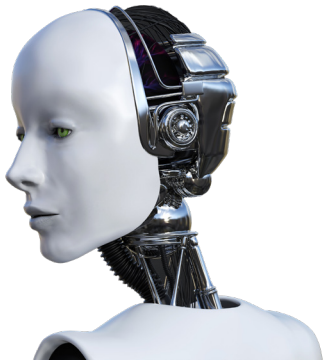
PROTECT YOUR ADVANTAGE

HiddenLayer's professional services leverage deep domain expertise in cybersecurity, artificial intelligence, reverse engineering, and threat research.

LEARN MORE →

BOLSTERING AI SECURITY TO INCREASE AI ADOPTION

Traditional security solutions are not designed to address adversarial AI attack vectors. Protecting the models we build & trust requires a **AI native approach**.



LEARN MORE →

HiddenLayer, a Gartner recognized AI Application Security company, is a provider of security solutions for artificial intelligence algorithms, models & the data that power them. With a first-of-its-kind, noninvasive software approach to observing & securing AI, HiddenLayer is helping to protect the world's most valuable technologies.