



VINDICARA

AI Runtime Security Platform

Guardrails, agent IAM, drift detection, and compliance automation for any team deploying AI in production.

```
from vindicara import Client

client = Client(api_key="vnd_...")

result = client.guard(
    input="User prompt here",
    policies=["pii", "toxicity"]
)

# Runtime protection in <5 min
```

THE PROBLEM

AI is shipping to production faster than security can keep up.



Prompt Injection

Attackers manipulate AI inputs to bypass controls, extract data, or hijack agent behavior.



Data Exfiltration

LLMs leak PII, credentials, and proprietary data through unguarded outputs.



Behavioral Drift

Models change behavior silently after updates, creating compliance gaps nobody detects.



Regulatory Pressure

EU AI Act deadlines approaching.
NIST AI RMF mandates growing.
Most teams have zero tooling.

Only 8% of MCP servers have proper OAuth | 77% of enterprises report AI security incidents | EU AI Act enforcement begins Aug 2026

WHY NOW

Three forces are converging to create a once-in-a-decade market window.

01

Competitors Acquired

CalypsoAI acquired by F5.
Lakera acquired by Check Point.
No independent, developer-first
solution remains.

02

Regulation Is Here

EU AI Act enforcement begins
August 2026. NIST AI RMF
mandates are growing.
Teams need tooling now.

03

Agent Explosion

92% of enterprises deploying AI
by 2026. MCP adoption is surging.
Every agent needs runtime
security.

The window is open. Vindicara is built to fill it.

FIVE PILLARS

One platform. Complete AI runtime security.



Core SDK

Input/output guards,
policy engine, real-time
interception



MCP Scanner

Evaluate MCP server
configs for auth gaps
and attack vectors



Agent IAM

Per-agent permissions,
scoped access, Zero
Trust enforcement



Drift Detection

Behavioral baselines,
anomaly alerts,
continuous monitoring



Compliance

EU AI Act, NIST RMF,
automated evidence
generation

Unified policy layer across all five pillars

HOW IT WORKS

`pip install vindicara`. Runtime protection in under 5 minutes.

01

INSTALL SDK

One pip install. Import the client.
Configure your API key. That's it.

02

DEFINE POLICIES

Pick from built-in policies (PII, toxicity, prompt injection) or write custom rules.

03

INTERCEPT & ENFORCE

Every AI call passes through Vindicara.
Bad inputs blocked. Bad outputs caught.

USER PROMPT



VINDICARA GUARD



AI MODEL



VINDICARA GUARD



SAFE RESPONSE

MARKET OPPORTUNITY

\$109.9B

AI Security TAM
by 2034

92%

Of enterprises
deploying AI by 2026

3

Major competitors
acquired in 18 months

COMPETITIVE LANDSCAPE

	Self-Serve	Open Core	Independent	5 Pillars
Guardrails AI \$7.5M raised	✗	✓	✓	✗
Lakera Acq. Check Point	✗	✗	✗	✗
CalypsoAI Acq. F5	✗	✗	✗	✗
Vindicara	✓	✓	✓	✓

BUSINESS MODEL

Self-serve SaaS. Developer-first pricing that scales with usage.

OPEN SOURCE

Free

- ✓ Core SDK
- ✓ Local policy engine
- ✓ Community support

DEVELOPER

\$49/mo

- ✓ Cloud dashboard
- ✓ MCP scanner (5)
- ✓ Email support

TEAM

\$149/mo

- ✓ Agent IAM
- ✓ Drift baselines
- ✓ 25 MCP servers

SCALE

\$499/mo

- ✓ Compliance engine
- ✓ Custom policies
- ✓ Priority support

ENTERPRISE: Custom pricing | On-prem/VPC | SSO/SAML | Dedicated CSM | SLA

TRACTION & ROADMAP

BUILT & LIVE

- ✓ All 5 security pillars production-tested on AWS
- ✓ Core SDK shipped (pip install vindicara v0.1.0)
- ✓ Published on PyPI with open-source tier
- ✓ Policy engine with real-time enforcement
- ✓ FastAPI backend on AWS Lambda (production)
- ✓ Live API with demo key at vindicara.io
- ✓ MCP Security Scanner operational
- ✓ Developer dashboard spec finalized

ROADMAP

Q2 2026

Developer dashboard launch
Agent IAM + Drift Detection live

Q3 2026

Compliance engine (EU AI Act)
First paid customers

Q4 2026

Hacker News / Product Hunt launch
500 GitHub stars target

Q1 2027

Enterprise tier + SOC 2
Series A positioning

TEAM

KEVIN MINN

Founder & CEO

Solo technical founder. Built 7 AI products from scratch across Next.js, React Native, Swift, AWS.

B.S. Cybersecurity (SNHU, 4.0 GPA). Direct domain expertise in what Vindicara protects.

Burmese-born, LA-based. Immigrant founder with global perspective.

Runs SLTR Digital LLC. Multi-product studio with live products in production.

WHY THIS FOUNDER

Builder, Not a Pitch Artist

Every product shipped from zero to production, solo. Vindicara's SDK is live, not a mockup.

Security-First Mindset

Cybersecurity education is the foundation of every architectural decision.

Daily AI Power User

Builds with Claude Code, Bedrock, Gemini daily. Vindicara was born from real pain.

Capital Efficient

Seven products built on AWS credits and sweat equity. \$500K goes further here.

Early signals: live SDK on PyPI, five pillars in production, EU AI Act timing

GO-TO-MARKET

Developer-first. Product-led growth. Land and expand.

PHASE 1: LAND

Now - Q3 2026

Open-source SDK on PyPI + GitHub
Developer content (blog, tutorials,
MCP security reports)
Reddit, Hacker News, dev Twitter
Free tier captures devs at point of need

PHASE 2: CONVERT

Q3 - Q4 2026

Usage-based upgrade triggers
Team features (dashboard, shared
policies)
MCP scanner as freemium acquisition
Target: 100 paid developers by Q4

PHASE 3: EXPAND

2027+

Enterprise tier with compliance engine
SOC 2 certification for enterprise trust
Channel partnerships with AWS
Land-and-expand within engineering
orgs

YOUR NEXT MOVE

\$500K

Post-Money SAFE | \$5M Cap

50%	Engineering	Complete pillars 4 & 5, harden SDK
25%	Go-to-Market	Content, community, developer relations
15%	Infrastructure	AWS, security certifications, SOC 2
10%	Operations	Legal, compliance, admin



VINDICARA

*The security layer AI
has been missing.*

Kevin Minn, Founder & CEO

Kevin.minn@vindicara.io

vindicara.io

Los Angeles, CA