AgentGuard

AI Security Governance Platform

Comprehensive control mapping, threat modeling, and policy enforcement for enterprise agentic AI systems

Series A Investment Opportunity • January 2026

The Problem

Agentic AI is an unguarded frontier.

Enterprises deploy AI agents that browse, execute code, and make autonomous decisions—with minimal security.

77%

of enterprises lack AI security controls

$4.2M

average cost of AI-related breach

0

vendors with NIST AI RMF crosswalk

The Solution

A unified platform for AI security governance, compliance, and observability.

Control Mapping

First complete NIST AI RMF → 800-53 crosswalk. Automated gap analysis and remediation roadmaps.

Observability

Extended OpenTelemetry for agent traces. LLM, retrieval, and tool spans with security signals.

Policy Engine

OPA-powered enforcement. Tool access, data flow, HITL gates, capability bounds. Sub-ms evaluation.

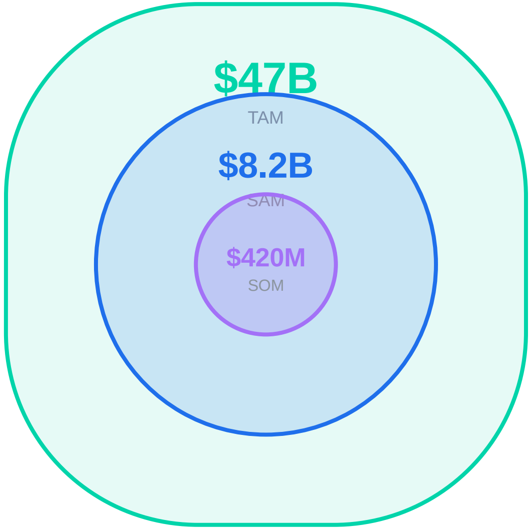
Threat Modeling

MITRE ATLAS integration. Agent-specific STRIDE analysis with trust boundary detection.

Maturity Assessment

Continuous AI security posture scoring. Benchmark against industry peers with actionable roadmaps.

Market Opportunity



TOTAL ADDRESSABLE MARKET

Global AI security + GRC software. MLSecOps, governance, compliance.

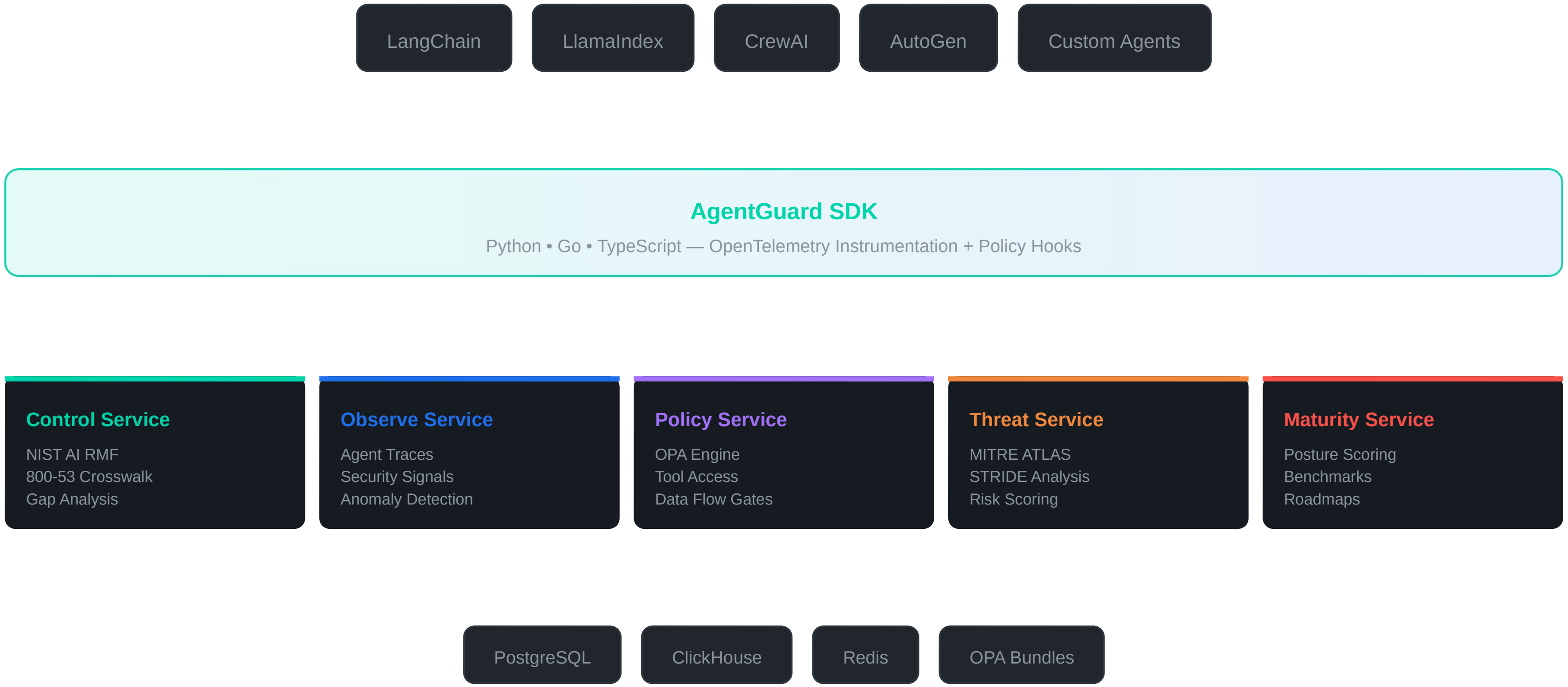
SERVICEABLE ADDRESSABLE MARKET

Enterprise AI security for regulated industries. Finance, healthcare, government.

SERVICEABLE OBTAINABLE MARKET

FedRAMP enterprises with agentic AI. Year 3 target: 150 customers.

Platform Architecture



LangChain

LlamaIndex

CrewAI

AutoGen

Custom Agents

AgentGuard SDK

Python • Go • TypeScript — OpenTelemetry Instrumentation + Policy Hooks

Control Service

NIST AI RMF
800-53 Crosswalk
Gap Analysis

Observe Service

Agent Traces
Security Signals
Anomaly Detection

Policy Service

OPA Engine
Tool Access
Data Flow Gates

Threat Service

MITRE ATLAS
STRIDE Analysis
Risk Scoring

Maturity Service

Posture Scoring
Benchmarks
Roadmaps

PostgreSQL

ClickHouse

Redis

OPA Bundles

Competitive Advantage

Capability	Lakera	LangSmith	Arize	AgentGuard
NIST AI RMF → 800-53 Crosswalk				
Tool Access Control Policies				
Data Flow Governance				
Human-in-the-Loop Gates				
Agent-Specific Threat Modeling				
LLM Observability				
Content Safety / Prompt Injection				

First-Mover

Only complete NIST AI RMF compliance crosswalk on the market

Agent-Native

Built for agentic AI, not retrofitted from LLM guardrails

Unified Platform

Single pane of glass: governance, observability, enforcement

Business Model

STARTER

$2,500/mo

Up to 10 agents

- ✓ Control mapping
- ✓ Basic observability
- ✓ Policy enforcement

Standard support only

POPULAR

PROFESSIONAL

$8,000/mo

Up to 50 agents

- ✓ Everything in Starter
- ✓ Threat modeling
- ✓ HITL workflows
- ✓ SSO / SCIM

ENTERPRISE

$25K+/mo

Unlimited agents

- ✓ Everything in Pro
- ✓ FedRAMP package
- ✓ Custom integrations
- ✓ Dedicated CSM

FEDRAMP HIGH

$50K+/mo

Gov cloud deployment

- ✓ Everything in Enterprise
- ✓ IL4/IL5 compliant
- ✓ SLED support
- ✓ 3PAO audit support

$85K	18 mo	130%	<5%
Target ACV	Target payback	Target NRR	Target churn

Roadmap

PHASE 1

Foundation

Q1-Q2 2026

- Core platform MVP
- NIST AI RMF crosswalk
- Python SDK
- 5 design partners

$500K ARR

PHASE 2

Scale

Q3-Q4 2026

- Policy engine GA
- Threat modeling
- SOC 2 Type II
- 25 customers

$2.5M ARR

PHASE 3

Expand

2027

- FedRAMP Moderate
- ISO 42001 mapping
- GRC integrations
- 75 customers

$8M ARR

PHASE 4

Dominate

2028

- FedRAMP High
- EU AI Act support
- Partner ecosystem
- 150 customers

$20M ARR

● Q2 26: Series A ● Q4 26: SOC 2 ● Q2 27: FedRAMP ● Q4 28: Series B

The Ask

SERIES A RAISE

$12M

Seeking lead from:

Security-focused VCs with enterprise GTM expertise and FedRAMP portfolio experience

USE OF FUNDS