The AI Security Category Launch Map
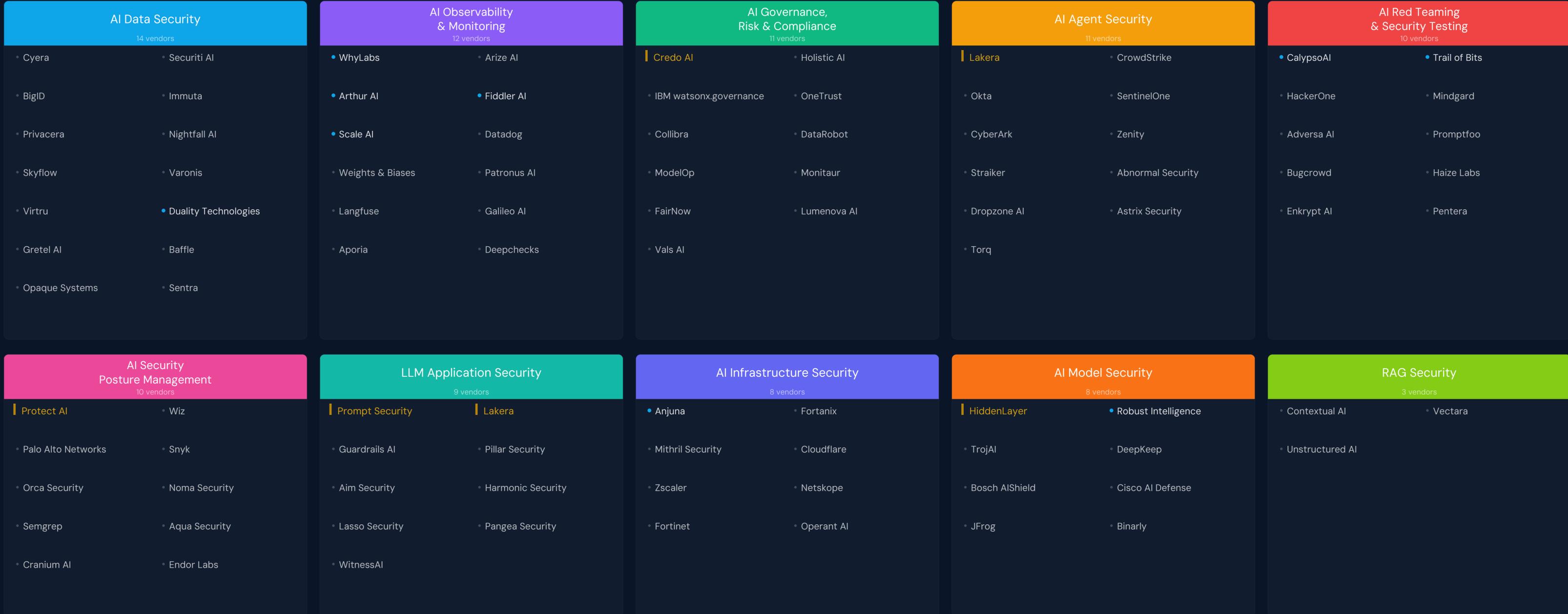
96 Vendors · 10 Categories · The Definitive AI Security Landscape

March 2026 Edition

AI Data Security
14 vendors

• Cyera	• Securiti AI
• BigID	• Immuta
• Privacera	• Nightfall AI
• Skyflow	• Varonis
• Virtru	• Duality Technologies
• Gretel AI	• Baffle
• Opaque Systems	• Sentra

AI Observability & Monitoring
12 vendors

• WhyLabs	• Arize AI
• Arthur AI	• Fiddler AI
• Scale AI	• Datadog
• Weights & Biases	• Patronus AI
• Langfuse	• Galileo AI
• Aporia	• Deepchecks

AI Governance, Risk & Compliance
11 vendors

Credo AI	• Holistic AI
• IBM watsonx.governance	• OneTrust
• Collibra	• DataRobot
• ModelOp	• Monitaur
• FairNow	• Lumenova AI
• Vals AI	

AI Agent Security
11 vendors

Lakera	• CrowdStrike
• Okta	• SentinelOne
• CyberArk	• Zenity
• Straiker	• Abnormal Security
• Dropzone AI	• Astrix Security
• Torq	

AI Red Teaming & Security Testing
10 vendors

• CalypsoAI	• Trail of Bits
• HackerOne	• Mindgard
• Adversa AI	• Promptfoo
• Bugcrowd	• Haize Labs
• Enkrypt AI	• Pentera

AI Security Posture Management
10 vendors

Protect AI	• Wiz
• Palo Alto Networks	• Snyk
• Orca Security	• Noma Security
• Semgrep	• Aqua Security
• Cranium AI	• Endor Labs

LLM Application Security
9 vendors

Prompt Security	Lakera
• Guardrails AI	• Pillar Security
• Aim Security	• Harmonic Security
• Lasso Security	• Pangea Security
• WitnessAI	

AI Infrastructure Security
8 vendors

• Anjuna	• Fortanix
• Mithril Security	• Cloudflare
• Zscaler	• Netskope
• Fortinet	• Operant AI

AI Model Security
8 vendors

HiddenLayer	• Robust Intelligence
• TrojAI	• DeepKeep
• Bosch AIShield	• Cisco AI Defense
• JFrog	• Binarly

RAG Security
3 vendors

• Contextual AI	• Vectara
• Unstructured AI	

Legend

Core Five	— AI-native security leaders defining the category
• Important Ten	— Critical infrastructure and emerging platform players
• Tracked Vendor	— Part of the 200+ company AI Security Intelligence database

200+
Companies Tracked

10
Market Categories

$8.5B+
Combined Funding

Real-Time
Signal Tracking