

The AI Safety, Security & Governance Landscape 2026

194

COMPANIES MAPPED

9

SUB-SECTORS

\$6bn

TOTAL CAPITAL RAISED*

~\$6bn

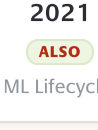
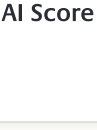
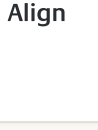
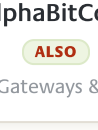
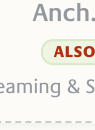
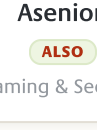
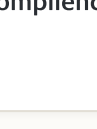
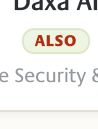
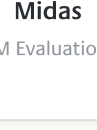
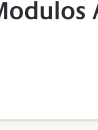
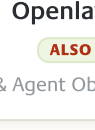
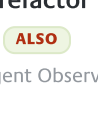
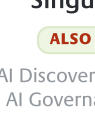
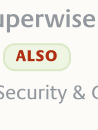
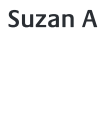
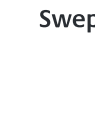
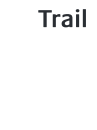
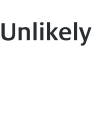
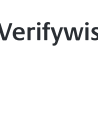
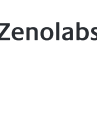
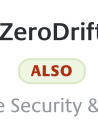
OF IT, VENTURE FUNDING

54%

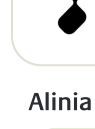
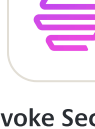
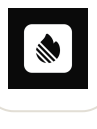
US-HEADQUARTERED

Almost all of the **\$5.6bn** raised here is venture equity, with **63% of companies still at Seed or Series A** on a median round of just \$9m. Governance, risk and compliance is still the largest single bucket at **55 companies**, but it no longer accounts for a third of the field: runtime security, red teaming and shadow AI discovery are pulling away from it, in several cases at the vendors' own insistence. This is the earliest and most fragmented layer of the stack, yet already consolidating fast: **26 of the companies mapped here have been acquired**.

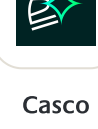
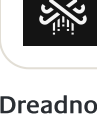
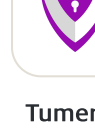
AI Governance, Risk & Compliance (GRC) 55

 2021 ALSO MLOps & ML Lifecycle Platforms	 AI Score	 Align	 AlphaBitCore ALSO Model Gateways & Routing	 Anch.ai ALSO AI Red Teaming & Security Testing	 Asenion ALSO AI Red Teaming & Security Testing	 Bast	 Calvin Risk
 Coalex.ai	 Compliance	 Credo AI	 Daxa AI ALSO AI Runtime Security & Guardrails	 Enzai	 Essert	 Fairly ALSO AI Red Teaming & Security Testing	 Fairnow
 Fairplay	 Geordie	 Holistic AI ALSO Shadow AI Discovery & Workforce AI Governance	 Howso	 Iridius	 Komply	 Konfer	 Latticeflow
 Lumenova ALSO AI Runtime Security & Guardrails	 Midas ALSO LLM Evaluation & Testing	 ModelOp	 Modulos AG	 Monitaur	 Naaila	 Onetrust	 Openlayer ALSO LLM & Agent Observability
 Polygraf ALSO AI Runtime Security & Guardrails	 Prediction Guard	 Prefactor ALSO LLM & Agent Observability	 Produktiv	 Recordpoint	 Saidot	 Seekr	 Singular ALSO Shadow AI Discovery & Workforce AI Governance
 SolasAI	 Spix ALSO AI Red Teaming & Security Testing	 Supervise ALSO AI Runtime Security & Guardrails	 Suzan AI	 Swept	 Trail	 Trustible	 Trustwise ALSO AI Security Posture & Threat Detection
 Unlikely AI	 ValidMind ALSO Agent Identity & Access Control	 Velatir ALSO Shadow AI Discovery & Workforce AI Governance	 Verifywise	 Yields	 Zenolabs AI	 ZeroDrift ALSO AI Runtime Security & Guardrails	

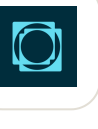
AI Runtime Security & Guardrails 37

 AetherLab ALSO AI Red Teaming & Security Testing	 AI Shield ALSO AI Red Teaming & Security Testing	 Alceberg	 Alert AI	 Alinia AI ALSO AI Governance, Risk & Compliance (GRC)	 Backlash Security	 CalyptoAI	 Capsule Security
 Cinder	 Ciphro	 Cleanlab	 CTGT	 DeepKeep ALSO AI Red Teaming & Security Testing	 Dynamo ALSO AI Governance, Risk & Compliance (GRC)	 Eve Security ALSO Shadow AI Discovery & Workforce AI Governance	 Evoke Security
 Gray Swan ALSO AI Red Teaming & Security Testing	 Guardrails	 Helmet Security	 HiveTrace	 Invariant Labs ALSO AI Red Teaming & Security Testing	 Jozu ALSO Shadow AI Discovery & Workforce AI Governance	 Lakera	 Mira
 Neo Security ALSO AI Security Posture & Threat Detection	 NOFire AI	 Pangea Cloud ALSO Agent Identity & Access Control	 Pinta AI ALSO AI Security Posture & Threat Detection	 Qualifire ALSO LLM Evaluation & Testing	 Quilr	 Silmaril	 Tenet Security ALSO AI Security Posture & Threat Detection
 Trojai	 Trussed AI ALSO AI Governance, Risk & Compliance (GRC)	 VeriSigil AI ALSO Agent Identity & Access Control	 Virtue AI ALSO AI Red Teaming & Security Testing	 ZenGuard AI			

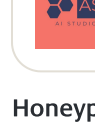
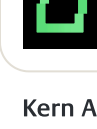
AI Red Teaming & Security Testing 23

 Adversa AI	 Airside Labs	 Alice ALSO AI Runtime Security & Guardrails	 Casco	 Cybret	 Dreadnode	 Giskard ALSO AI Runtime Security & Guardrails	 HackerOne
 Haize Labs	 Harmony Intelligence	 Irregular	 Legit Security	 Mindgard ALSO AI Security Posture & Threat Detection	 Preamble	 Promptfoo ALSO AI Runtime Security & Guardrails	 Repello ALSO AI Security Posture & Threat Detection
 Revalor ALSO Synthetic Data Generation	 Robust Intelligence ALSO AI Runtime Security & Guardrails	 Safe Intelligence	 Trent AI	 Turneryk ALSO AI Runtime Security & Guardrails	 Verno Labs ALSO AI Runtime Security & Guardrails	 White Circle ALSO LLM & Agent Observability	

Shadow AI Discovery & Workforce AI Governance 20

 AIM Security ALSO AI Runtime Security & Guardrails	 Aurascape ALSO AI Runtime Security & Guardrails	 Etiquette	 Harmonic Security	 Knostic ALSO Agent Identity & Access Control	 Lanai	 Lumia Security ALSO AI Runtime Security & Guardrails	 NROC Security
 Onyx Security ALSO AI Runtime Security & Guardrails	 Prompt ALSO AI Runtime Security & Guardrails	 Rencore	 SurePath	 SurePath	 Swift Security ALSO AI Data Privacy & Confidential Computing	 Unseen Security ALSO AI Runtime Security & Guardrails	 Vallum
 Verax AI ALSO AI Runtime Security & Guardrails	 Wald	 Willow ALSO Agent Identity & Access Control	 WitnessAI ALSO AI Runtime Security & Guardrails				

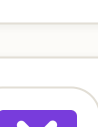
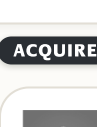
AI Data Privacy & Confidential Computing 18

 Almure	 Antimatter	 Bitfount ALSO Enterprise ML & Data Science Platforms	 ConfidentialMind ALSO LLM & Model Inference Serving	 Honeypotz	 Kern AI ALSO Enterprise AI Platforms & Operating Systems	 Mirror Security ALSO AI Red Teaming & Security Testing	 Mithril Security
 Nenna AI	 Opaque	 Prem	 Redactive	 Securiti ALSO AI Governance, Risk & Compliance (GRC)	 Sherpa.ai ALSO Enterprise ML & Data Science Platforms	 skyflow	 Telescope
 Tinfoil	 Wodan AI						

Agent Identity & Access Control 17

 Astrasync ALSO AI Governance, Risk & Compliance (GRC)	 Billions	 Clawvisor ALSO AI Runtime Security & Guardrails	 ConductorOne	 Credal ALSO Agent Tool Integration & MCP Gateways	 Cyata	 Cyata	 GitGuardian
 Hush Security	 Javelin	 Keycard	 LangGuard ALSO AI Runtime Security & Guardrails	 Nava Labs	 Riptides	 Saviynt	 Synergetics
 Token Security							

AI Security Posture & Threat Detection 16

 Acuvity	 AllTrue ALSO Shadow AI Discovery & Workforce AI Governance	 Blindsight	 Craniun ALSO AI Governance, Risk & Compliance (GRC)	 General Analysis ALSO AI Red Teaming & Security Testing	 Hardshell	 Hiddenlayer ALSO AI Red Teaming & Security Testing	 Lasso Security ALSO AI Governance, Risk & Compliance (GRC)
 Neuraltrust ALSO AI Red Teaming & Security Testing	 Noma Security ALSO Agent Identity & Access Control	 Ovalix ALSO Shadow AI Discovery & Workforce AI Governance	 Pillar Security ALSO AI Red Teaming & Security Testing	 Prompt Armor	 ProtectAI ALSO AI Red Teaming & Security Testing	 Starsteer	 Superalign ALSO Shadow AI Discovery & Workforce AI Governance

Deepfake & Content Authenticity Detection 5

 Aurigin	 Identifai	 Label4	 Reality Defender	 Resemble
---	--	---	---	---

Hyperscaler / SaaS Giant 3

 Amazon Web Services	 Google	 Microsoft
---	---	--

*Funding from Crunchbase, 155 of 194 companies matched. "Total capital raised" includes all funding types (venture, debt, post-IPO, grants); "venture funding" excludes debt, private equity, post-IPO and grant rounds. Companies may appear in more than one sub-sector. Logos via logo.dev.