NUCLEAUS

Total Addressable Market Analysis

AI Safety & Security - (NUCL-C2S02M005)

Technologies that protect AI systems from adversarial attacks, ensure model safety and alignment, govern responsible deployment, and prevent misuse.

$31B

TAM (2025)
AI in Cybersecurity

$3.5B

SAM (2025)
AI TRiSM + Governance

$800M

SOM (2025)
Pure-Play Vendors

28-36%

CAGR
2025–2030

Table of Contents

AI Safety & Security - Total Addressable Market Analysis (NUCL-C2S02M005)

MARKET DEFINITION

01 Market Definition & Scope

02 Top-Down Approach

03 Bottom-Up Approach

04 TAM / SAM / SOM

SIZING & PROJECTIONS

05 5-Year Growth Projections

06 Analyst Report Comparison

MARKET INTELLIGENCE

07 Key Buyers & Geography

08 Vendor Landscape

METHODOLOGY & SOURCES

09 Key Assumptions & Methodology

Delivering

- 10-slide presentation deck
- TAM/SAM/SOM with 5 analyst cross-references
- All market statistics independently sourced and cited



Market Intelligence

Market Definition & Scope

What we mean by "AI Safety & Security"

Technologies, tools, and frameworks that protect AI systems from adversarial attacks, ensure model safety and alignment, govern responsible deployment, and prevent misuse.

AI Runtime Security	Guardrails, prompt injection defense, model shielding, adversarial attack detection	*HiddenLayer, Protect AI, Aim Security, Lakera, Pangea* (5 of 14)
AI Governance & Compliance	Policy enforcement, bias auditing, regulatory compliance (EU AI Act), model risk mgmt	*Credo AI, Holistic AI, Saidot.ai, Monitaur, Giskard* (5 of 12)
AI Model Safety & Alignment	Red-teaming, alignment research, safety evaluation, adversarial testing	*Gray Swan, FAR.AI, Redwood Research, CAIS, Mindgard* (5 of 8)
AI Content Authenticity	Deepfake detection, AI-generated content identification, provenance tracking	*Zama, Reality Defender, Apheris* (3 of 3)

Top-Down Approach

Global Market → Segment Narrowing

Global Cybersecurity Spend — $454B

2025 estimate

AI in Cybersecurity (TAM) — $31B

2025 analyst estimate

AI TRiSM + AI Governance (SAM) — $3.5B

2025 analyst estimate

Pure-Play Vendors (SOM) — $800M

Bottom-up estimate (see next slide)

Key Assumptions

AI = ~7% of total cybersecurity spend in 2025, accelerating to 15%+ by 2030 | AI TRiSM/Governance = ~11% of AI cybersecurity
SOM = revenue of 37 specialized vendors

Bottom-Up Approach

Unit Economics × Addressable Customer Base

Segment	Count	ACV	Revenue
Global 2000 Enterprises	2,000	$150K	$300M
Mid-Market (1K–10K emp.)	50,000	$35K	$1,750M
AI/ML Teams & Startups	25,000	$12K	$300M
Government & Defense	500	$250K	$125M
AI Model Providers	200	$500K	$100M
TOTAL BOTTOM-UP TAM			**$2.58B**

Note: ACV = Annual Contract Value.

Unit Economics Assumptions

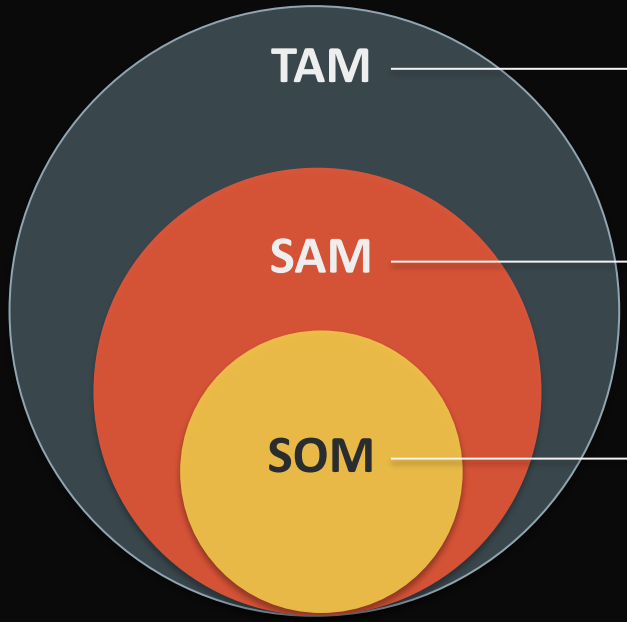
- **Enterprise ACV $100K–$500K**
  Based on disclosed pricing from Lakera, Protect AI, Calypso AI, Credo AI
- **Mid-market ACV $25K–$50K**
  Via self-serve and team tiers
- **AI model providers pay premium**
  For custom red-teaming & safety evaluation

Reconciliation

Top-Down SAM: $3.5B | Bottom-Up: $2.58B
Delta = services, consulting, and adjacent GRC tools

TAM / SAM / SOM

AI Safety & Security - Market Sizing (2025 → 2030)



Total Addressable Market

$31B → $86B 22.8% CAGR

All AI-powered cybersecurity solutions globally - includes AI-enhanced legacy security (SIEM, EDR, NDR), AI-native threat detection, and AI safety tools.

Serviceable Addressable Market

$3.5B → $12B 28% CAGR

Purpose-built AI TRiSM and AI Governance solutions - runtime guardrails, model monitoring, AI compliance, bias detection.

Serviceable Obtainable Market

$800M → $3.2B 32% CAGR

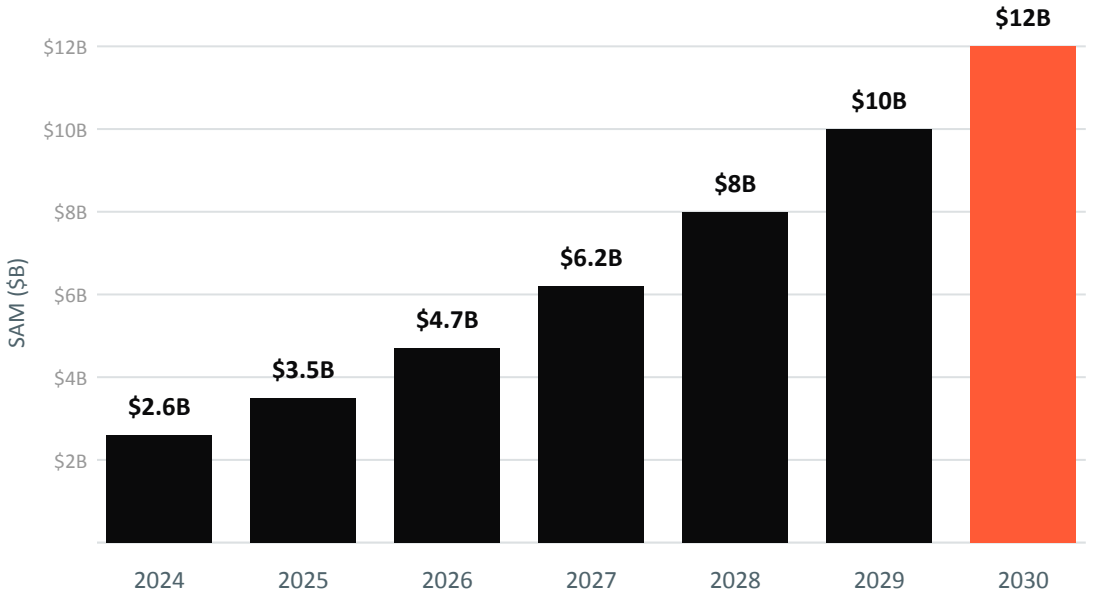
Revenue captured by pure-play AI safety startups and specialized vendors (37 companies). Higher growth driven by greenfield opportunity.



Sizing & Projections

5-Year Growth Projections

SAM Forecast: AI Safety & Security (AI TRiSM + Governance)



Note: Blended CAGR of 28% (AI TRiSM 21.6% + AI Governance 36%, weighted by market size).

Growth Drivers

- **EU AI Act Enforcement**
  Transparency rules live Aug 2026; high-risk duties deferred to Dec 2027 (Omnibus)
- **Agentic AI Explosion**
  Autonomous AI agents need runtime guardrails and monitoring
- **Enterprise AI at Scale**
  78% of orgs now deploy AI; safety follows
- **Regulatory Momentum**
  US executive orders, SEC AI disclosure, NIST AI RMF
- **M&A Consolidation**
  8 deals in 2025 (~$2.0B+); 2026 wave: Cisco, CrowdStrike, Okta, SailPoint, A10

Analyst Report Comparison

Cross-referencing 5 major research firms

Research Firm	Market Defined	2024/2025 Size	2030 Forecast	CAGR
Analyst 1	AI TRiSM	$2.3B (2024)	$7.4B	21.6%
Analyst 2	AI Governance	$890M (2024)	$5.8B (2029)	45.3%
Analyst 3	AI Cybersecurity Solutions	$30.9B (2025)	$86.3B	22.8%
Analyst 4	AI in Cybersecurity	$34.1B (2025)	$234.6B (2032)	31.7%
Analyst 5	AI Governance	$750M (2024)	$5.6B	40.0%

Key Takeaway

Analysts converge on a broad AI cybersecurity market of $31-34B in 2025 at 22-32% CAGR. The narrower AI TRiSM/Governance segment ranges from $2.3-3.5B, growing at 21-45% CAGR. Our blended SAM of $3.5B at 28% CAGR represents the consensus midpoint.

Market Definition

Key Buyers & Geography

Top Buyer Personas

35% CISO / VP Security

Primary budget holder. AI-specific threats and board-level risk reporting.

25% Chief AI Officer / VP ML

Owns AI governance & model safety. 25% of Fortune 500 now have a CAIO.

20% GRC / Compliance Lead

EU AI Act, NIST AI RMF, sector mandates. Needs audit trails.

12% VP Engineering / Platform

Guardrails for LLM pipelines. Developer experience and API integration.

8% CDO / Data Privacy Officer

AI data governance, PII leakage through LLMs, cross-border compliance.

Top Geographies

North America 32–36%

$1.1–1.3B (2025)

US leads. NIST AI RMF drives compliance.

Europe 28–30%

$1.0–1.1B (2025)

EU AI Act is #1 global regulatory catalyst.

Asia-Pacific 22–25%

$0.8–0.9B (2025)

Fastest growing. Japan, Australia, Singapore.

Rest of World 10–15%

$0.3–0.5B (2025)

UAE, Saudi, Israel, Brazil.

Top Verticals: Financial Services (28%), Tech (22%), Healthcare (15%), Gov/Defense (14%), Manufacturing (8%)

Vendor Landscape

37+ pure-play vendors across four sub-segments - (NUCL-C2S02M005)

AI Runtime Security	HiddenLayer, Protect AI, Aim Security, Lakera, Prompt Security, Pangea, CalypsoAI, SPLX, PromptArmor, GuardrailsAI, Credal, Kindo, WitnessAI, Nvidia NeMo Guardrails
AI Governance & Compliance	Credo AI, Holistic AI, Saidot.ai, Trustible, Konfer, Lumenova, Monitaur, Quantpi, Giskard, Enzai, Insightcircle, Fairly (Asenion)
AI Model Safety & Alignment	Gray Swan, FAR.AI, Redwood Research, CAIS, Preamble, Mindgard, TrojAI (A10), Veris AI
AI Content Auth. & Privacy	Reality Defender, Apheris, Zama

Notable M&A (2025, ~$2.0B+): PANW → Protect AI ($650-700M) | CrowdStrike → Pangea (~$260M) | Check Point → Lakera (~$300M) | SentinelOne → Prompt Sec. (~$180M) | Cato → Aim Sec. ($350M) | F5 → CalypsoAI ($180M) | Zscaler → SPLX | Fairly+Anch.AI → Asenion

Assumptions & Methodology

Key Assumptions & Methodology

Assumptions

- Enterprise AI adoption reaches 87% in large enterprises by 2025
- 10-15% of AI-deploying enterprises purchase dedicated AI safety tooling in 2025, growing to 40%+ by 2030
- EU AI Act drives 30%+ of European enterprise AI governance adoption by 2028 (post-Omnibus)
- Agentic AI adoption (33% of enterprise software by 2028) creates net-new demand for runtime security
- Market consolidation accelerates post-2026 (substantial GenAI TRiSM vendor consolidation expected)
- Average pure-play vendor ARR of $5-20M in 2025, with leaders at $30-50M

Methodology

Top-Down

Global cybersecurity spend ($454B) → AI penetration (7%) → AI safety sub-segment (11%)

Bottom-Up

Customer segments × ACV × penetration rate. Cross-referenced with vendor revenues and funding.

Triangulation

Compared 5 analyst estimates against a common framework definition.

SAM Validation

Bottom-up ($2.58B) falls within top-down SAM range ($2.3-3.5B), confirming consistency.

For questions or deep-dives on specific sub-segments, contact the Nucleaus team.