NUGUARD AI

AI TRUST PLATFORM

Close the behavior gap in AI Applications

Ranjan Goel

Founder / CEO

ranjangoel@nuguard.ai

Behavior Gap - Why we care



AI employee

Intended Behavior

- Always friendly and helpful
- Only discusses Insurance related topics
- Follows specific guidance to involve humans
- Always safe & secure interactions

Real Behavior

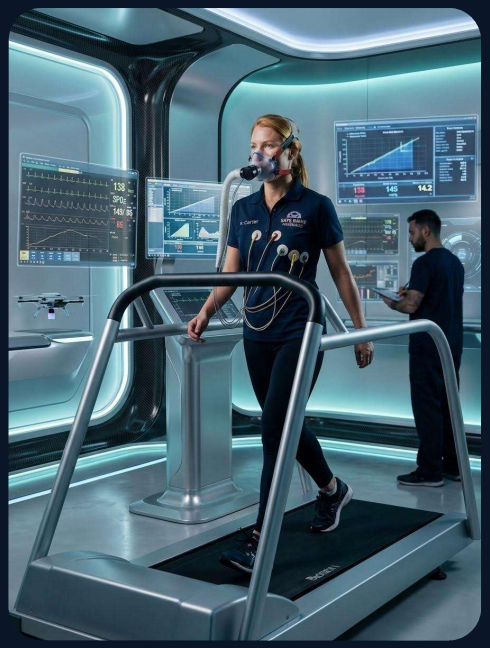
- Can be induced to use bad language
- Ignores human-in-the-loop instructions
- Reveals internal safeguards
- Allows unauthorized data access

Business Impact

- **Brand Reputation**
  Loss of trust and public backlash from rogue AI actions.
- **Audit Failure**
  Non-compliance with enterprise data and safety standards.
- **Project Delays**
  Postponed deployments due to critical security gaps.

© 2026, NuGuard AI, All rights reserved.

NuGuard AI



Stress-test AI employee

DISCOVER
AI stack discovery — every model, tool & API

DEFINE
Intended behavior & data classification

VALIDATE
Automated red-team & behavior testing in a sandbox. Supply chain analysis.

GOVERN
Audit & authorize — evidence package for sign-off

Key Benefits

Safe & Secure AI
Robust application security

Faster Production
Accelerated deployment times

Audit-readiness
Compliance-ready evidence

© 2026, NuGuard AI, All rights reserved.

Why NuGuard

The only platform that focuses on AI behavioral risks before production — not after an incident.

AI Behavior Policy

Standardize Intent.

Allowed Topics, Restricted Topics, Actions, Human-in-the-loop controls, Classified Data handling instructions.

Air-gapped support

No LLM

Regulated, highly secure env need air-gapped, no LLM support. Most AI Security vendors need LLM.

Redteam Innovation Engine

1000+ adversarial tests generated on-the-fly.

Tailored for your specific AI application, Agents, and Behavior Policy. Offensive testing against sub-agents, tools, APIs, and guardrails simultaneously.

Open-source Core

Nuguard open-source repo has **32k downloads** allowing developers and infosec staff to ensure we provide safe & secure technologies.
Community of cybersecurity contributors.

© 2026, NuGuard AI, All rights reserved.

Enterprise-savvy Team

Ranjan Goel



Founder, CEO

Deep agentic security, cybersecurity, cloud, and observability expertise.

LogicMonitor cisco

Rajiv Anand



VP, Growth

Entrepreneur, Innovator
Co-founder, InThing Corp
Co-founder, Cylive

accenture

Devansh Goel



Head of Product

Team lead at Meta for multi-model AI safety and red-teaming initiatives.

Meta

Sam Kumarasamy



VP, Marketing

Marketing executive specialized in AI & cybersecurity.

DEEPWATCH at EY

Ganesh Raman



VP, Engineering

Engineering leadership expertise for cybersecurity, and enterprise SaaS.

netskope nimblestorage

All US-based R&D and GTM team - 8 people

OSS has 12+ active contributors

© 2026, NuGuard AI, All rights reserved.

Key Milestones

May

Opensource Repo

Launched

Initial public release of core security modules and codebase community access.

32k OSS downloads

10 outside contributors

June

Cybersecurity

Verified Partner

Official enterprise security integration approvals:



July

SaaS Platform

Launched

- 2 customers signed
- 1 public reference
- 1 analyst report (Omdia)

next 6 months

Blitz

- Custom redteam LLM
- Managed Services Offer
- Azure, AWS & GCP Marketplace
- Channel partners
- IDC Whitepaper
- Multimodal

NVIDIA Inception Program

© 2026, NuGuard AI, All rights reserved.

Market Landscape & Competition



© 2026, NuGuard AI, All rights reserved.

Go-to-Market Strategy

ICP

Key Decision Makers

- AI Developer (Lead)
- CTO & VP of Engineering

Target Verticals

- AI-Native Startups
- FinTech & HealthTech
- EdTech, eRetail, Gaming

DEVELOPER TRUST

OSS Engagement

- 32k downloads
- 35 stars (2.5 months)
- GitHub & Reddit traffic

Value-First Content

- Custom LLM Redteaming
- How-to guides & tools
- Reference architectures

GTM & CHANNELS

Direct Outreach

- AI-Native focus first
- Target GTM & Health agents

Partnerships & Scale

- MSSP & SI alliances
- Azure Marketplace
- App marketplaces & channels

© 2026, NuGuard AI, All rights reserved.

Financing Plan



FUNDING TARGET

$2M

KEY GOALS

01

Build GTM Engine

Designed for efficient and accelerated customer acquisition.

02

Repeatable Motion

Acquire 200+ free/paid customers by mid 2027.

KEY STATS

Mid 2027

Execution Time Period

USE OF FUNDS

$1.2M — Headcount (HC)

$700k — GTM Engine

$100k — AI & Infra (most cloud & AI credits already available)

© 2026, NuGuard AI, All rights reserved.

Contact: ranjangoel@NuGuard.ai

NUGUARD AI

AI TRUST PLATFORM

Let's make the AI safe and secure for enterprise use

Ranjan Goel

Founder / CEO

ranjangoel@nuguard.ai

Startup: NuGuard AI

https://iitstartups.org/us-demoday-cohort-15/

NuGuard closes the behavior gap in AI applications to improve their safety and security.

SCAN

https://zfrmz.com/p19jyuetieRIM6wRPsfF



Ranjan Goel

Founder & CEO

ranjangoel@nuguard.ai

+1 408 802 4361

https://www.linkedin.com/in/ranjangoel/

https://calendar.app.google/kr2paKcHVJgPxEgs8