I L. M ? O. ,) X > 6* < M ! =M
Ll _ }• Çò * }Çí j / 6ÄhŸ
Æ™® V ¨ ™Ä Mé/ M™_
? 1 ò XÇç| / ? X©®®´ Æ Ul çétÇÄ

THE PATH TO DETERMINISTIC AI GOVERNANCE

How Realflow.ai Builds the Infrastructure Layer That Makes Enterprise AI Trustworthy

Realflow.ai

Investor Whitepaper | Confidential | December 2025

EXECUTIVE SUMMARY

The AI industry has a fundamental security problem that no one has solved: **prompt injection attacks work because governance rules are suggestions, not boundaries**.

Today's large language models rely on training-based defenses; patterns learned during training that can be bypassed by creative attackers. The model "decides" whether to comply with an attack based on probabilistic interpretation. This creates an arms race that defenders cannot win.

Realflow.ai moves governance enforcement from the semantic layer to the mathematical layer of AI inference. By leveraging the attention mechanism that underlies all transformer-based models, we create **cryptographically-enforced trust boundaries that are architecturally inviolable**-not because the model learned to respect them, but because the mathematics of attention computation makes violation impossible.

This breakthrough has three components:

1. **Prompt State Protocol (PSP)** - Open standard for cryptographic prompt integrity
2. **Covenant Declaration Language (CDL)** - Open standard for data governance that travels with data
3. **Attention-layer enforcement** - Patent-pending method for deterministic governance in transformer inference

Combined with our existing platform (semantic-level threat reporting and response, audit logging, human-in-the-loop workflows, and 185 connectors for CDL data governance), this positions Realflow.ai as the definitive infrastructure layer for enterprise AI governance.

Investment Thesis:

- AI governance is a $50B+ market emerging from necessity, not convenience
- Current solutions are fundamentally limited by their approach
- We patented deterministic enforcement and will ship it Q1 2026
- Standards-first strategy creates ecosystem lock-in before competition emerges
- Team has 40 years of enterprise consulting experience and successful exits

---

THE PROBLEM: AI GOVERNANCE IS BROKEN AT A FUNDAMENTAL LEVEL

The $4.4 Trillion AI Market Has a Security Problem

Enterprise AI adoption is accelerating, but security and compliance concerns are the primary barrier. According to industry surveys, 60-70% of enterprises cite AI governance as their top concern when deploying LLM-based systems.

The concerns are justified. The OWASP Top 10 for LLM Applications identifies prompt injection as the #1 vulnerability, and there is no reliable defense.

Why Current Defenses Don't Work

Training-Based Approaches:

Every major LLM provider attempts to train models to resist prompt injection. The core problem: **training teaches the model to recognize patterns, not to enforce boundaries**. An attacker who reformulates their approach can bypass learned defenses because the model is still "deciding" whether to comply based on probabilistic interpretation.

This is not a solvable problem through more training. It's an architectural limitation.

Input/Output Filtering:

External filters that scan inputs for malicious patterns and outputs for policy violations add latency, cost, and still operate in the probabilistic domain. They can catch obvious attacks but miss sophisticated ones.

The Result:

Enterprises face an uncomfortable choice:

- Deploy AI with known vulnerabilities and accept the risk
- Limit AI to non-sensitive use cases, sacrificing value
- Delay adoption entirely, falling behind competitors

The Data Governance Problem Is Equally Severe

Beyond prompt injection, enterprises need assurance that:

- Customer data won't be used for unauthorized purposes
- Regulatory requirements (GDPR, HIPAA, CCPA) will be respected
- Data handling policies will persist across multi-step workflows
- External agents and APIs won't bypass governance rules

Current approaches rely on policy engines external to the AI system. But if an attacker can manipulate the model's interpretation, they can convince it that policies don't apply to their request.

The fundamental insight: governance rules that can be reinterpreted can be bypassed.

THE BREAKTHROUGH: ARCHITECTURAL ENFORCEMENT

Moving from Semantic to Mathematical Enforcement

Realflow.ai's novel approach addresses the root cause: **governance enforcement at the attention layer of transformer models**.

To understand why this matters, consider how transformers process input:

```
Input: [System Prompt] [User Message] [Data]


During processing, every token can "attend to" every other token.
The model decides how to weight different parts of the input.
User content can influence how system prompts are interpreted.
```

This architecture-which enables the remarkable capabilities of modern LLMs-also creates the vulnerability. User content can manipulate how the model interprets system instructions.

Our approach changes the mathematics:

```
Input: [Signed System Prompt] [Signed Data Covenant] [User Message]
During processing, attention masks prevent lower-trust tokens
from influencing higher-trust token representations.
System prompts and covenants are computed in isolation.
User content cannot change what governance rules mean.
```

This isn't about teaching the model to resist attacks. It's about making the attack mathematically impossible within the attention computation.

Patent-Pending Innovation

Realflow.ai filed provisional patent applications covering:

Just-in-time retrieval of cryptographically signed prompt nodes

- Dynamic loading reduces context window consumption by 60-75%
- MCP-based retrieval with signature verification
- Configurable adjacent node loading for execution planning

State-only context reconstruction for extended workflows

- Single JSON state structure replaces full conversation replay
- Importance-based summarization (0-100 scoring)
- 73-97% token reduction vs. traditional approaches

Indefinite human-in-the-loop pause with cryptographic state persistence

- Workflows pause for days or weeks awaiting external approval
- HMAC-signed resume links with expiration

- Selective context reconstruction on resume

Cryptographic trust boundary enforcement in transformer attention mechanisms

- Signature verification triggers attention isolation
- Trust level hierarchy with hard boundaries between levels
- Priority-weighted composition within trust levels
- Agent trust containment and governance gateway for legacy systems

The Standards Strategy

Following the playbook of successful infrastructure protocols (OAuth, JWT, TLS), Realflow.ai releases core specifications as open standards:

Prompt State Protocol (PSP):

- Cryptographic signing for prompt integrity
- Trust level and priority attributes
- Verification without requiring signature authority

Covenant Declaration Language (CDL):

- Data governance specifications that travel with data
- Permitted uses, prohibited actions, jurisdictional requirements
- Inheritance for derived data

Why Open Standards?

Approach	Adoption	Moat
Proprietary only	Slow, resistance from ecosystem	Easily commoditized
Open standard	Fast, ecosystem embrace	Implementation excellence + patents

By establishing the standard, we define how the industry thinks about AI governance. Competitors implementing PSP/CDL validate our approach and feed our ecosystem. Our patents protect the enforcement mechanisms that make the standards meaningful.

THE PLATFORM: WHAT WE HAVE BUILT TO-DATE

Realflow.ai is not a research project. We have a shipping platform with real capabilities:

Governance Observability (Shipping January 2026)

Semantic-Level Threat Reporting and Response:

- 41 violation types across behavioral, semantic, and data governance categories

- Real-time monitoring, alerting, and automated response
- Pattern analysis across conversations

Signature Verification:

- PSP signature validation for prompt integrity
- CDL covenant verification for data governance
- Chain of custody across workflow steps

Audit Infrastructure:

- Complete conversation logging with governance metadata
- Compliance-ready reporting (SOC 2, ISO 27001, HIPAA)
- Forensic analysis capabilities

Human-in-the-Loop Workflows (Coming February 2026):

- Pause/resume with cryptographic state integrity
- Approval workflows with arbitrary duration pauses (days, weeks)
- Secure link distribution for external approvals

Pricing Tiers

Tier	Price	Capabilities
Starter	$79/mo	Threat reporting, declarative response, shared infrastructure
Professional	$299/mo	CDL definitions, semantic enforcement, identity provider integration
Dedicated	$799/mo	Private containers, SLA guarantees
Enterprise	Custom	BYOC, unlimited scale, custom integration

Progressive capability model. Starter provides visibility and response; Professional adds data governance and enforcement.

THE ROADMAP: FROM DETECTION TO ENFORCEMENT

Phase 1: Governance Observability (January 2026)

What we ship:

- Semantic-level threat reporting, alerting, and response
- Signature verification (integrity assurance)
- Audit logging and compliance reporting
- Human-in-the-loop workflows

Positioning: "See what's happening in your AI workflows. Verify integrity. Maintain compliance."

Why this matters: Detection has genuine value. SOC 2 and ISO 27001 require monitoring controls. Audit trails provide liability protection. Enterprises need visibility regardless of enforcement mechanism.

Phase 2: Hosted Deterministic Enforcement (Q1 2026)

What we ship:

- Hosted open-source model (Llama 3 / Mistral) with attention-layer trust boundary enforcement
- Cryptographic governance that is architecturally inviolable
- Full PSP/CDL support with deterministic compliance
- Attack-resistant inference for immediate production use

The play: This hosted model is not intended to compete with foundation models. It serves two purposes:

1. **Proof of concept at scale** - Demonstrates that attention-layer enforcement works in production, with measurable attack resistance statistics
2. **Licensing pressure** - Foundation model providers (Anthropic, OpenAI, Google) see the technology working and license it rather than build from scratch

Target customers for hosted model:

- Smaller firms with immediate compliance requirements
- Enterprises needing proof-of-concept validation before broader deployment
- Regulated industries requiring deterministic governance guarantees
- Organizations blocked by security review on foundation model deployments

Positioning: "The industry's first deterministic defense against prompt injection. Available now."

The Licensing Endgame

We fully expect foundation model providers to license this technology. The attention-layer enforcement mechanism is:

- **Patent-protected** - We control the IP
- **Model-agnostic** - Works with any transformer architecture
- **Essential for enterprise adoption** - Governance is a procurement requirement

The hosted open-source model proves the technology. The patents protect it. Foundation models pay to implement it.

Revenue model evolution:

Phase	Revenue Source
Now	Platform subscriptions (detection + hosted enforcement), Enterprise engagements
12-18 months	Licensing revenue from foundation model providers
24+ months	Per-inference royalties at scale (Could reach 1.25%-2.5%)

MARKET OPPORTUNITY

Total Addressable Market

AI governance sits at the intersection of multiple large markets:

Market	2025 Size	Growth	Relevance
AI Infrastructure	$50B	35% CAGR	Direct
Cybersecurity	$180B	12% CAGR	Adjacent
GRC Software	$45B	14% CAGR	Adjacent
Enterprise Integration	$35B	10% CAGR	Platform

Conservative TAM estimate: $50B by 2028 for AI-specific governance

Timing

Several factors create urgency:

Regulatory pressure:

- EU AI Act enforcement beginning 2025
- NIST AI Risk Management Framework adoption
- Industry-specific requirements (healthcare, finance)

Enterprise adoption inflection:

- Major enterprises moving from pilots to production
- Security reviews blocking deployment
- Governance becoming procurement requirement

Protocol standardization:

- MCP (Model Context Protocol) gaining adoption
- A2A (Agent-to-Agent) protocol emerging
- Industry seeking governance standards

Competitive Landscape

Current players (detection/filtering):

- Robust Intelligence, Lakera, Protect AI
- Approach: LLM-based input/output analysis
- Limitation: Probabilistic, costly, latency

Cloud providers:

- AWS Bedrock Guardrails, Azure Content Safety
- Approach: Platform-integrated filtering
- Limitation: Vendor lock-in, still probabilistic

Foundation model providers:

- Training-based defenses
- Approach: Model-level hardening
- Limitation: Fundamental architectural constraint

Realflow.ai differentiation:

- Only company shipping deterministic enforcement (Q1 2026)
- Patent protection on attention-layer mechanism
- Open standards creating ecosystem lock-in
- Licensing leverage over foundation model providers
- Full platform vs. point solution

BUSINESS MODEL

Revenue Streams

Platform Subscriptions:

- Recurring SaaS revenue
- Land with Starter (visibility), expand to Professional (enforcement)
- Natural upgrade path as governance needs mature

Enterprise Contracts:

- Custom deployment (BYOC)
- Dedicated support
- Compliance attestation services

Partner Channel:

- Consulting firms implement governance programs
- Platform subscription to Realflow.ai
- Services revenue to partners
- Margin profile attractive to Big 4, boutique consultancies

Marketplaces Channel:

- Our CDL starter packs and Realflow.ai technology can be sold on ERP marketplaces
- Platform subscription to Realflow.ai
- SAP/Salesforce/ZenDesk/MS/Azure/AWS etc.
- Implied endorsement
- Low CAC

Go-to-Market Strategy

Trojan Horse Approach:

Individual user discovers Realflow.ai → Solves integration problem

↓

Multiple users in organization adopt → Network effect

↓

CTO discovers usage → "Your teams are already using us"

↓

Governance conversation → Enterprise contract

Partner Channel:

- Consulting firms need AI governance practice revenue
- Platform enables high-margin services
- Partners handle implementation, we provide infrastructure

Unit Economics (Projected)

Metric	Target
CAC	$200 (product-led) (lower via Marketplaces)
LTV	$2,400 (2-year average)
LTV:CAC	12:1
Gross Margin	85%
Net Revenue Retention	130%

TEAM

Mick Seals, Founder/CEO

- 40 years enterprise consulting experience
- Consulting firms since 1993, independent since 2023
- Serial entrepreneur with successful exits
- Deep expertise in enterprise integration and governance

[Additional team members to be added]

INVESTMENT OPPORTUNITY

Current Round

Instrument: SAFE (Simple Agreement for Future Equity) **Status:** Pre-Seed closed. Seed round open. **Use of Funds:**

- Platform launch (January 2026)
- Hosted enforcement model deployment (Q1 2026)
- Patent completions for full filings
- Initial marketing and sales

Terms discussed in conversation.

Why Now

1. **Patent window:** Provisional applications filed; 12 months to establish priority dates
2. **Market timing:** Enterprise AI adoption accelerating, governance demand urgent
3. **Standards opportunity:** First mover in AI governance protocols
4. **Competitive gap:** No one else has identified the attention-layer approach
5. **Licensing leverage:** Hosted model creates pressure for foundation model licensing

Exit Potential

Strategic Acquirers:

- Anthropic (AI safety alignment with their mission)
- Microsoft (Azure AI governance)
- Salesforce (Agentforce governance)
- AWS (Bedrock governance layer)

Licensing Revenue Path:

- Foundation model providers license attention-layer enforcement
- Per-inference royalties at scale
- Essential infrastructure = recurring revenue without customer acquisition cost

IPO Path:

- Target: $50M ARR (subscriptions + licensing)
- Timeline: 3-4 years
- Positioning: Essential AI governance infrastructure

THE MAGNITUDE OF THE OPPORTUNITY

Realflow.ai is positioned to become the **SSL/TLS of AI systems**: invisible infrastructure that makes everything else trustworthy.

Every enterprise deploying AI needs governance. Every AI workflow needs trust boundaries. Every regulated industry needs compliance. Every foundation model provider needs a solution to prompt injection.

The question isn't whether this market exists. The question is who builds the infrastructure layer and who owns the patents.

We have:

- The insight (attention-layer enforcement)
- The patents (filed)
- The standards (PSP, CDL)
- The platform (shipping January)
- The hosted enforcement model (shipping Q1)
- The licensing leverage (foundation models need this)
- The team (experienced)
- The timing (now)

This is infrastructure-level innovation in a market that's just recognizing it needs infrastructure.

NEXT STEPS

To learn more about Realflow.ai:

Contact: Mick Seals Founder/CEO mick@realflow.ai 315-359-9198

CONFIDENTIALITY NOTICE

This whitepaper contains confidential information regarding Realflow.ai's technology, business plans, and intellectual property. Distribution is limited to potential investors under NDA. Patent applications are pending; please do not disclose technical details regarding attention-layer enforcement mechanisms.
