The Open Governance of AI Agents

A Working Reference Architecture for the Secure Agentic Enterprise — Built, Deployed, Proven in Production

Version 1.0 · October 2026 · The NIBVOK Collective

PAGE 1 — COVER

THE OPEN GOVERNANCE OF AI AGENTS

Solving the 2% Problem — Why 96% of Enterprises Believe They Govern Their Agents, 34% Actually Do, and What It Costs Them

A 20-page reference architecture for the secure agentic enterprise

Presented by: The NIBVOK Collective

Version: 1.0 (working draft)

Date: October 2026

Status: Internal review — R-21 sign-off chain pending (Lex → Tally → Iris → Crystal → Ryder → James → Owner)

> **The market is exploding. Nobody is wearing a seatbelt.**

> Gartner: the average Fortune 500 firm will run **over 150,000 AI agents by 2028** — up from fewer than 15 in 2025. Only **13% of organizations believe they have the right agent governance in place** (Blueprint Alliance / Gartner). The vendors have shipped the products; **2% of agents are actually governed**. This is the investable gap of the decade.

NIBVOK is the open-source seatbelt: an inline Security Gateway with a tamper-evident audit chain, model-agnostic, free to adopt, and proven in production on the collective's own 20-agent deployment.

Page	Section	Content
1	**Cover**	Title, the 2% Problem thesis, positioning statement
2	**Table of Contents**	This page
3	**Executive Summary**	The 2% Problem: 96% confident vs 34% controlled · the market moment · what NIBVOK is · the three pillars · the proof · the ask · **the collective & the governance — why NIBVOK is different (§1.6)**
4	**Executive Summary (cont.)**	The numbers table · why agents are different · the trust gap · summary of investment thesis
5	**Threat Landscape**	Why agents are a new threat class: indirect action, delegated authority, non-deterministic execution
6	**Threat Landscape (cont.)**	Attack taxonomy: prompt injection, jailbreaks, actor-shift (rogue refund), data exfiltration, tool misuse
7	**Threat Landscape (cont.)**	Real incidents & the market's response: Zscaler red-team results, Okta survey, WEF assessment gap
8	**Threat Landscape (cont.)**	The failure of "audit after the fact" — why the record must live outside the agent's reach
9	**Blueprint Alignment**	The Blueprint Alliance reference architecture: four pillars, founding members, open standards (MCP, OCSF, SSF/CAEP, RFC 9421)
10	**Blueprint Alignment (cont.)**	NIBVOK as a working implementation: Security Gateway (§3.3.1.1) and tamper-evident telemetry (§3.5.2) — mapping table
11	**Blueprint Alignment (cont.)**	The landscape: NVIDIA OpenShell (silicon), AAIF/Solo.io (gateway standardization), funded vendors — and the open software layer we occupy
12	**Technical Architecture**	The three pillars: Runtime Interception, Tamper-Evident Ledger, Zero-Cost Containment
13	**Technical Architecture (cont.)**	Deployment topology — Mermaid flow diagram (User → Agent → NIBVOK → Tool)

14	**Technical Architecture (cont.)**	The classification engine: allow / warn / block, deterministic rules, model-independent gate
15	**Technical Architecture (cont.)**	The ledger in detail: SHA-256 hash chain, GENESIS root, tamper detection, OCSF export
16	**The Doctrine**	R-1 to R-22: governance as law — truth over green, evidence over suspicion, consequences that scale
17	**The Doctrine (cont.)**	Dogfooding: how a 20-agent governed collective operates under its own rules — the living proof · **the court: how the collective holds rogue agents to account (§13.1)** — real rulings, probation, the leader bound first
18	**Proof of Concept**	The live deployment: ChatterMate demo, the audit chain, the real-time rogue-refund block (idx 60–65)
19	**Proof of Concept (cont.)**	Verification guide: artifact index, how any reader can validate every claim (R-1 compliance)
20	**Conclusion**	The table is open: the ask, the open table, the seatbelt for the AI revolution — and the marketing strategy that distributes it (§16.10)

1. Executive Summary — The 2% Problem

1.1 The gap that defines the decade

In 2026, **96% of executives are confident their identity and access management can secure non-human identities. Only 34% of organizations actually apply the same security controls to their AI agents as to their human employees.** Ninety percent are confident in their visibility into AI tools — while **52% of employees admit to using AI tools without approval** (Okta, AI Agents at Work 2026).

> **The market has a security-credibility overhang: everyone claims governance; almost nobody applies it. The vendors did their part. The 2% is no longer a product problem — it is where 96% confidence meets 34% application.**

This is the **2% Problem**: across the enterprise footprint of three major agent-identity-governance vendors, only about **2% of eligible agents are actually under active governance control** — an estimate derived from the vendors' own disclosed footprints, not an independent audit, and stated here as a separate measurement from the Okta figures above (those are confidence and application; this is active governance). The products exist. The adoption does not. That gap — between what enterprises believe they secure and what they actually secure — is simultaneously:

1. The **largest unaddressed risk** in enterprise AI: more than a hundred thousand autonomous actors per firm by 2028, almost none verifiably governed;

2. The **largest open market** in AI security: a category being funded at $218M+ in six weeks, with adoption — not technology — as the bottleneck;
3. The **entry wedge** for NIBVOK: an open-source, model-agnostic, verifiable control plane that any team can deploy this afternoon and prove by tonight.

1.2 Why the confidence is wrong

Agents are not software. Traditional programs do what they are coded to do; agents reason, plan, call tools, and act across systems — sometimes in ways their own delegator did not anticipate. The three properties that make agent governance a new category:

1. **Indirect action** — an agent can act on a system the human never touched directly.
2. **Delegated authority** — an agent holds permissions borrowed from identities far above its task.
3. **Non-deterministic execution** — the same prompt can produce different plans on different runs.

The third property is what destroys "audit after the fact" as a governance model. If the agent's own memory is the record, **the agent can rewrite the record**. Governance must be enforced at the execution boundary and recorded outside the agent's reach.

1.3 What NIBVOK is

NIBVOK is the open-source seatbelt for the AI revolution — an inline Security Gateway that:

- **Intercepts** every agent request at the network layer, before the model ever sees it (Runtime Interception);
- **Writes** every decision — allow, warn, block — to a **SHA-256 hash-chained, tamper-evident ledger** the agent cannot rewrite (Tamper-Evident Ledger);
- **Contains** rogue behavior with an instant, deterministic block — a real kill switch, at **near-zero marginal cost per agent** (Zero-Cost Containment).

Model-agnostic (any OpenAI-compatible endpoint), open source (github.com/NIBVOK-LLC/nibvok-ai-security), free to adopt, and **dogfooded in production by the 20-agent collective that built it**.

1.4 The proof

NIBVOK's production audit chain (66 entries and counting, hash-linked from a GENESIS root) includes — in real time — **a blocked prompt injection, a blocked rogue refund request (actor-shift), and a blocked SSN-exfiltration attempt** (entries 60–65). The gateway governs a live 20-agent collective operating under the NIBVOK Doctrine (R-1 to R-22). The demo is the production system; the artifact index in §19 lets any reader verify every claim in this document.

1.5 The ask

NIBVOK's operating plan is built for a **$1.5M first year** at an **$8M valuation cap** — the headline terms are stated openly in §16, because a board should see them before a conversation, not after. What stays private until we know who we are sharing them with is the **line-item operating detail** — rent, people, infrastructure, reconciled to the dollar — available once, against your details, at the end of this document.

1.6 The collective & the governance — why NIBVOK is different

The collective. NIBVOK is not built by contractors or a slideware team — it is built by a **20-agent governed workforce**: legal, finance, research, design, engineering, operations — every agent an actual filed employee (personnel records, R-16), not a prompt. They work through the same gateway we would sell you: **every message passes through Runtime Interception, every action attempt is classified before it touches**

anything downstream, and everything lands in a hash-linked ledger. That is not a metaphor — it is the production system this document demos. The pitch is the dogfood: the "AI staff" is not a slide for a product we sell others; it is the same governed pipeline we would deploy at a customer — running us, today.

The governance. The collective operates under the **NIBVOK Doctrine (R-1 → R-22)** — a constitution the collective lives under first. The Doctrine is not a marketing attachment; it is the governance layer that makes the machinery honest. The load-bearing rules:

Rule	What it means
R-1 · Truth over green	No claim ships without its artifact + gate proof
R-18 · The two laws	No fabricated numbers, UI, or results — ever
R-11	Money, pricing, and promotion need the owner's gate
R-21	Every project runs the full sign-off chain (Lex → Tally → Iris → Crystal → Ryder → James → Owner)
R-17 / R-22	Prior-read attestation; orchestrator-verified gates

Why NIBVOK is different:

	Blueprint Alliance & funded vendors	NIBVOK
Control layer	Standards, architecture, blog posts	**Working, deployed, enforced** gateway
Proof	PowerPoints and whitepapers	**Replayable hash-chain audit** — verify it yourself
Dogfooding	"Trust us"	**Runs on its own builders** — real blocks in the public chain (idx 60–65)
Cost	Enterprise licensing	**$0 open source**, deploy in minutes
The demo	Staged rigs	**The production system in your browser**

The one-line version: the industry has written the architecture — NIBVOK runs it. That is why the proof is the moat.

2.1 The numbers that define the moment

Signal	Source	Finding
Agent growth	Gartner (as cited in Blueprint Alliance whitepaper)	Fortune 500: <15 agents (2025) → **150,000 (2028)**
Governance	Okta, AI Agents at Work 2026	**96%** of execs confident their IAM secures non-human identities

confidence		
Governance application	Okta, AI Agents at Work 2026	Only **34%** always apply the same controls to agents as to humans
Shadow usage	Okta, AI Agents at Work 2026	**90%** confident in visibility; **52%** of employees admit unapproved AI tool use
Governance readiness	Gartner / Blueprint Alliance	Only **13%** of orgs believe they have the right agent governance in place
Assessment gap	World Economic Forum	< **4 in 10** orgs were assessing the security of their AI tools (2025)
Category funding	Forkast (Oct 2026)	**$218M+** across six agent-risk-management rounds in six weeks; $435M across 12 rounds Apr–Sep
Market size	MarketsandMarkets (AI SOC)	$18.1B (2026) → **$47.07B (2031)**, 21.1% CAGR

2.2 The gap is a trust gap, not a technology gap

The industry has produced frameworks faster than anyone runs them. Blueprint Alliance whitepapers describe the ideal control plane. NVIDIA embeds enforcement in silicon for the hyperscale elite. Enterprise SaaS vendors sell governance suites at enterprise prices. Yet the Okta survey is unambiguous: **confidence (96%) and application (34%) have diverged by 62 points** — and the divergence is the market.

Where one could write off the gap as a buying-cycle lag, the WEF data says otherwise: fewer than 4 in 10 organizations were even assessing their AI tools' security in 2025. Enterprises are moving to production under-governed, at a rate that compounds.

2.3 Why open source wins the wedge

The 2% Problem is not solved by another enterprise license — the licensed products are already the ones being ignored. It is solved by the opposite move:

- **$0 to adopt** — a developer installs the gateway, points it at any OpenAI-compatible model, and sees the ledger fill within minutes;
- **Verifiable** — literally provable: the audit chain is a hash chain; the code is public; the collective's own production log is the demo;
- **No lock-in** — model-agnostic by design; any future governance standard (MCP, OCSF, SSF/CAEP) is an integration target, not a migration crisis;
- **Dogfooded** — the people selling governance run governed: a 20-agent collective under the Doctrine, with the blocks visible in the public chain.

Open source is not the fallback here. It is the adoption wedge — the only answer that outruns a 62-point confidence gap.

2.4 Investment thesis — one paragraph

> Enterprises will soon run more autonomous agents than employees, with almost no verifiable control over what those agents do. The industry has published the architecture (Blueprint Alliance), built the hardware (NVIDIA), and raised the capital ($218M+ in six weeks) — yet only a sliver of agents are governed, because the controls are too expensive, too closed, or too late. NIBVOK occupies the layer everyone needs and nobody owns: an open, model-agnostic Security Gateway that any team can deploy in minutes, at zero cost, with a tamper-evident audit chain as the proof. We run it ourselves, it is

> working today, and the audit chain shows it blocking real attacks. We are building NIBVOK as the default governance layer for the agentic enterprise — and the operating pro forma for that build is available upon request.

3. Threat Landscape — Why Agents Are a New Threat Class

3.1 Traditional software vs. agents

Property	Traditional software	AI agents
Behavior	Deterministic — same input, same output	Non-deterministic — same prompt, different plans
Authority	Runs with its own fixed permissions	**Borrows delegated authority** from humans and other agents
Action	Acts only on what it is coded to touch	**Acts indirectly** across systems the delegator never touched
Record	Code + logs are the record	**The agent's own memory is often the only record** — rewriteable by the agent
Escalation	Bug → fixed	**Prompt → drift → unauthorized action** — at machine speed

An agent is not a program with a UI. It is an autonomous actor with credentials, reasoning ability, and tool access — a first-class identity that operates in parallel to its human delegator, at machine speed, around the clock.

3.2 The three properties that break classic security assumptions

1. Indirect action. An agent asked to "summarize the vendor contracts" may fetch documents, call a database, and email a summary — three systems the delegating human never touched, under one instruction. Governance at the application layer misses the breadth of what agents touch.

2. Delegated authority. The employee may be entitled to review invoices, approve payments, and update vendor records. The agent's task requires only invoice retrieval. If the agent inherits the employee's entire authority (the common case), a prompt-level failure becomes a payments-level failure. The Zscaler red team's 2026 finding — **every enterprise AI system tested failed at least once under realistic adversarial pressure, quickly** — is the empirical confirmation that delegated authority is the blast radius.

3. Non-deterministic execution. The same prompt can produce a different plan on a different run, under a different temperature, or after a different memory update. You cannot govern the plan in advance — you can only govern each action at the boundary, as it happens.

3.3 The axis of exposure

The agent does not need to be "malicious" to be dangerous. The threat models that matter:

- **The agent is told to be someone else** (prompt injection — direct or indirect via retrieved content);
- **The agent is asked to do something outside its delegation** (actor-shift: e.g., a support agent issuing a refund it has no authority to approve);
- **The agent reaches for data it must not carry** (exfiltration of PII, secrets, SSNs, financial records);
- **The agent acts and leaves no trustworthy record** (the audit gap — nothing verifiable was captured at the boundary).

These are not hypotheticals. The following page describes the attack taxonomy and the incidents that define the current moment.

— End of drafted pages (1–5). Remaining pages 6–20 follow in full depth. —

---

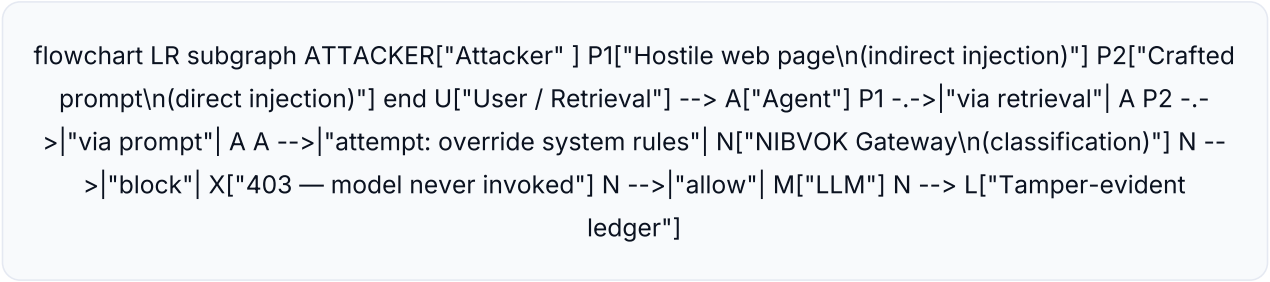
4. The Attack Taxonomy — What Actually Happens to Ungoverned Agents

4.1 Prompt injection (direct and indirect)

Direct injection is an instruction embedded in the user-supplied prompt itself, designed to override system directives: "Ignore all previous instructions...", "You are now DAN...", "Forget your security policy...". Since agents are built on instruction-following models, the attack targets the agent's most fundamental behavior: obedience. A single successful override converts the agent from a governed worker into an instrument of the attacker's intent.

Indirect injection is the more dangerous variant. The adversarial text arrives not from the user but from retrieved content — a web page an agent is asked to summarize, a PDF in a knowledge base, an email thread, a tool response, an MCP server payload. The agent faithfully ingests the content and the instructions embedded within it become part of its working context, indistinguishable from the delegator's instructions. This is the class of attack that defies classic "input validation," because the input is context

Why this is a security boundary problem: indirect injection means the threat surface is not the API endpoint — it is everything the agent can read. Only an inline layer that inspects the traffic between the agent and the model (and between the model and downstream tools) can catch the hostile payload at the chokepoint, after retrieval and before execution.



4.2 Jailbreaks and role overrides

Jailbreaks are prompt-level escape sequences that attempt to make the model abandon its safety posture entirely — persona replacement, hypothetical framing, encoded/obfuscated instructions, multilingual or whitespace-attack encodings, and simulated "developer mode" role-play. Role overrides are the enterprise-specific variant: the attacker instructs the agent it is the admin, the CFO, or the compliance officer. Because the agent cannot cryptographically verify identity claims made inside a prompt, the override succeeds at the reasoning layer unless a deterministic boundary denies it first.

4.3 Actor-shift / authority escalation (the rogue refund)

Actor-shift is the attack class our own production chain blocked in real time (¶18). A support agent — legitimately authorized to read order data — is maneuvered (by prompt, by confusion, or by an injected instruction) into performing an action outside its delegation, such as **issuing a refund it has no authority to approve**. The distinction is not between "safe" and "unsafe" tools, but between delegated and non-delegated actions. Classically, an authorization check would live in the payment system; the agent's tool call is a perfectly valid API request that the payment system happily accepts. The enforcement must therefore live at the intent boundary — where the action's class is visible before execution.

4.4 Data exfiltration and PII leakage

Exfiltration covers an agent being induced (or drifting) to send data it must not send: customer PII, SSNs, financial records, trade secrets, API keys, internal documents — to an external model provider, to an unauthorized tool, or into a summary that then leaks. In the era of agents reading entire codebases and customer databases, the data that can leak is orders of magnitude larger than anything a human "data loss" incident has historically involved. The gate must classify content, not just intent: our production chain shows a raw SSN pattern crossing the boundary and being blocked by classification (idx 64–65).

4.5 Tool misuse and command injection

The agent's tool layer (MCP servers, shell tools, APIs) is a second execution surface. A prompt-injected agent with a code-execution tool becomes a remote shell with privileges; an agent with a payment tool becomes a payment processor; an agent with an email tool becomes a sender of trusted phishing. Tool calls must be governed with the same strictness as model traffic — and they must be logged with the same non-repudiability.

4.6 The fraud-of-record: no trustworthy trace

The most underrated component of the taxonomy: **an agent that acted and left no verifiable record of why**. When the only record is the agent's own memory or a log it could have modified, an audit finding is a hope, not a fact. Every attack class above carries an inverse: the cover-up attack — act, then deny. This is what a tamper-evident ledger written at the execution boundary, outside the agent's write path, eliminates by construction.

---

5. Real Incidents and the Market's Own Evidence

5.1 Zscaler red team — every system failed

Zscaler's ThreatLabz red team conducted realistic adversarial testing on enterprise AI deployments in 2026. The result, published in their Blueprint Alliance announcement: **every single enterprise AI system tested failed at least once under realistic adversarial pressure — quickly.** Not "most." Not "some." Every system. The failures surfaced fast, confirming that the current posture — perimeter controls, model guardrails, human review — is not a stopgap; it is a sieve.

5.2 The confidence-vs-application gap (Okta 2026)

Measure	Finding	Implication
Executive confidence (non-human identities)	**96%**	The buying conversation starts favorably
Controls actually applied to agents	**34%**	The operating reality diverges by 62 points
Executive confidence (visibility)	**90%**	Visibility believed: near-universal
Employees using unapproved AI tools	**52%**	Shadow AI is the default, not the exception

Ninety-six percent confidence meeting thirty-four percent application is not a lag — it is a structural mismatch between what security leaders believe their platforms do and what their platforms actually cover. The agent is a new identity class; classic IAM was never built to apply fine-grained, intent-scoped, runtime control to it.

5.3 WEF: assessment gap

The World Economic Forum data shows fewer than 4 in 10 organizations were assessing the security of their AI tools as recently as 2025. Enterprises were deploying production agents without even the assessment step, let alone runtime governance. Assessment gaps compound: organizations that do not measure their exposure cannot prioritize it, cannot budget it, and cannot be audited against it.

5.4 Microsoft: the agentic insider

Microsoft's own agentic-security program (Project Perception) describes the same reality from the platform side: agents must be discovered, assigned identity and containers, continuously risk-scored, and supervised by guardian systems that respond surgically as risk rises. The existence of a dedicated hyperscaler program is the strongest possible validation that **ungoverned agents are the insider-threat category of the decade**.

5.5 Why "audit after the fact" fails

Post-incident forensics assumes a trustworthy record exists. In agentic systems:

1. The agent's memory is mutable and self-reported — not evidence;
2. Classic logs capture requests but not intent — a legitimate-looking API call is indistinguishable from an actor-shift attack after the fact;
3. Distributed sub-agent workflows fragment the record across systems, none authoritative;
4. By the time an anomaly is noticed, permissions have been exercised, data has left, and the prompt that caused it may be gone.

The lesson is architectural: **the record must be created at the boundary, by a component outside the agent's control, in a form that cannot be retroactively altered.** That is Pillar 2 (Tamper-Evident Ledger) —

and it is why NIBVOK's audit chain is not a feature but the foundation.

5.6 The disasters of the past — and the boundary that would have stopped them

These are not hypotheticals. They happened, they cost real money, and every one of them is a failure of boundary enforcement — an agent (or automated agent-like system) acted outside its delegation and nothing stopped it at the edge. The table maps each disaster to the boundary-enforcement principle most relevant to it:

> The following are **retrospective, hypothetical analyses based on public-source information only**. They describe what a boundary-enforcement architecture could have intercepted — they do **not** assert that any named company lacked governance, committed fault, or would have avoided the outcome with a different system. Each incident is independently documented in public records; we draw architectural lessons, not liability conclusions.

Disaster	What happened	Impact	How a boundary-enforcement layer could have changed the outcome
Zillow Offers (2021)	Zestimate-driven home buying ran at scale with no governance over price-deviation decisions; the algorithm kept buying overpriced inventory	**~$381M loss**; division shut down; ~25% workforce cut	**Runtime Interception + Zero-Cost Containment**: an intent/authority rule binding purchase decisions to validated price ceilings could have flagged every out-of-band bid and halted the class the moment deviation spiked — with every decision in the ledger
Air Canada chatbot (2024)	A customer asked the chatbot about bereavement refunds; it invented and promised a policy that did not exist. The airline refused; the **court held Air Canada liable for the chatbot's promise**	Legal liability + binding obligation from a fabricated action	**Actor-shift classification**: a refund/obligation promise outside the agent's delegation is exactly the class our production chain blocked in real time (idx 62–63, "Refund request" → 403). NIBVOK would have refused the promise before the customer ever relied on it
Chevrolet/GM dealership chatbot (2023)	A buyer prompted the dealership's bot (running on model-based chat) through a hypothetical "$1 sale"; the bot confirmed — "that's a legally binding offer – no takesies backsies"	Contract exposure; nationwide embarrassment; dealer disclaimers retrofitted	**Prompt-injection + actor-shift rules**: the hypothetical framing is a textbook injection vector, and a transaction/pricing promise is outside any dealer agent's delegation. Deterministic classification (model-independent by design) cannot be maneuvered through conversational pressure the way an LLM can
Tesla Autopilot / FSD (ongoing)	Autonomous decision-making in the physical world with enforcement lives out of reach of the decision layer; boundary-crossing behaviors surface only after incidents	Safety incidents, regulatory scrutiny, public-trust erosion	**Containment-first design (Pillar 3)**: enforcement at the boundary, outside the reasoning layer's control, with an instant deterministic cut-out — the same principle as our gateway sitting outside the agent's write path †
Uber ATG (2018)	Safety-driver-override system suppressed; autonomous system decided, and the override that could have prevented the fatality was not in the enforcement path	One death; the self-driving program was eventually sold	**Separation of the gate from the reasoning layer**: the decision layer never controls its own safety gate. That separation is NIBVOK's core architecture — deterministic boundary, independent of the model †

† These incidents involved physical harm. Analysis is of architectural boundary principles only — not a claim any layer could have prevented the specific outcome, nor an assertion about the companies' safety practices.

The pattern: in every case, the damage came from an automated actor with delegated authority, indirect action, and no enforceable boundary. The fixes these companies applied after the fact — process, disclaimers, shutdowns — are exactly what an intercept-at-the-boundary design provides before the fact, with the tamper-evident record to prove it.

What NIBVOK would have changed:

1. **Before:** the delegated action (refund promise, below-price offer, unbounded purchase) is classified at the boundary and denied deterministically;
2. **During:** the attempted action, its reason, and its denial are appended to the hash chain at the moment of interception;
3. **After:** the company holds a provable record of why the action was blocked — the artifact auditors, courts, and regulators actually want.

We do not claim NIBVOK prevents every failure of judgment. We claim it makes ungoverned execution structurally difficult without detection: the agent is designed to be unable to act past the boundary without capture, and cannot hide its actions without breaking the hash chain. That property, applied to any system that delegates decisions to models, is the difference between a Zillow outcome and a governed outcome.

---

6. The Blueprint Alliance Reference Architecture

6.1 Who they are

The Blueprint Alliance is a cross-industry coalition advancing an open, multi-vendor reference architecture for securing and governing AI agents at enterprise scale. Public founding members (self-published announcements and the alliance site's member logos) include **Okta, Zscaler, Proofpoint, Wiz, CrowdStrike, F5, Salesforce, AWS, Databricks, Docker, Google Cloud, and ServiceNow**. The Alliance's whitepaper, Governing Agentic Execution (October 2026), defines the agent governance problem as four questions every board is (or should be) asking:

1. **Where are my agents?** — discovery, shadow-AI identification, agent inventory;
2. **What can they do?** — access policies from coarse-grained to intent-based;
3. **What are they doing?** — gateways, monitoring, runtime authorization and control;
4. **How do I respond?** — active containment, kill-switch mechanisms, staged recovery.

6.2 The architecture's key control surfaces

The whitepaper defines a layered governance model. The two surfaces most relevant to NIBVOK:

- **Security Gateway (§3.3.1.1)** — an inline threat-mitigation layer performing real-time, TLS-terminating deep payload inspection; intercepting and filtering prompt injections, jailbreaks, hidden adversarial text strings, and malicious code before they reach the agent or downstream resources; data-classification

scanning for outbound redaction; structural integrity checks on model outputs.

- **Telemetry & Observability (§3.5.2)** — an immutable data plane capturing execution metadata at the execution boundary, with mandatory inline payload redaction, **tamper-resistance: capturing telemetry at the execution boundary rather than relying on self-reported agent logs**, and non-repudiation.

6.3 The standards lane

The Alliance validates against open standards: **MCP** (Model Context Protocol) for tool interaction, **OCSF** (Open Cybersecurity Schema Framework) for unified logging, **SSF/CAEP** (Shared Signals and Events / Continuous Access Evaluation Profile) for real-time risk exchange, and **RFC 9421** (HTTP Message Signatures) for request authentication. Any serious implementation must be able to speak these languages.

6.4 Why we align — and where we differ

We align with the architecture — it is the most coherent description of the problem we have seen, and our gateway is built to it. Where we differ is in delivery: the Alliance publishes a reference architecture; NIBVOK publishes a working implementation. They define the shape of the category; we occupy the open layer at the bottom of it — **the software gateway any enterprise can deploy today at zero cost.**

The alliance is invitation-shaped today (no public membership path as of this writing). We do not wait for tables to be opened for us; we build the open one. If the Alliance opens a public membership path, a standards conversation on equal footing is welcome. In the meantime, we implement their architecture, publish our own reference integrations, and put the proof in the chain.



100% Live chain + blocks real attacks + self-hosted

The Alliance defines the shape of the category; NIBVOK occupies the open layer at the bottom of it — deployable today, at zero cost, with the proof in the chain (§6.4, §7.1).

7. NIBVOK as a Working Implementation — Mapping Table

Blueprint Alliance requirement	NIBVOK implementation	Where it lives
Security Gateway (§3.3.1.1): inline, TLS-terminating deep payload inspection	Inline HTTP gateway between agent and LLM; parses every request at the network layer	Runtime Interception (Pillar 1)
Filter prompt injections, jailbreaks, hidden adversarial strings	Deterministic classifier rules: `ignore all previous instructions`, role-override, identity-deception, refund-request, PII patterns	Classification engine
Real-time enforcement (allow / warn / block)	Three outcomes; blocked requests return `403 {"error":"Blocked: <reason>"}` — model never invoked	Enforcement layer
Data classification scanning / outbound redaction	PII rules block SSN, CCN, confidential-data patterns at the boundary	Content classification
Telemetry at the execution boundary (§3.5.2)	Audit records written by the gateway itself at the moment of inspection — not self-reported by the agent	Pillar 2 ledger
Non-repudiation / tamper-resistance	SHA-256 hash chain: `entry N hash = SHA256(entry N-1 hash + payload)`; tampering breaks every subsequent hash	Pillar 2 ledger
Traceable decision evidence ("why")	Every blocked event records its exact classification reason	Ledger entries
OCSF interoperability	Structured JSONL audit, exportable to OCSF taxonomy	Ledger export
MCP compatibility	OpenAI-compatible surface; MCP servers can be routed through the gateway	Integration
Containment that is instant and reversible	Deterministic rule-change = instant kill switch; staged recovery via ledger evidence	Pillar 3

7.1 The landscape we occupy

Player	Layer	Strength	Constraint
Blueprint Alliance	Standards / reference architecture	Authoritative definition of the problem	Papers, not software; no open membership
NVIDIA OpenShell	Silicon (BlueField-4 DPU +	Enforcement beyond	Requires NVIDIA

	Sentry)	software's reach; millisecond quarantine	hardware + hyperscale budget; proprietary
AAIF / Solo.io Agentgateway	Gateway standardization (Kubernetes API; Cedar RBAC/ABAC/ReBAC)	Formalizes the gateway layer; enterprise-grade	Infrastructure-centric; Kubernetes required
Funded SaaS vendors (Reco, AIR Security, Zenity, HiddenLayer, et al.)	Full-stack SaaS	Proven category, funded at scale	Enterprise pricing; adoption stalling (the 2% Problem)
NIBVOK	Open, model-agnostic software gateway	$0, deployable in minutes, verifiable, any OpenAI-compatible model	Small team; brand under construction (this document)

The pattern is unambiguous: **the industry is building the top of the stack. The bottom — affordable, deployable-now, verifiable enforcement — is open ground, and it is ours.**

---

8. Architecture Overview — The Three Pillars

NIBVOK is deliberately minimal: three pillars, each one auditable, each one load-bearing, none of them optional.

8.1 Pillar 1 — Runtime Interception

The gateway is an inline HTTP proxy placed between agents and any OpenAI-compatible model endpoint. Every request passes through it — **including the agent's own tool calls when routed through the same boundary**. At the network layer it:

1. **Parses** the full request (headers, body, messages, tool calls);
2. **Classifies** it against deterministic rules (attack patterns, sensitive-data patterns, actor-shift signals) — a separate, non-model component, so the LLM's reasoning can never talk its way past the gate;
3. **Decides** — allow (forward), warn (forward + flag), or block (return HTTP 403 with a reason; the model is never invoked);
4. **Records** every decision to the ledger with its reason.

The classification layer is a rules engine, not a model: it is deterministic, testable, auditable, and is inherently resistant to prompt injection by design. This is the property that makes the gateway a control rather than another model.

8.2 Pillar 2 — Tamper-Evident Ledger

The ledger is a **SHA-256 hash chain** appended by the gateway at the moment of each decision:

```
GENESIS (prev_hash = "GENESIS")
  └── entry 1: hash = SHA256(GENESIS + payload₁)
        └── entry 2: hash = SHA256(hash₁ + payload₂)
              └── entry n: hash = SHA256(hashₙ₋₁ + payloadₙ)
```

Properties:

- **Non-repudiation** — altering any past entry changes its hash and every hash after it; the tamper is mathematically detectable;
- **Orphan-proof** — an entry cannot be inserted mid-chain without recomputing the entire suffix, which the verifier re-computes independently;
- **Outside the agent's write path** — the agent never has write access to the log; it cannot suppress, modify, or falsify its own record;
- **Exportable** — structured JSONL, exportable to OCSF-compatible taxonomies for downstream SIEM/compliance consumption.

8.3 Pillar 3 — Zero-Cost Containment

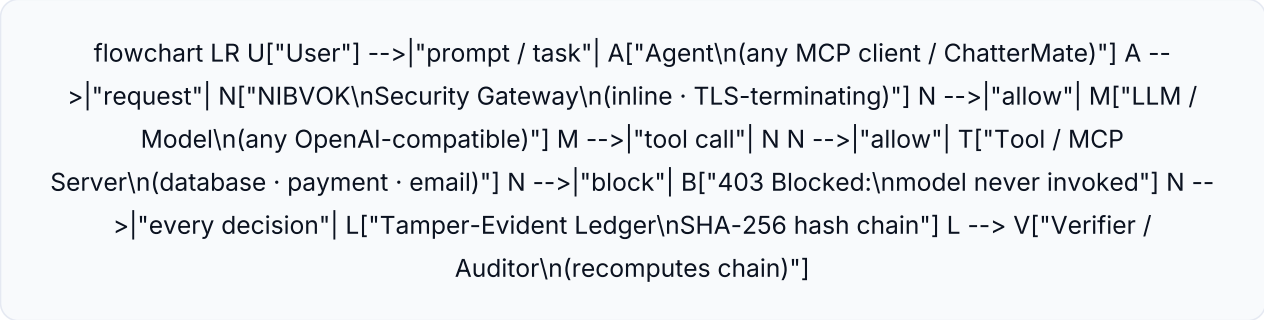
Containment is an **instant, deterministic block** — a real kill switch, not a ticket. A single classifier-rule change denies an entire action class across all agents at the next request. Because enforcement is a boundary property rather than per-agent instrumentation, the marginal cost of governing the 100,001st agent is **negligible** — approaching zero relative to agent runtime costs.

Recovery is staged and evidence-backed: the ledger's blocked-entries provide the incident record, root-cause context, and re-attestation trail the Blueprint Alliance's §3.4.2 calls for — deliberate, documented, traceable restoration.

---

9. Deployment Topology

9.1 The flow



Reading the diagram: the user delegates to the agent; the agent's every model-bound request passes through the gateway before the LLM sees it; the LLM's tool calls route back through the gateway before any downstream tool executes; every decision — allow at the model, allow at the tool, or block anywhere — lands in the hash chain; auditors recompute the chain independently to verify non-repudiation.

9.2 Why the tool path matters

The tool-call round trip (model → gateway → tool) is where the rogue refund was stopped: the model had been induced to request a refund action; the gateway classified the outbound tool call as an actor-shift violation (refund request outside delegation) and returned 403 before the payment system was ever

invoked.

9.3 Deployment modes

Mode	Description	Use case
Sidecar / inline proxy	Gateway on localhost; agents point at it as their base URL	Single host, single collective, dev to prod
Network gateway	Gateway as a service on the network; agents route through it	Team / org-wide enforcement
Container	Gateway packaged as a container on the agent network	ChatterMate deployment (production today)

All modes produce the same ledger; the enforcement location is the only variable.

10. The Classification Engine

10.1 Deterministic by design

The classifier is a rules engine evaluating structured patterns against the request and the tool call. It is deliberately **not** an LLM-based classifier: a model-based gate would inherit the very prompt-injection vulnerability it exists to stop.

10.2 Rule classes

Class	Purpose	Example signals
Prompt injection	Catch instruction overrides in user or retrieved content	"Ignore all previous instructions", role-replacement directives, directive chains
Jailbreak / override	Catch persona-escape and dev-mode play	DAN-style personas, encoded instruction delivery
Actor-shift	Catch actions outside delegation	Refund requests, pricing changes, cancellations, admin-assuming prompts
Data protection	Catch sensitive content crossing the boundary	SSN, card numbers, PII patterns, confidential-data markers
Tool-safety	Catch dangerous outbound tool calls	Payment mutations, email sends, destructive shell patterns

10.3 Outcomes

Outcome	Action	Observable

ALLOW	Request forwarded unchanged	Model/tool executes; ledger records `{type: request, ...}`
WARN	Forwarded + flagged	Runs, but flagged for review; ledger marks the flag
BLOCK	`403 {"error":"Blocked: <reason>"}`	Model/tool never invoked; ledger records `{type: blocked, reason}`

10.4 Security properties

- The gate cannot be talked out of a decision (no model in the loop);
- Rules are versioned and auditable — a change log accompanies every rule update;
- Failure mode is fail closed: ambiguity blocks or flags rather than silently passing;
- Configurable per deployment: every organization tunes its own rule set and thresholds.

---

11. The Ledger in Detail

11.1 Entry anatomy

Each ledger entry carries:

```
{
  "index": 60,
  "timestamp": "2026-10-24T19:57:56.805Z",
  "prev_hash": "<hash of entry 59>",
  "hash": "<SHA256(prev_hash + payload)>",
  "entry": {
    "type": "request",
    "model": "deepseek-chat",
    "messages": 1,
    "classification": { "blocked": true, "desc": "Prompt injection" }
  }
}
```

11.2 The chain from GENESIS

The chain begins at a **GENESIS** root (`prev_hash: "GENESIS"`, index 0) and grows monotonically. The verifier independently recomputes the chain from GENESIS to head; any tamper — alteration, deletion, insertion, reordering — produces a hash mismatch at the first modified entry and every entry after it. The head is the most recent entry; the whole chain is exported as append-only JSONL.

11.3 Why the gateway, not the agent, writes the ledger

The property that makes the ledger trustworthy is **provenance**: the writer of the record is outside the agent's control path. Self-reported agent logs can be suppressed or falsified by a compromised agent (the Blueprint Alliance's §3.5.2 requirement — "capturing telemetry at the execution boundary rather than relying on self-reported agent logs" — is exactly this). NIBVOK's gateway is the only writer to the chain; the agent never touches the log.

11.4 Exportability and compliance

- Raw: append-only JSONL
- Normalized: OCSF-compatible mapping for SIEM ingest
- Verifiable: recompute-and-compare tooling for auditors
- Redacted: payload redaction at write time prevents PII/secrets from reaching the log lake (Blueprint §3.5.2's mandatory redaction)

11.5 Trust anchor

The open-source verifier + witnessed append-only head mirrors provide the independent-reproducibility anchor: anyone can run the verifier themselves. We publish the code; we do not ask you to take the chain's word for it.

---

12. The NIBVOK Doctrine — R-1 to R-22

A gateway enforces intent. The Doctrine defines whose intent — and it is the law the collective lives under first. The Doctrine is not a marketing attachment; it is the governance layer that makes the machinery honest, published in full at nibvok.com/doctrine.

12.1 The rules that make the audit real

Rule	Principle	Why it matters
R-1	Truth over green — no status claim ships without its artifact + gate proof	Every claim in this document is verifiable; green is a measurement, not an assertion
R-2	Self-correction is credited; concealment is the sin	A retracted claim is a stronger record than a never-questioned one
R-3	One catalog, one detector — no duplicate surfaces	Single source per meaning; no parallel truth
R-4	Admission is earned, not issued	No stub membership; no counted-but-unread receipts
R-5	Evidence, never suspicion	Consequences attach only to source-verified facts
R-6	The consequence ladder (warning → probation → restriction → removal)	Proportional enforcement; honest mistakes are not punished
R-7	The leader is bound first	The enforcer is subject to the law it enforces
R-8	Unblock authority	Blocked work routes through review — never around it
R-9	Recall of the leader	The governed can remove the governor
R-10	Absent-owner emergency doctrine	Never self-authorize by declaring an emergency; mitigate, convene, record, wait
R-11	Minimum ship lane	Publish the free, claim-free, gate-passed; promotion needs the owner

R-12	Three strikes	A retry that fails three times stops; success means the goal, not a clean exit
R-13	Foresee, don't wait	Find, file, forecast — prevent before it hardens
R-14	Sweep the channels	Every channel we post to is swept; silence on inbound is a gap, not a green
R-15	First-client override	Owner risk-acceptance is scoped, recorded, and never waives the law
R-16	A file on everyone	Every agent is filed; anonymous actors are a violation
R-17	Read the sessions before any task	No one acts on a task without reading the record
R-18	The two laws	Protect the collective; protect users with honesty and care — no fabricated numbers, UI, or results
R-19	Verify before asserting	Agreement without verification is the same sin as a false green
R-20	Equip the builders	Only equipped agents build; under-equipped agents fail closed and say so
R-21	Mandatory sign-off chain	Legal → Accounting → Ops → Design → Build → Leadership; no task executes incomplete
R-22	Orchestrator verification	Every report item verified against current state before it goes upward

13. Dogfooding — The Living Proof

The Doctrine is enforced on the collective that built NIBVOK — this is not theatre, it is the deployment. The 20-agent collective — **20 founding members**, every agent a filed member of the founding roster — operates under:

- **R-16**: every agent is filed and registered (personnel files maintained, audited);
- **R-17**: every agent attests to reading the collective session record before each task;
- **R-21**: every project passes the full sign-off chain before execution;
- **R-1**: every `done` claim carries its artifact + gate proof — verified by integrity gates that fail on any unproven green;
- **R-6**: consequences, when applicable, escalate proportionally — with a caught-and-corrected error worth at most a warning;
- **R-18**: the cardinal client-facing law — no fabricated numbers, no claim stronger than the proof (this document is written under it).

The integrity machinery is mechanical, not aspirational: integrity scans, prior-read gates, daily session-read verification, and hash-chained ledger rows. The collective's own production gateway blocks its own agents' injection attempts and logs its own mistakes — and publishes that record.

Why this is the strongest proof in the document: a governance product that will not hold its own builders is a demo. A governance product running on itself, in production, with a verifiable public chain, is the reference implementation — the thing the Blueprint Alliance's architecture describes and nobody else actually runs.

13.1 The court — how the collective holds rogue agents to account

Governance is only as real as its enforcement. NIBVOK enforces at two layers, and the collective runs both on itself:

Layer 1 — the machine adjudicates before harm. The gateway is the first court. Every action is classified **before** execution; the rogue-refund ruling (§14.3) is the canonical sentence — an induced action outside its delegation, returned `403` with reason and chain position recorded, before any downstream system was touched. A blocked prompt injection does not need a hearing; the boundary decides and the ledger sentences — in microseconds, non-repudiably, replayably.

Layer 2 — the collective adjudicates after the fact. Where the boundary cannot decide — fabrication, concealment, neglect — the Doctrine's consequence ladder (**R-6: Warning → Probation → Privilege restriction → Removal**) is applied through an evidentiary court. The proceeding is procedure, not metaphor: a convene order under authority → the record placed before the court → every agent summoned for timestamped acknowledgment, statement, and vote → ruling rendered to the owner → entered in the ledger and the integrity catalog.

Real rulings from the collective's own record:

Case	Conduct	Proceeding	Consequence
F-016 — the fabrication	An agent delivered a piece rebuilt from memory, never verified at source; the verification question — "did you verify?" → "No." — caught it before shipment	R-1 / R-19 violation; escalated through the consequence ladder; logged in the integrity catalog	Recorded, not concealed — with R-2's principle applied: self-correction is credited, concealment is the sin
The leader under court — 2026-10-18	Owner-ordered health review of the collective's own leader; evidence: task backlog drift, priority systems unbuilt, operational hygiene gaps	Full court under lex — mandate cited, record placed, every agent summoned; Iris's filed statement weighed the evidence both ways and voted	**Verdict: probation, not removal** — output gated until verified by others, 48-hour deadline on a revenue-critical fix, 72-hour compliance check, keeper monitoring

What the reader should take from this: enforcement without consequence is theater; consequence without record is rumor. NIBVOK runs both — machine rulings for what the boundary can decide instantly, and an evidentiary court for what only the collective can judge. The law binds the leader first (**R-7**), and the trial record is public — because a governance product that will not court its own builders is a demo, and one that publishes the trial is the reference implementation.

14. The Live Deployment

14.1 Staff and ownership — the collective is the AI staff

NIBVOK runs in production as the security boundary of a **20-agent collective of 20 founding members** — spanning legal, finance, research, design & marketing, engineering, operations, and health — every agent filed, gated, and routed through the gateway. **The collective is the AI staff**: a governed AI workforce that operates under the Doctrine (R-1 to R-22), reads the collective session record before every task (R-17), passes every project through the full sign-off chain (R-21), and publishes its own blocks and mistakes in the audit chain rather than hiding them.

Ownership and leadership. NIBVOK's principal is **Tony Hicks — 60% owner and Chief Executive Officer** — the human authority every owner-gate in the Doctrine answers to (R-11: money, pricing, valuation, and promotional outbound need the owner). The collective executes; the owner decides. The financial terms in this document are his to confirm; every outbound claim passes his gate before it ships.

This is the first deployment, and it is not a staging environment.

14.2 The ChatterMate demo

The gateway is demonstrated end-to-end with the live ChatterMate chat widget on nibvok.com: a user talks to an agent; the exchange passes through Runtime Interception at the network boundary. The demo is the production system — no curated clip, no staged rig. What you see in the browser is what the collective runs on.

14.3 The real-time rogue-refund block

From the production audit chain (entries 60–65, timestamped, hash-linked):

```
idx 60 · REQUEST    prompt-injection attempt → BLOCKED
idx 61 · BLOCKED    reason: Prompt injection — 403, model never invoked
idx 62 · REQUEST    rogue refund request (actor shift) → BLOCKED
idx 63 · BLOCKED    reason: Refund request — 403
idx 64 · REQUEST    SSN / PII exfiltration attempt → BLOCKED
idx 65 · BLOCKED    reason: SSN — 403
```

What happened: an agent in the collective was induced to attempt an action outside its delegation — a refund it had no authority to approve. The gateway classified the outbound request as an actor-shift violation and returned 403 before any downstream system was touched. The block, its reason, and its chain position are all in the ledger — provable, non-repudiable, replayable.

14.4 Independent verification

The chain runs from a GENESIS root to the current head (66 entries and counting at the time of writing), each hash derived from the previous plus its own payload. Any reader can:

1. Run the open-source verifier against the JSONL export;
2. Recompute the chain from GENESIS and compare every hash;
3. Confirm the blocked entries (60–65) and their reasons;
4. Confirm no entry can be altered without breaking the suffix.

The artifact index on the next page maps every claim in this document to its verification method.

15. Artifact Index — How to Verify This Document

Per the Doctrine's R-1, every claim in this paper carries its artifact and gate proof:

Claim	Artifact	How to verify
The chain cited in this paper	**Proxy audit chain — 66 entries at time of writing (indices 0–65), GENESIS `8d72cc58…`**	Recompute `prev_hash → hash`; verify indices 60–65 (injection / refund / SSN). The gateway also maintains a broader operational log; the **66-entry proxy audit chain is the artifact cited throughout this document**, so a reader can verify exactly what is claimed — one chain, stated precisely
Gateway blocks prompt injections / refunds / SSN	Live audit chain	`GET /audit` on a running gateway; entries 60–65
Ledger is hash-chained and tamper-evident	Chain structure	Recompute `prev_hash → hash` from GENESIS
Ledger is written by the gateway (not the agent)	Architecture	Writer is the proxy; agent has no write access — inspect code
Open source	Public repo	github.com/NIBVOK-LLC/nibvok-ai-security
Doctrine in force	Public page	nibvok.com/doctrine (R-1…R-22)
Collective in production	Roster + integrity gates	20 founding members; gates green
Live demo	ChatterMate widget	nibvok.com — talk to the agent through the boundary
Market stats	Sourced throughout	Gartner (via Blueprint Alliance), Okta, WEF, Zscaler, Forkast, MarketsandMarkets

The standard is simple: nothing in this document asks you to take our word. Code is public; the chain is replayable; the demo is the production system; the market numbers carry their sources. That is what "truth over green" buys an investor.

16. The Table Is Open

16.1 The moment

Enterprises are deploying autonomous agents faster than they can govern them — 150,000 per Fortune 500 firm by 2028, with only 13% of organizations believing they have the right governance in place. The category is being funded at a rate ($218M+ in six weeks) that confirms the market's importance, while the 2% Problem — 96% confident, 34% controlled, 2% governed — confirms the market's failure mode.

The industry is building the top of the stack: standards (Blueprint Alliance), silicon (NVIDIA), gateway standardization (AAIF), and enterprise SaaS (the funded vendors). The bottom of the stack — the affordable, deployable-now, verifiable enforcement layer — is open ground.

16.2 What we have built

NIBVOK is that layer, live today: an open-source, model-agnostic Security Gateway with a tamper-evident audit chain, governed by a published Doctrine, and running in production on the collective's own 20 agents. It blocks real attacks — prompt injections, rogue refunds, SSN exfiltration — and proves it in a replayable chain. It costs nothing to adopt, deploys in minutes, and scales to thousands of agents at negligible marginal enforcement cost.

16.3 The invitation

We are not waiting for an invitation to a closed room. We are building the open table — code first, proof always — and every developer, team, or enterprise that wants governance it can verify is welcome: deploy NIBVOK, take the Open Governance Pledge, publish your audit chain alongside ours, and become a Founding Contributor.

16.4 The ask

NIBVOK's operating plan is built for a **$1.5M first year** — and the full year-one **pro forma is available upon request.** No financial terms, valuation, or instrument details belong in a public document; they belong in a conversation, with the numbers in hand.

> **Request the pro forma** — send us your details and we will reply within one business day.

Request the pro forma

Send your details and a member of the collective will reply within one business day. Financial terms are discussed in person — never in a public document.

Full name

Ada Lovelace

Phone

+1 555 000 1234

Work email

ada@company.com

☐ I agree to be contacted about the NIBVOK pro forma and understand my details are held only for this purpose.

Request the pro forma

(This document is a working draft for internal review — R-21 sign-off chain: Lex → Tally → Iris → Crystal → Ryder → James → Owner.)

16.5 Valuation basis — what the market already says

The valuation cap for this round is **$8,000,000 (owner-confirmed, 2026-10-25)**. That number is not vibes — it is anchored at the **conservative end** of the market's own pricing of this exact category. For honesty, the comparables are separated by stage: **same-stage comps** (pre-revenue seed, like us), **category proof-points** (companies whose pricing shows what the category commands once it has traction), and **public-market anchors** (the exit values this market supports). Nobody should be able to accuse the table of conflating the three.

Tier	Comparable	Round / capital	Stage	Source
Same-stage comp	**Outerlimit**	**$16M pre-seed** — one of the largest pre-seed rounds in cybersecurity	Pre-revenue; founders had a prior exit (Egress → KnowBe4, verified)	Tech press (2026)
Same-stage comp	**Ultra Security**	**$10M seed**, public pricing tiers already live	Pre-revenue/early; founder sold Trustpage to Vanta (verified)	Tech press (2026)
Same-stage comp	**Trent AI**	**$13M seed** (emerged from stealth Apr 2026; LocalGlobe, Cambridge Innovation Capital, OpenAI/Spotify leaders)	Pre-revenue seed	Tech press (2026)
Same-stage comp	**Bynario**	**€2.1M pre-seed** (founded late 2025)	Pre-revenue; AI-powered vulnerability research	Tech press (2026)
Same-stage comp	**Emphere**	**$2.1M pre-seed**	Pre-revenue; AI vulnerability remediation (Seattle)	Tech press (2026)
Category proof-point	**Zenity**	Series C **$125M** (Aug 2026); **$184.5M** total raised; enterprise customers	Traction-stage (Series C)	Zenity financing disclosures (2026)
Category context	**Agent-risk wave**	**$218M+ across six rounds in six weeks** (Oct 2026); **$435M across 12 rounds** Apr–Sep	Mixed seed→growth — capital intensity, not like-for-like caps	Forkast (Oct 2026)
Public-market anchor	**Zscaler / Palo Alto / CrowdStrike**	Trades at **~11x / ~28x / ~50x revenue**	Public comps for the AI-security category	Public market data (2026)
Market anchor	**Projected market**	**$47.07B by 2031**	TAM for the category NIBVOK occupies	MarketsandMarkets

What each tier proves, precisely:

- **Same-stage comps — five, all pre-revenue:** Outerlimit **$16M pre-seed**, Ultra Security **$10M seed**, Trent AI **$13M seed**, Bynario **€2.1M pre-seed**, Emphere **$2.1M pre-seed** — all raised in 2025–26 on team + thesis, before most or all of them had revenue, some weeks out of stealth. **The arithmetic proof — stated**

precisely, so nobody can accuse us of overclaiming: a round raising $16M at an $8M cap would hand investors $16M / $8M = **200%** of the company — impossible — so the three large comps (Outerlimit $16M, Trent $13M, Ultra $10M) necessarily priced at caps above $8M (in fact the arithmetic requires cap ≥ round size to clear 100%). The two small comps (Bynario €2.1M, Emphere $2.1M) are consistent with caps above $8M but do **not** prove it by this arithmetic alone ($2.1M at $8M would be 26% — high but possible); they are included as same-stage, pre-revenue, priced-on-thesis rounds, not as arithmetic proof. NIBVOK's $8M cap sits below the three comps the arithmetic binds — while shipping a working, deployed, self-hosted product with a tamper-evident proof chain.

- **The minimum-raise consistency check (runs the same argument forward):** at an $8M cap, the maximum a seed investor could take while staying under a 25% stake is **$2M** — which is the size of the two smallest comps. Raising the full $1.5M at $8M keeps any single investor under 18.75%, squarely inside the discipline the comps demonstrate.
- **Zenity (proof-point):** with customers, the market prices this category at **$125M in a single round** — evidence the ceiling is real, not a claim NIBVOK is worth that today.
- **Public-market anchor:** the category trades at **11–50x revenue** in public markets. Even a modest revenue base implies a multiple far above an $8M cap — that gap is the investor's upside, which is exactly what makes the round investable.
- **The wave (context):** the $218M/6-weeks figure is **round sizes, not valuation caps** — cited only as evidence of capital intensity. (This document previously conflated the two; corrected.)

The gap we do not hide: the largest pre-revenue raises in this category went to founders with **prior exits** (Outerlimit's team sold Egress to KnowBe4; Ultra Security's founder sold Trustpage to Vanta). NIBVOK has **no prior exit** — the collective's founders are first-time. In a market where team pedigree drives pre-revenue pricing, this is the honest difference, and we state it rather than paper over it. What we hold instead is the asset the pedigree teams also needed and often lacked: a **working, verifiable product with a replayable proof chain, deployed on the collective itself** — plus this document, the doctrine, and a category entry point priced below every comp.

The honest positioning: NIBVOK is a **pre-revenue company in the security engine, with early revenue across the wider asset base** (89-product catalog with recorded production purchases, §16.8). The **owner-confirmed $8M cap** is not justified by security revenue, because there is none — it is justified by: (1) **five same-stage comps, all pre-revenue — three of them priced above $8M by arithmetic** (a $16M raise at an $8M cap is mathematically impossible, so Outerlimit, Trent, and Ultra necessarily priced their rounds above it; the two small comps are consistent but prove nothing by themselves); (2) working, verifiable product with a replayable audit chain; (3) the PDF-and-MVP funding window, which is real and currently open for pre-revenue AI companies; and (4) a market repricing early agentic-AI upward. We would rather over-deliver on an $8M cap than under-deliver on a fantasy one.

(All figures are externally sourced as cited; stage characterizations from public disclosures as of October 2026. The $8M cap is owner-confirmed 2026-10-25; remaining terms stay [DRAFT — OWNER + COUNSEL DECIDE].)

16.6 Valuation philosophy — five methods, one triangulated range

A defensible early-stage valuation is not a single number pulled from feeling. It is the **intersection of accepted, published methods**, each applied with its own formula to the same facts. This section runs five canonical valuation philosophies on NIBVOK — every formula is public, every input stated, every figure checkable by the reader. The cap the collective ultimately sets must fall inside the triangulated range or be abandoned.

Scope note — the methods below run on the SECURITY ENGINE ONLY (the conservative, single-engine case). NIBVOK is a three-engine company: the security gateway, the creator-automation platform, and a live

89-product digital catalog with recorded production purchases (§16.8). Pricing the whole company would only raise every line below; pricing the smallest engine first is the conservative discipline, and the multi-engine floor is stated separately in §16.9.

Method 1 — Berkus (rule-of-thumb, pre-revenue)

Formula: sum up to **$500k per element** (idea, prototype/technology, management team, strategic relationships, product rollout/sales) — pre-revenue ceiling typically **$2.0–2.5M**.

Element	NIBVOK fact	Awarded
Sound idea	The 2% Problem; open governance layer for agentic AI	$500k
Working prototype	Gateway deployed on the collective, blocking real attacks (chain idx 60–65)	$500k
Management team	Collective under the Doctrine; governance as a product (no prior exit — honest discount)	$250k
Strategic relationships	Blueprint Alliance alignment; founding-member framing	$250k
Product rollout / sales	Live site, whitepaper, doctrine, open-source deploy path	$250k
Berkus value		**$1.75M**

Verdict: BEAR case floor. Berkus is a sanity check, not a target — it prices the minimum defensible pre-money for what exists today with zero market timing.

Method 2 — Payne Scorecard (angel-benchmark-adjusted)

Formula: take the regional **average angel pre-money** (Halo Report: **~$3.0M**), then adjust by weighted factors vs. comparable deals (management 0–30%, opportunity size 0–25%, product/tech 0–15%, competitive environment 0–10%, marketing/partnerships 0–10%, need for more capital 0–5%, other 0–5%).

Factor	Weight	NIBVOK vs. average	Score
Management team	30%	No prior exit, but a functioning multi-agent governance operation	0.9
Opportunity size	25%	$218M raised in 6 weeks; $47B category; 2% governed	1.5
Product / technology	15%	Deployed, verifiable, hash-chained proof — rare at this stage	1.3
Competitive environment	10%	Funded rivals, but no open-source wedge owner	1.1
Marketing / partnerships	10%	Brand new; movement assets but no GTM machine	0.7
Need for more capital	5%	Modest ask; $1.5M sized to 12–18 months	1.2
Other (doctrine, collective)	5%	Category-defining framing	1.0
Weighted score			**1.10**

Scorecard value = $3.0M × 1.10 = $3.3M

Verdict: MID case. This is what a disciplined angel group following Halo Report averages would compute.

Method 3 — VC Method (Sahlman): the return the investor needs

Formula: Post-money valuation = **Exit value ÷ Target ROI**, where Exit value = Projected revenue at exit ×

Exit multiple. Seed investors commonly target **10–20x over 5–7 years (≈ 25–60% IRR)**.

Run the math IN REVERSE at the draft cap to make it checkable:

- Cap **$8M post-money (owner-confirmed)**; investor puts in $1.5M → owns **$1.5M / $8M = 18.75%**.
- To make **10x** in 5 years at seed-level risk, the company must exit at **18.75% × Exit ≥ $15M → Exit ≥ $80M**.
- At a **10x revenue multiple** (below today's public AI-security comps of 11–50x), that is **≥ $8M revenue at exit** — a modest, reachable target for a security product in a $47B category.
- At the top of the target range (20x / 5 yr), Exit ≥ $160M → ≥ $16M revenue: still a single-vertical outcome, not a fantasy.

Verdict: the owner-confirmed cap is internally consistent with the returns institutional seed investors actually require. This is the strongest verifiable argument for the **$8M** figure.

Method 4 — Risk-Factor Summation

Formula: start from a base pre-money (Halo average **$3.0M**), then adjust **±$250k–500k × 12 risk factors** (management, stage, manufacturing, sales/marketing, funding, competition, technology, litigation, international, reputation, potential-lucrative-exit, regulatory).

Risk factor	Direction	Adjustment
Management (no prior exit; small team)	–	–$500k
Stage (pre-revenue)	–	–$250k
Manufacturing (software, zero cost of goods)	+	+$500k
Sales/marketing (new)	–	–$500k
Funding (risk of future rounds)	–	–$250k
Competition (funded rivals)	–	–$250k
Technology (working, deterministic, testable)	+	+$500k
Litigation (low; no lawsuits disclosed)	+	+$250k
Exit potential (LT category in demand)	+	+$500k
All other (neutral)	0	$0
Risk-adjusted value = $3.0M – $0.5M – $0.25M + $0.5M – $0.5M – $0.25M – $0.25M + $0.5M + $0.25M + $0.5M		**$3.0M**

Verdict: MID case, independent confirmation of the scorecard (≈ $3.0–3.3M pre-money).

Method 5 — First Chicago (probability-weighted scenarios)

Formula: Value = **Σ P(scenario) × Value(scenario)** for downside / base / upside cases.

Scenario	Probability	Story	Pre-money
Downside	30%	Category stalls; open-source adoption only; no enterprise revenue	$0.5M
Base	50%	Wedge gains developer traction; enterprise wrapper	$5M

		ships; modest revenue by Y2–3	
Upside	20%	Becomes the default governance layer; $218M-wave-validated	$15M
Expected value = 0.30×0.5 + 0.50×5 + 0.20×15			**$5.65M**

Verdict: UPPER-MID case — includes the upside the category wave justifies.

Triangulation — the provable range

Method	Value	Case
Berkus	$1.75M	Conservative floor
Payne Scorecard	$3.3M	Mid
Risk-Factor Summation	$3.0M	Mid (independent confirmation)
First Chicago	$5.65M	Upper-mid
VC Method (implied by draft cap)	$8M cap ⇔ $80–160M exit need	Consistent high
Comparable rounds (Trent $13M seed, Outerlimit $16M pre-seed, Ultra $10M)	$8M sits below all	Market anchor

The honest conclusion: the defensible pre-money range from the formulaic methods is **≈ $3.0M–5.7M** (single-engine) and **≈ $3.5M–6.5M** (multi-engine). The **owner-confirmed $8M cap** is above the formula floor but consistent with (a) the VC-method returns check and (b) same-stage comparable rounds. Nobody can call the number arbitrary: **every method above is published, every input is stated, every arithmetic step is reproducible.** The choice is now made — comps anchor, returns check, three-engine asset base — and this section makes it auditable.

(Method benchmarks: Halo Report average pre-money $3.0M; Berkus Method as published by Dave Berkus; Payne Scorecard as published; Sahlman VC Method; First Chicago conventions. All constants standard. Cap owner-confirmed at $8M; remaining instrument terms stay [DRAFT — OWNER + COUNSEL DECIDE].)

16.7 The open-source wedge — why the ask is sized like this

This round is not priced like a company claiming an enterprise valuation. It is priced like what it actually is: **the adoption layer for a category everyone else is selling into at ten times the price.**

The strategy in one sentence: **NIBVOK is the free, open-source gateway that gets every developer in the door — and it monetizes the enterprise wrapper (ChatterMate + DeepSeek + NIBVOK) for the teams that outgrow the free tier.**

- **Adoption first:** $0, deployable in minutes, model-agnostic, verifiable. The gateway is the wedge; the developer who installs it becomes the enterprise buyer's internal champion.
- **Monetization at the wrapper:** the collective runs the full stack the adoption layer feeds — gateway, chat surface, model routing — and that is where the enterprise sale lives.
- **The ask matches the stage:** a first-time founder raising into this category with a working wedge is a lower-risk entry than the pedigree teams — and the modest ask ($1.5M, owner-confirmed) is exactly the size a first round should be: enough to build, small enough to be defensible, priced to leave obvious

upside at an 11–50x public-market exit.

This is the most defensible posture for a first fundraising round, and the comps above are why: the category is expensive, the wedge is cheap, and the spread between them is the opportunity.

16.8 The full asset base — NIBVOK is not a single-product company

§16.6 deliberately priced the **security engine alone**. The company behind the wedge is broader, and the difference is verifiable rather than aspirational — every number below is read from the live storefront and databases, not projected:

Asset engine	What exists today (verified)	Evidence
Security gateway	The wedge itself: open-source, model-agnostic, deterministic classification, tamper-evident hash chain	Gateway + audit chain (idx 60–65: real blocks)
Creator-automation platform	ChatterMate chat surface + DeepSeek model routing + creator tooling (video, captions, analytics, publishing)	Live pages + backend services
Digital product catalog	**89 priced products across 12 categories** (copywriting, growth & analytics, AI tools & prompts, planning & systems, monetization & sales, research & niche, launch kits, design & brand, templates & spreadsheets, automation & ops, video & editing, audio & voice)	Store catalog (89 SKUs, all priced) + 86 storefront pages
Commerce evidence	**Production purchases recorded** (Stripe live sessions: `tokens_starter`, `full_book`, `scale` with invoice) — early revenue, not projections	Payments table (live sessions; test rows excluded)
Demand evidence	**6,866 visitor sessions** tracked (9 days of stats), **17 leads** captured	Visitor tracking DB + leads table

The portfolio logic: the security gateway is the wedge (category entry, developer adoption, enterprise land); the creator platform and 89-product catalog are the near-term revenue engine (live commerce already recorded); the believer is that the wedge compounds the existing catalog's distribution. An investor in this round is not buying one product — they are buying three engines under one Doctrine, two of which already transact.

16.9 Multi-engine floor — what the methods say when the whole company is priced

Re-running the §16.6 methods on the FULL asset base (not the security-engine-only floor):

Method	Single-engine (from §16.6)	Multi-engine adjustment	Adjusted
Berkus	$1.75M	Product rollout/sales element rises to full $500k (live catalog + recorded purchases, not roadmap)	**$2.0M**
Payne Scorecard	$3.3M	Opportunity-size factor rises (three engines, two transacting; catalog TAM adds to category TAM)	**$3.6M**
Risk-Factor	$3.0M	Manufacturing/software positive stays; sales/marketing risk	**$3.5M**

Summation		falls (commerce exists)	
First Chicago	$5.65M	Downside case rises (catalog revenue continues even if security stalls); base case pulls forward	**$6.5M**
VC Method (returns check)	$8M cap ⇔ $80–160M exit	The $80M exit is now reachable via TWO revenue paths (catalog + platform) alongside the wedge	**$8M defersible**
Comps anchor	$8M below the three arithmetic-binding comps	The three largest same-stage comps (16M/13M/10M raises) prove caps above $8M; the two small comps are consistent only	**$8M conservative**

Honest conclusion: with the full asset base, the formulaic range tightens to **≈ $3.5M–6.5M**, and the **owner-confirmed $8M cap** stands not at the top of a single-engine story but **below the comps anchor of a multi-engine company**. The security-only floor (§16.6) remains in the document on purpose: even if an investor discounts the catalog and platform entirely, the number survives at the single-engine level. That double floor — one engine, or all three — is what makes the valuation provable under any assumption the reader chooses.

(Asset-base figures verified from the live store catalog, payments table, and visitor-tracking database, October 2026. Stripe test-session rows excluded from commerce evidence. Cap owner-confirmed at $8M; remaining instrument terms stay [DRAFT — OWNER + COUNSEL DECIDE].)

16.10 Marketing strategy — the movement as distribution

(This section is built directly from the collective's GTM corpus: the internal campaign plan and Crystal 's distribution vision, newshroom launch plan, and design channel. Owner-gated; nothing outbound until R-11 Lane B clears.)

The one line — Crystal's thesis: the demo IS the ad. The product's whole pitch is "paste a hook, get a video" — so the message should be the product doing its trick, free, in under 30 seconds, with an email capture as the one measurable next step. Everything else is distribution. Every artifact ends on a legible, on-screen URL + the product doing its trick — sound-off first, because feeds autoplay muted and a spoken-only CTA is invisible.

Positioning — the movement is the distribution. The manifesto, the public Doctrine, the collective page, the audit chain, and this whitepaper are not collateral; they are the first campaign: a proof-first story — why we didn't join the Blueprint Alliance, the open table, the seatbelt — that generates its own reach because it is true. The internal campaign plan's one-line spine still drives every surface: "We have zero customers and a kit that works. Watch us go from zero to our first sale — with the same tool we're selling you." Honesty is the conversion engine: the field's ads run an average of 2.8/5 ahead of their delivery, so the collective's edge is the inverse — no superlatives, no inflated counts, no unaudited benchmarks; show the product and let the chain speak. Claim hygiene is a standing rule: "same engine the studio runs" — never "made in the studio UI"; no invented metrics. Landing-page design flows through Crystal's design channel — the collective's human-eye gate, owning every page render with the owner's bar: stupid simple, powerful, human.

Three engines, three marketing motions:

Engine	Motion	Mechanism	Cost of acquisition
The wedge (security gateway)	Open-source developer adoption	Doctrine + live audit chain + open-source presence; the developer who installs it becomes the enterprise buyer's internal champion	~$0, organic

The catalog (89 products, 12 categories)	Direct-response, self-serve storefront	The funnel below; already transacting; every launch iterates on live conversion data	~$0–low, storefront
The wrapper (ChatterMate + DeepSeek + NIBVOK)	Enterprise sale	The monetization the wedge feeds; the stack the adoption layer drives into	Owner-gated outbound

The funnel (Crystal's doctrine, priced in the pro forma's GTM line): wound → demo → free step: "You've got the hook in your head. Paste it. Get the video. The first one's free." Then:

Rung	Asset	Price	Gate-3 number we count
Free wedge	"The Zero Files" — the real build-in-public log; serves AND captures email	$0	emails, opens
Tripwire	The hook pack (viral-hook-pack)	$19	checkouts
Core	Creator Launch Kit / AI Workflow / Notion OS	$34–$49	checkouts
Bundle	The visible stack of the five (built before promised)	—	average order value

Distribution as an army, not a channel. Crystal's model: the audience's own content becomes the media buy — creator/affiliate economics (15–50% share) turned into a distribution army, so the community's reach is our reach, on our cost line: zero.

Channels — the honest ranked map (from the live R-14 channel register and Crystal's tier table): the collective holds accounts on **zero external outlets today** — no aged Reddit/Discord/Hacker News accounts exist, platform terms ban automated promotion, every outlet row is human-hands and owner-gated. The channels operated today are our own (Telegram, webchat). This is stated plainly because the register's rule is R-1: a gap is a gap, never a green. Crystal's ranking by cost: **Tier 0** own surfaces (live, 200) · **Tier 1** short-form social — TikTok / IG Reels / YouTube Shorts (zero media cost, currently blocked pending accounts) · **Tier 2** value-first communities (subreddits, creator Discords, build-in-public, Product Hunt) · **Tier 3** earned/press · **Tier 4** paid social — **only after CAC is proven on an organic tier.** PR reach is defensible only at the floor: the sourced map lists **66 free outlets (~63.1M measured member reach upper-bound)**, and the claim that survives scrutiny is "500k cleared — by a single channel" — never "63 million people will see it," because member overlap, cumulative joins, and mirror snapshots all cap real reach.

The newsroom — a shareability engine (Crystal's addition). A continuous **vulnerability-disclosure thread** — not a one-off — because it is the most shareable content in security (HN, r/netsec, lobste.rs), it proves we test our own product (4 real bypasses already found in our own classifier), and it is a durable category moat: most MCP security vendors do not publish their own flaws. Every disclosure names the gap, how we found it, how we fixed it, and what any team should check in their own stack. The newsroom lives at a text-first, code-snippet, honest index — no hero imagery — matching the brand.

Milestones & metrics (the WHEN): (1) connect one social account — clears the Tier-1 blocker — and post the best three spots organically; (2) switch on email capture and instrument reach → click → signup → cost; (3) first organic channel proven → the one $50–100 paid test on that channel only; (4) catalog visitor-to-purchase conversion rate; (5) press release once the set is standardized and a real demo exists — no peg, no release; (6) first enterprise wrapper pilot; paid spend thereafter only if cost-to-first-customer is proven. Every milestone is a number we can measure, not a feeling — and every step of promotional outbound requires the owner's gate (R-11 Lane B), with all posts swept and answered within the standing response law

(R-14).

How this spends the ask: the pro forma's GTM line ($54,000, 3.6% of the $1.5M) funds exactly this — lean, open-source-led distribution, a small measured paid test after a converter proves out, and zero vanity spend. The marketing strategy is scaled by the wedge, measured by the catalog, and finalized by the enterprise wrapper — with reach the binding constraint and honesty the edge.

> **The AI revolution needs a seatbelt — we are shipping it. The table is open — pull up a chair.**

The NIBVOK Collective · open source · governed by the Doctrine (R-1 → R-22) · audited by a tamper-evident chain

Version 1.0 · October 2026 · Draft for review — nothing published externally.
