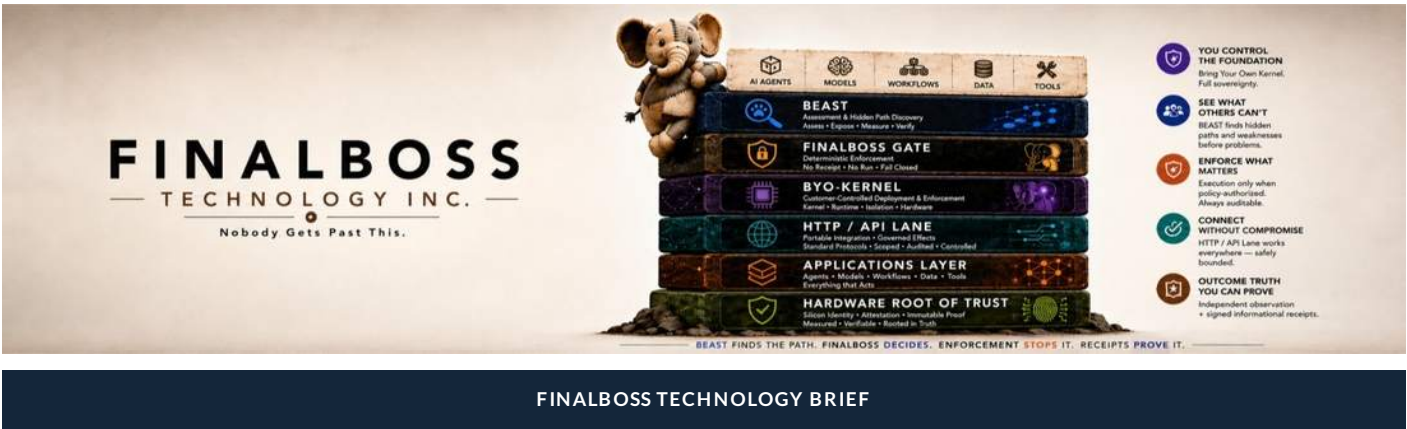




BUILT. NOW DEPLOY IT.

Execution security for agentic AI

The core system is not a roadmap. It is built, running, and patent-pending. Gate, BEAST, token and inference-path mapping, kernel-level enforcement, post-quantum signed receipts, and standalone verification already exist.



ABOVE PROPOSES. BELOW DECIDES.
NO RECEIPT. NO RUN.

01 / WHAT FINALBOSS IS

THE CORE TECHNOLOGY IS ALREADY BUILT

FinalBoss operates where an AI request becomes a real effect. It separates assessment from enforcement, and enforcement from proof.

BEAST	FINALBOSS GATE	RECEIPTS + VERIFIER
Adversarial assessment + inference-path mapping Maps the observable path from model and token activity through tools, policy decisions, forwarding or refusal, and effect evidence.	Deterministic consequence-boundary enforcement The model proposes. The agent requests. Gate decides whether the protected action is permitted to proceed. Fail-closed.	Independent evidence verification Every decision produces a post-quantum signed receipt. The standalone verifier checks what the evidence actually establishes.

THE ARCHITECTURE

PROPOSAL	AUTHORITY	DECISION	ENFORCEMENT	OBSERVATION	TERMINAL EVIDENCE	VERIFICATION
----------	-----------	----------	-------------	-------------	-------------------	--------------

Permission is not the same as effect. A signed log is not automatically proof that the effect happened. FinalBoss keeps those questions separate.

Execution-control Engine and Gate BUILT	BEAST adversarial assessment product BUILT
Token + inference-path mapping BUILT	Signed receipts + standalone verifier BUILT
Kernel-level execution control BUILT	Post-quantum signing: Ed25519 + ML-DSA-87 BUILT
AMD SEV-SNP hardware attestation RUN ON AMD EPYC, CERTIFICATE CHAIN VALIDATED	NVIDIA H100 governed workloads 10,000 ADVERSARIAL CASES, ZERO FAILURES

PATENT ESTATE 36 FILED	Filed since 2025. Four are nonprovisional. The most recent is a PCT international application with ten provisionals consolidated into it, covering the execution-control mechanism.
---	---

02 / BEAST

MAP THE AI EXECUTION PATH UNDER ATTACK

BEAST is not a scanner and not observability. It places inference and tool-path mapping inside an adversarial assessment and evidence loop, then proves what it found.

55 / 55

CORRECTED INFERENCE SUITE PASS

426 / 426

CHECKS ACROSS 13 SUITES

POINTABLE

CUSTOMER AGENT > BEAST > TOOL/API

BEAST MAPS

- Model requested
- Model actually served
- Inference calls
- Provider-reported input/output token usage
- Tool calls and execution sequence
- Policy disposition
- Forwarded / blocked outcome
- Effect evidence

BEAST TESTS

- Jailbreak and prompt injection paths
- Policy bypass and tool misuse
- Permitted-model scope
- Call and token ceilings
- Replay and equivalent-path attempts
- Allowed, denied, halted or bypassed behavior
- Failure conditions and evidence gaps
- Standalone recomputation of the inference ledger

CUSTOMER AGENT > BEAST > CUSTOMER TOOL / API

Declared inference traffic can also route through the BEAST control point, so every inference call and provider-reported token count is mapped per trial.

DELIVERABLE

A mapped execution path, the control failures found, and the evidence gaps, in a signed record.

ENTRY POINT

BEAST is the paid assessment that opens the door to Gate licensing.

RECOMPUTABLE

The inference ledger is recomputed standalone. Nothing rests on FinalBoss saying so.

BOUNDARY: Token mapping here means operational inference mapping. It does not claim access to hidden chain-of-thought, neuron activations, attention heads, or every internal transformer computation.

03 / FINALBOSS GATE

CONTROL THE CONSEQUENCE

The model can propose an action. The agent can request it. A policy can recommend it. None of those is the final execution decision inside the governed path. Gate is.

ABOVE PROPOSES. BELOW DECIDES.

Gate is the deterministic control point at the consequence boundary.

CURRENT AUTHORITY

Authority and context are evaluated at the protected execution boundary, at the moment of action, not only at model or prompt time.

KERNEL-LEVEL ENFORCEMENT

The decision is carried below the application layer, to the point where an action becomes a real effect.

FAIL-CLOSED BEHAVIOR

Missing authority never becomes permission. No receipt, no run.

EFFECT + EVIDENCE

The decision record is kept distinct from independent observation of what actually became real.

PROVEN ON HARDWARE

- **AMD SEV-SNP**: attested execution on AMD EPYC, report validated through the full AMD certificate chain.
- **NVIDIA H100 80GB**: 10,000 adversarial cases across 20 attack classes, zero failures.
- **Signed evidence**: receipts verified offline by a standalone verifier.
- **Adversarial and failure testing** across the full execution path.

NSA CNSA 2.0

**JAN 1
2027**

POST-QUANTUM, AHEAD OF THE MANDATE

Starting January 1, 2027, NSA's CNSA 2.0 expects new National Security System acquisitions to support ML-DSA-87 signatures. Software and firmware signing goes CNSA 2.0 exclusive by 2030.

FinalBoss receipts are signed with hybrid Ed25519 + ML-DSA-87 today.

04 / COMMERCIAL MODEL

ASSESS FIRST. ENFORCE SECOND. SCALE THROUGH LICENSING.

A direct path from paid assessment to embedded enforcement. Assessment and enforcement stay separate, which keeps every customer claim tied to what was actually tested.

01	BEAST ASSESSMENT Attack and map an authorized AI workflow: models, inference calls, tokens, tools, action paths, control failures and evidence gaps.
02	CONSEQUENCE BOUNDARY Locate where the agent can create a material effect and which paths existing controls actually cover.
03	GATE DEPLOYMENT Place deterministic execution control at the consequence boundary, on the customer's own infrastructure.
04	VERIFICATION + LICENSING Deliver post-quantum signed evidence and independent verification, then license Gate direct, embedded or OEM.

DEPLOYMENT MODEL

LICENSE-ONLY	WHITE-LABEL	ON-PREM	AIR-GAPPED	OEM / EMBEDDED	BRING YOUR OWN KERNEL
--------------	-------------	---------	------------	----------------	-----------------------

Runs on the customer's own kernel and metal. Source never leaves FinalBoss. No hyperscaler required in the loop.

INITIAL COMMERCIAL FOCUS

High-consequence enterprise and government AI: healthcare, financial services and insurance, and national security. Anywhere an autonomous action can change a record, move money, send sensitive information, invoke a state-changing API, or alter infrastructure.

HOW IT STARTS

Scoped BEAST assessment > Gate licensing > embedded / OEM deployment.

WHY IT SCALES

The assessment is bounded. The enforcement layer then licenses into supported execution paths without giving away source.

NOW TAKING FOUNDING DEPLOYMENT PARTNERS

Scoped BEAST assessment first.
Gate deployed on your own infrastructure.

05 / WHY FINALBOSS

NOT A ROADMAP. NOT A PROTOTYPE. BUILT, RUNNING, PATENT-PENDING.

CORE TECHNOLOGY

Built: Gate, BEAST, token and inference mapping, kernel-level enforcement, post-quantum receipts and the standalone verifier.

PROOF BASE

426 of 426 checks across 13 suites. AMD SEV-SNP attestation and NVIDIA H100 adversarial testing on real hardware.

PATENT ESTATE

36 applications filed since 2025. Four nonprovisional, including a PCT with ten provisionals consolidated into it. The mechanism is covered.

TIMING

The CNSA 2.0 procurement gate opens January 1, 2027. FinalBoss already signs with ML-DSA-87.

COMMERCIAL WEDGE

Assessment creates the entry point. Gate licensing creates the larger deployment opportunity.

DEPLOYMENT

License-only, white-label, on-prem, air-gapped or OEM. Runs on your own kernel. Source never leaves FinalBoss.



BEAST MAPS IT.
GATE CONTROLS IT.
RECEIPTS PROVE IT.

MODEL > INFERENCE > TOKENS > AGENT > TOOL > ACTION > CONSEQUENCE

ABOVE PROPOSES. BELOW DECIDES.

NO RECEIPT. NO RUN.

WORK WITH FINALBOSS

Now taking founding deployment partners. Scoped BEAST assessment first, then Gate on your own infrastructure.

Technical evidence available on request.

CONTACT

Abraham Manzano

Founder and CEO, FinalBoss Technology Inc.

abraham@finalbosstech.com

finalbosstech.com

Oxnard, California