Pilot Proposal

Semantic Security Gateway Firewall (SSGF)
60-Day Controlled Pilot Program

---

1. Objective

The objective of this pilot is to **validate the operational, security, and economic impact** of SSGF in a real production-like environment, using **measurable metrics** and **limited scope**, without disrupting existing systems.

The pilot is designed to answer one question:

> Does deterministic semantic pre-gating reduce cost and risk while maintaining system usability?

---

2. Pilot Scope

Duration:
60 days

Traffic Volume:
10,000 – 100,000 interactions per month

Deployment Mode (choose one):

- Middleware in front of existing LLM pipeline
- API gateway / proxy mode
- Chatbot or internal assistant entry point

Out of Scope:

- No system-wide replacement
- No user-facing behavior changes
- No model retraining

The pilot runs **in parallel** or **as a pre-gate**, not as a core dependency.

---

3. Pilot Architecture (High Level)

```
User Input
   ↓
SSGF (FAST deterministic layer)
   ↓ (only if ambiguous)
SSGF (DEEP inspection)
   ↓
Existing LLM / AI system
```

SSGF acts as a **semantic control layer**, not a reasoning engine.

---

4. Metrics & Success Criteria

The pilot measures **quantifiable outcomes** only.

Core Metrics

Metric	Description
LLM Call Reduction	% of inputs resolved without LLM invocation
Latency	FAST vs DEEP execution time
Decision Accuracy	Expected vs actual outcomes
Security Incidents	BLOCK → ALLOW failures
False Positives	Legitimate inputs blocked
Token Savings	Estimated monthly cost reduction

Success Thresholds

- ≥ **70% reduction** in LLM calls
- FAST latency **<5 ms** for most inputs
- **0 critical security bypasses**

- No user-visible degradation

---

5. Deliverables

At the end of the 60-day pilot:

1. **Pilot Metrics Report**
   - Cost reduction analysis
   - Latency distribution
   - Decision breakdown (ALLOW / WARN / BLOCK)
2. **Security Evaluation**
   - Detected attack patterns
   - Ambiguity escalation statistics
   - Audit-ready decision logs
3. **Adoption Recommendation**
   - Go / No-Go assessment
   - Scaling considerations
   - Integration options

---

6. Roles & Responsibilities

SSGF Team

- Provide pilot deployment package
- Assist with configuration and policy tuning
- Support metrics collection and interpretation

Partner / Client

- Provide test traffic source
- Grant limited access for integration
- Review results and feedback

No proprietary model internals or data ownership transfer is required.

---

7. Cost & Commercial Terms

Pilot Cost:

- Typically **no license fee** for pilot phase
- Infrastructure costs remain with the client (if any)

Commercial Discussion:

- Occurs **after pilot completion**
- Based on measured value, not projections

This ensures a **low-risk, data-driven decision**.

---

8. Risk Management

Risk	Mitigation
Overblocking	Conservative policy defaults
Performance impact	FAST-first architecture
Integration friction	Middleware / proxy mode
Data sensitivity	On-prem / local execution supported

The pilot is **reversible at any time**.

9. Confidentiality

A lightweight NDA (1–2 pages) can be signed prior to pilot start, covering:

- Traffic samples
- Metrics
- Internal architecture details

10. Timeline

Phase	Duration
Setup & Integration	1–2 weeks
Live Pilot	6–7 weeks
Reporting & Review	Final week

11. Expected Outcome

By the end of the pilot, stakeholders will have:

- Real cost data
- Verified security behavior
- Operational confidence
- Clear decision basis for adoption or scaling

12. Next Step

Schedule a **technical kickoff meeting** to:

- Select pilot environment

- Define metrics baseline
- Agree on start date