

— SOLUTION OVERVIEW



Synapse: Secure AI Coding Ecosystem

Context

Federal agencies are eager to harness autonomous, agentic AI software development processes to accelerate software development lifecycles (SDLC) across digital domains.

The Problem

Commercial and open-source agentic software development tools create severe compliance and security risks in government networks:

- **Lack of Federal Hardening:** Commercial tools, such as Codex and Cursor and open-source tools, such as OpenCode and Cline, were not engineered for federal security constraints or air-gapped deployment.
- **Guardrail Bypass:** Existing agentic harnesses frequently drop or bypass security controls when model context windows fill up during long sessions.
- **Audit Deficiencies:** Lack of immutable auditing creates non-repudiation and data leakage risks when connecting agents to internal APIs and repositories.

The Solution

Synapse is a hardened agentic software development harness built on open-source OpenCode, hardened with enterprise security controls for federal information systems.

- **Interceptor & Governance Layer:** Implements administrative model access controls, deterministic regex filtering, and AI/ML classifier adaptors to enforce policy guardrails.
- **Immutable Audit Persistence:** Formats all prompts, outputs, and agent actions in OpenTelemetry, cryptographically signs logs, and streams them to Write Once Read Many (WORM) storage (e.g., Azure immutable storage).
- **Cost Control & Compression:** Features intelligent context compression, cost analytics, and automatic model routing (e.g., Bedrock, Azure AI Foundry, GENAI.MIL, self-hosted).

Differentiation

- **Gov-First Security & Compliance:** Built from the ground up to support federal non-repudiation, custom LLM routing, and disconnected, air-gapped environments.
- **Shift-Left Local Enforcement:** Unlike cloud based solution such as AWS Bedrock Guardrails that use consumption based pricing and require data to leave local development devices, Synapse enforces controls natively on the local machine to provide full data sovereignty and cost savings.
- **Intelligent Interceptor Layer:** Every request to a LLM is evaluated at an interceptor layer that applies robust controls, with adaptors for AI/ML based filtering, to prevent data exfiltration and provide secure interactions.

Your mission is our commitment

Contact us at build@bridgephase.com to inquire about working together.