System Context Diagram: Code Guardian

Developer

JavaScript/TypeScript developer using VS Code for secure coding

Writes code, triggers analysis, reviews findings, applies fixes

Privacy Boundary: All source code analysis stays within localhost

Visual Studio Code

[IDE Platform]

Provides extension host, editor API, diagnostics UI, and language services.

Document events, language services, diagnostics API

Code Guardian

[VS Code Extension + Local Backend]

Privacy-preserving vulnerability detection and repair assistant. Analyzes JavaScript/TypeScript code locally, provides real-time diagnostics, explanations, and fix suggestions.

Code snippets + prompts (localhost:11434) ← JSON findings

Ollama LLM Runtime

[Local LLM Inference]

Hosts local models (qwen3, gemma3, CodeLlama). Runs on localhost:11434.

Query embeddings ← Retrieved CWE/CVE knowledge chunks

Local Vector Database

[ChromaDB / Qdrant]

Stores CWE/OWASP/CVE knowledge embeddings for RAG retrieval.

[Optional] Fetch public vulnerability metadata (no source code sent)

CVE/NVD APIs

[External APIs - Optional]

Public vulnerability metadata for knowledge base refresh. Disabled in offline mode.

Legend:

Code Guardian (main system)

External system
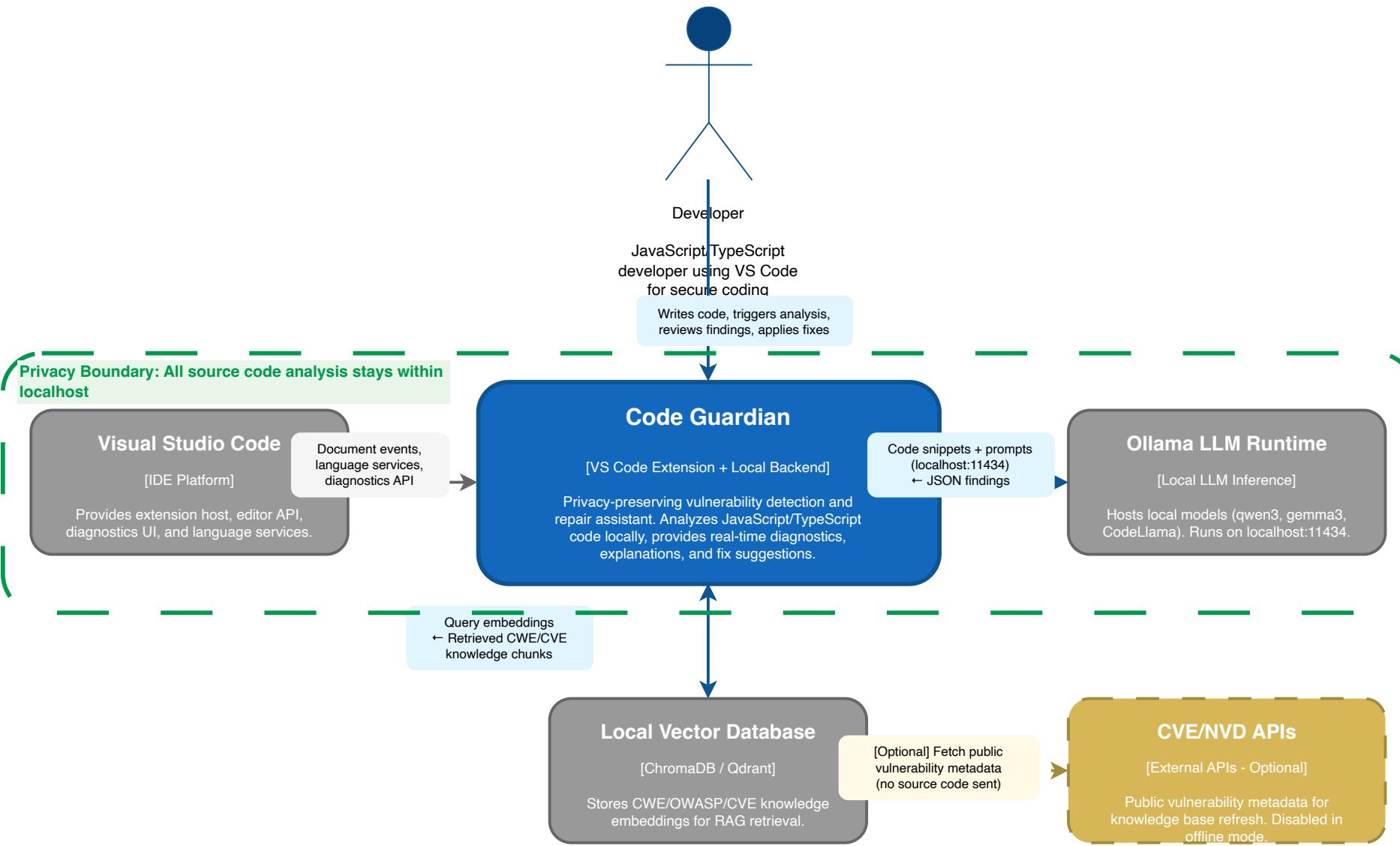
Optional/external

Note: Code Guardian operates entirely within the developer's local machine. Source code is never transmitted to external APIs.
Optional CVE/NVD refresh fetches only public vulnerability metadata and can be disabled for fully offline operation.