

bulletproof-prd- platform — System Overview

Full-stack architecture for the end-to-end
Product Requirements Document lifecycle.

From abstract concept to approved artifact.

bulletproof-prd-platform is a full-stack web application designed to manage the **entire lifecycle** of a PRD, pairing a **Next.js App Router** front end with a Postgres data layer and local AI CLI integrations.



Six Dedicated Workspaces



Brainstorm

Chat with Claude to explore concepts. The assistant extracts themes, which can be promoted directly to ideas, research prompts, or draft PRDs.



Ideas Board

Capture, tag, and triage ideas. Seamlessly promote any valid idea into a formal draft PRD.



Research

Fan out a single prompt into seven parallel Gemini queries (standards, security, UX, competitors, pitfalls, integration, best practices). Live results stream via Server-Sent Events.



PRDs

Central dashboard to manage documents, create blank drafts, or upload existing .md files (title extracted from first # heading).



Editor

Tiptap v3 WYSIWYG editor featuring markdown round-tripping, auto-save, and numbered version history.



Reviews

Comprehensive validation gating. Features AI executive summaries, duplication scans, threaded comments, and content security scans.

The Technology Stack

Client Layer

Next.js 16 / React 19: Server components and App Router.
Styling & UI: Tailwind CSS v4, shadcn/ui.
Editor: Tiptap v3 (lowlight syntax highlighting, tables, images).



Server / API Layer

Runtime: Node.js 20+, executing Route Handlers (REST & SSE).
Processing: unified ecosystem (remark / rehype / turndown) for robust markdown conversion.



Data Layer

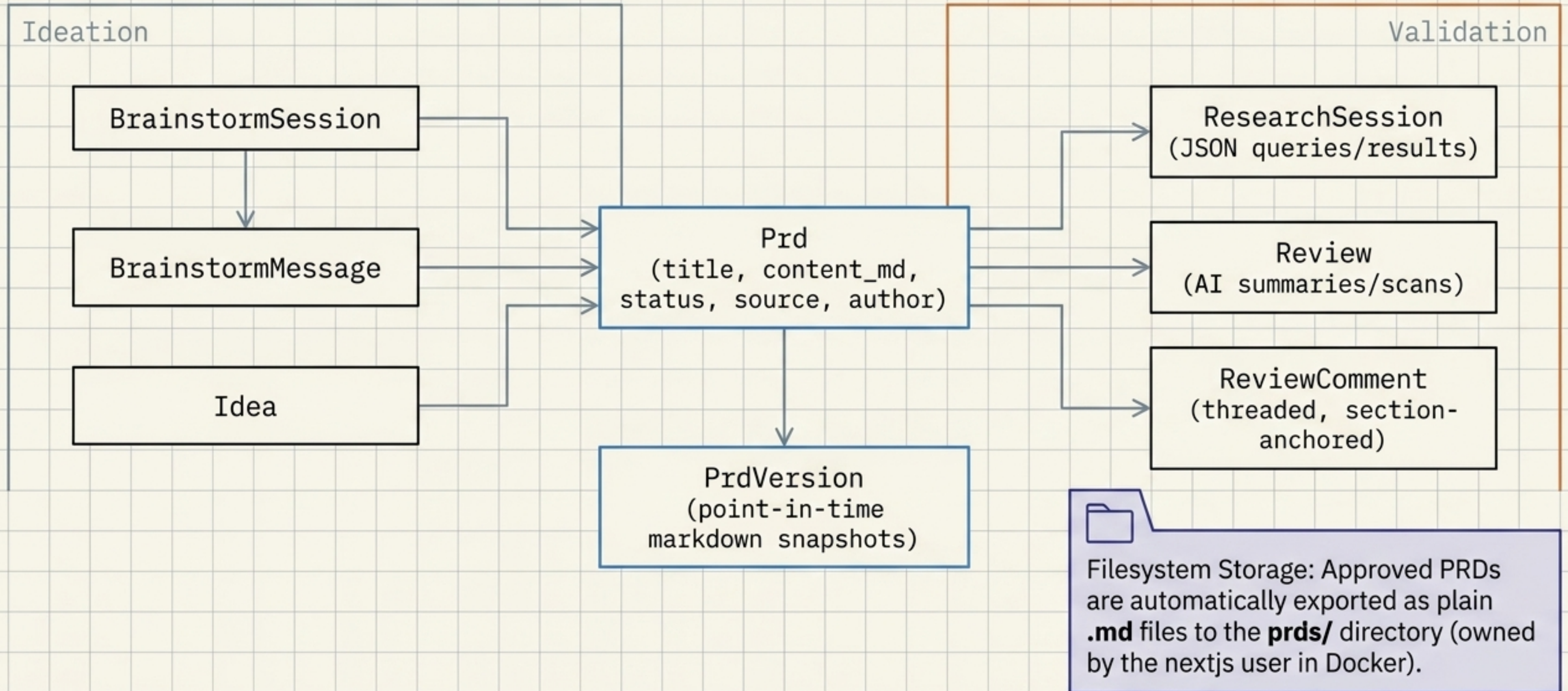
ORM: Prisma 7 utilizing the @prisma/adpater-pg driver adapter.
Storage: PostgreSQL Database.



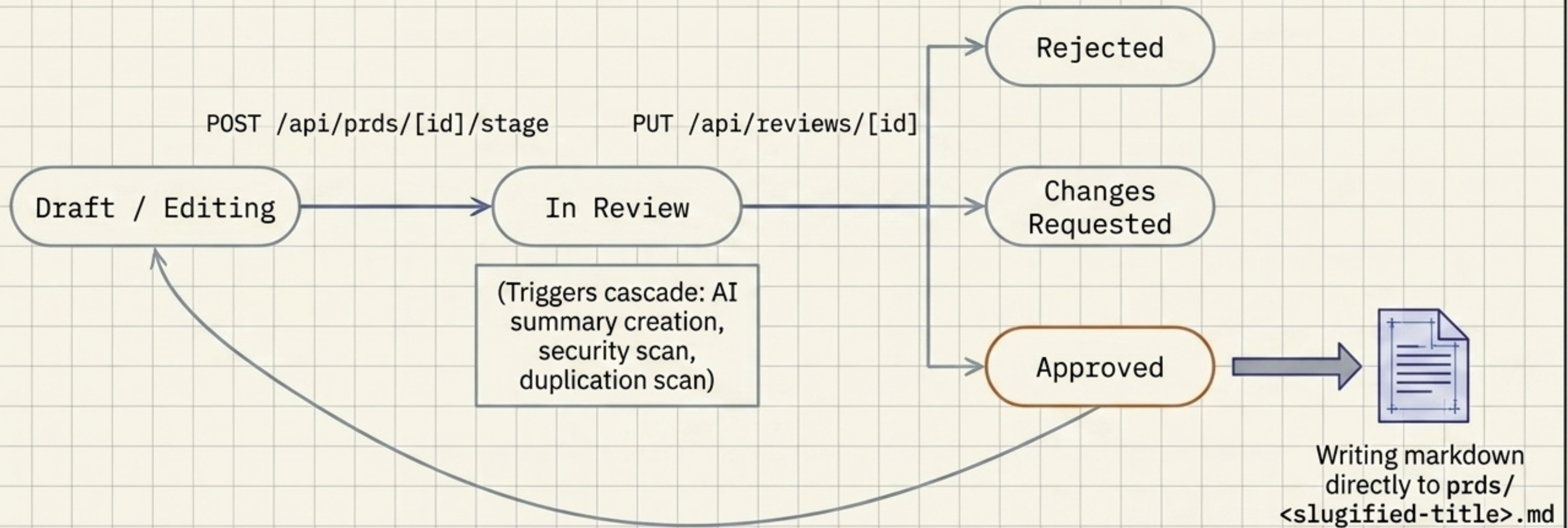
External / AI Layer

Execution: Local Claude CLI and Gemini CLI binaries for generation and research processing.

Relational Data Model (prd_platform schema)



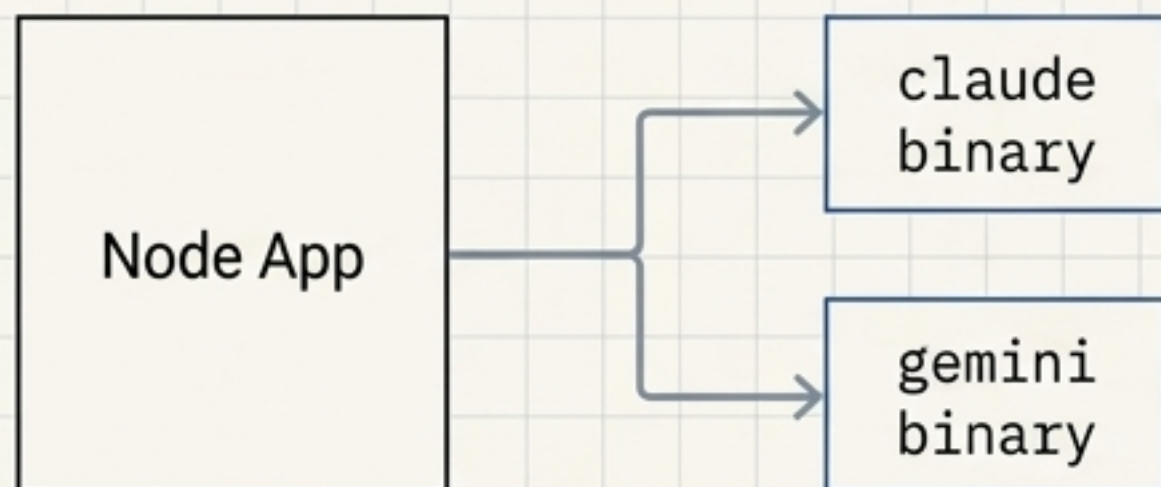
Document Lifecycle & State Machine



AI CLI Runtime Topology

Managing host-level CLI access securely across deployment models.

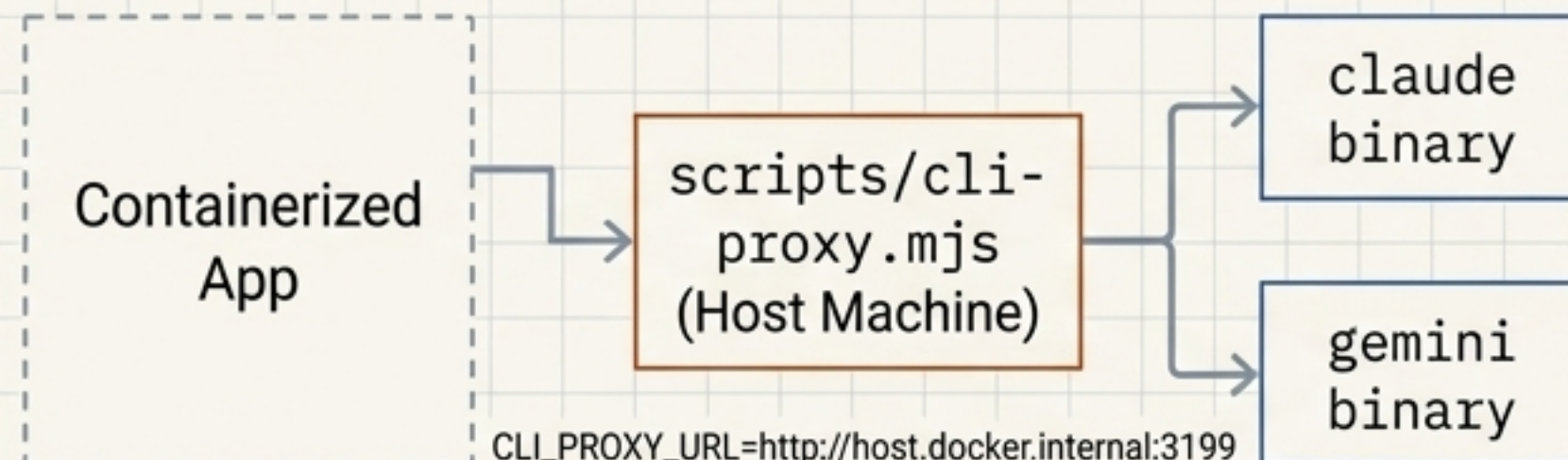
Local Execution



Node App directly executes claude and gemini binaries on the system PATH.

Condition: CLI_PROXY_URL is unset.

Docker Execution



Containerized App cannot reach host binaries natively. Traffic routed via proxy on the host machine, which accepts JSON POST requests and executes the local CLIs.

❗ **Technical Callout:** The proxy is a minimal stdlib-only HTTP server with a 10 MB output buffer. It enforces strict timeouts (Claude: 120s, Gemini: 60s). It is unauthenticated and must remain bound only to trusted local container networks (0.0.0.0:3199).

Operations & Governance

Configuration (Env)

DATABASE_URL

Required. Throws on startup if missing. Must include `?schema=prd_platform`.

CLI_PROXY_URL

Enables Docker proxy routing.

GOVERNANCE_PLUGIN_PATH

Path to a Python threat detector (`governance.lib.llm_threat_detector` or). Scans degrade gracefully to zero findings if missing.

Security Posture



- Assumes a trusted single-tenant deployment (author defaults to 'local'). Shared use requires an external auth proxy.
- Zero critical/high dependency vulnerabilities tracked. Zero gitleaks secrets findings.

Maintenance & Upgrades



Backups: `pg_dump --schema=prd_platform`

Upgrade Path:

1. `git pull`
2. `npm ci`
3. `npx prisma migrate deploy`
4. `npm run build && npm run test:run`
5. Restart service.