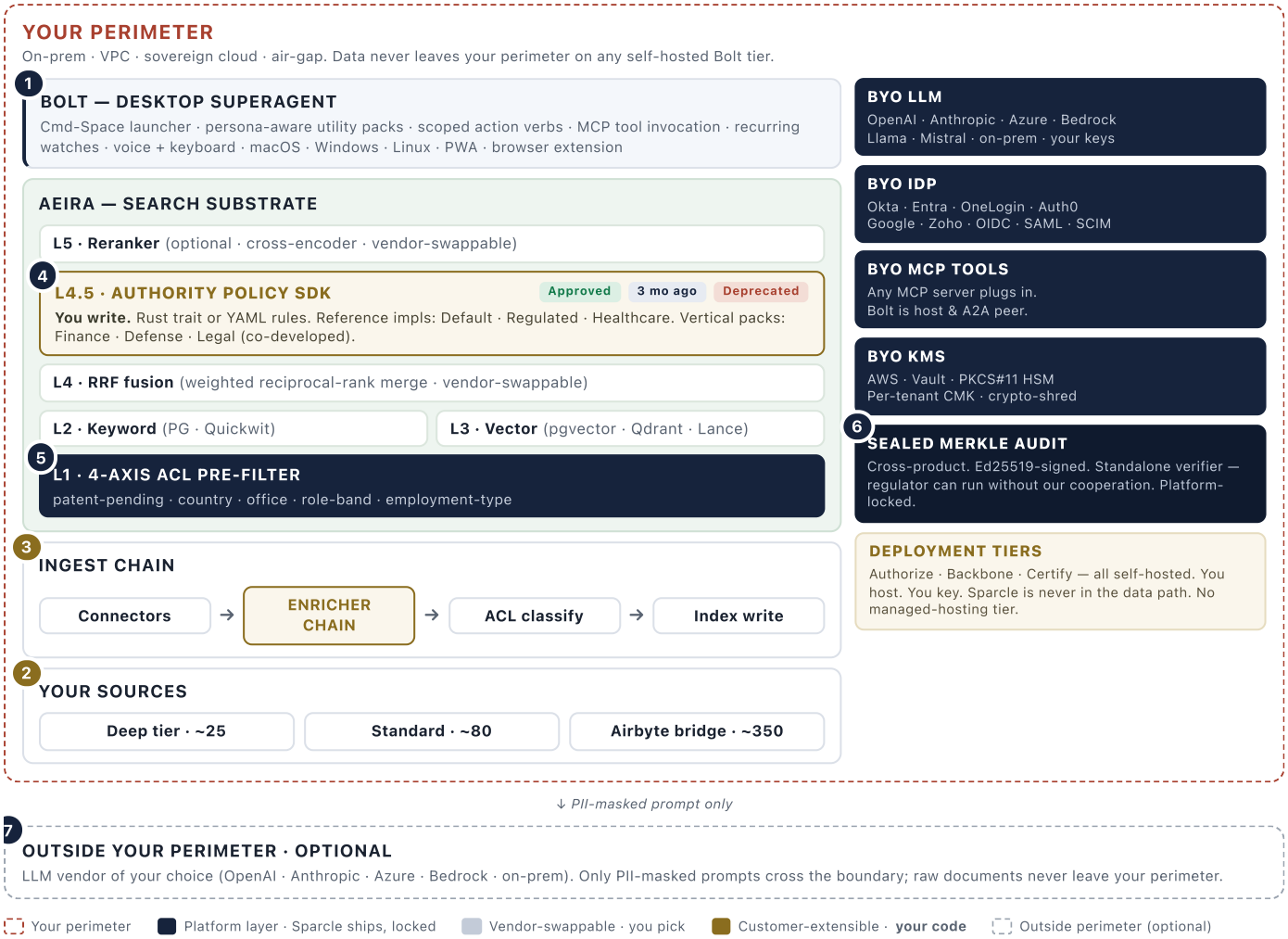
Your search. Your policy. Your code.

Bolt + Aeira inside your perimeter, with the Authority Policy SDK on top.

Architecture overview · how the three layers compose



HOW IT WORKS · 7 LAYERS

Numbered to the diagram. The architecture, layer by layer.

1. **Bolt — desktop superagent.** Cmd-Space launcher runs on the user's own desktop. Queries are identity-bound. No data leaves the machine to start the search.
2. **Three connector tiers.** Deep-integration sources (~25) preserve source-fidelity ACL plus per-source enrichment. Standard in-house connectors (~80). Airbyte bridge (~350) for long-tail breadth. Depth matters where your domain authority signals live.
3. **Enricher chain at ingest.** Per-source rules pull domain metadata into authority signals. **FHIR evidence levels, classification markings, regulatory-source tiers.** Your domain knowledge enters the search index through this channel.
4. **Authority Policy SDK.** The customer-extensible ranking layer. Reference impls ship for general enterprise, regulated industries, and healthcare. Vertical packs for finance, defense, and legal are co-developed by engagement. The trust model is written in customer code (Rust trait or YAML rules) and runs inside the customer perimeter.
5. **Patent-pending 8-axis ACL.** Country, office, role-band, and employment-type pre-filter at index time. The ACL layer is platform-locked. The Authority Policy ranks on top, on documents the ACL already authorized.
6. **Sealed Merkle audit chain.** Every query, every result, every score, every policy decision. Ed25519-signed. A standalone verifier binary lets an auditor or regulator verify the chain independently, without vendor cooperation.
7. **BYO everything.** LLM, IdP, MCP tools, KMS. Customer choice at every external boundary. Outside the perimeter, only PII-masked prompts cross to the customer-chosen LLM vendor. On every self-hosted Bolt tier, Sparcle is not in the data path.