

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

YOUR PERIMETER

On-prem · VPC · sovereign cloud · air-gap. Data never leaves your perimeter on any self-hosted Bolt tier.

1

BOLT — DESKTOP SUPERAGENT
Cmd-Space launcher · persona-aware utility packs · scoped action verbs · MCP tool invocation · recurring watches · voice + keyboard · macOS · Windows · Linux · PWA · browser extension

AEIRA — SEARCH SUBSTRATE

L5 · Reranker (optional · cross-encoder · vendor-swappable)

4

L4.5 · AUTHORITY POLICY SDK

Approved3 mo agoDeprecated

You write. Rust trait or YAML rules. Reference impls: Default · Regulated · Healthcare. Vertical packs: Finance · Defense · Legal (co-developed).

L4 · RRF fusion (weighted reciprocal-rank merge · vendor-swappable)

L2 · Keyword (PG · Quickwit)

L3 · Vector (pgvector · Qdrant · Lance)

5

L1 · 4-AXIS ACL PRE-FILTER
patent-pending · country · office · role-band · employment-type

3

INGEST CHAIN

Connectors → ENRICHER CHAIN → ACL classify → Index write

2

YOUR SOURCES

Deep tier · ~25Standard · ~80Airbyte bridge · ~350

BYO LLM
OpenAI · Anthropic · Azure · Bedrock
Llama · Mistral · on-prem · your keys

BYO IDP
Okta · Entra · OneLogin · Auth0
Google · Zoho · OIDC · SAML · SCIM

BYO MCP TOOLS
Any MCP server plugs in.
Bolt is host & A2A peer.

BYO KMS
AWS · Vault · PKCS#11 HSM
Per-tenant CMK · crypto-shred

6

SEALED MERKLE AUDIT
Cross-product. Ed25519-signed. Standalone verifier — regulator can run without our cooperation. Platform-locked.

DEPLOYMENT TIERS
Authorize · Backbone · Certify — all self-hosted. You host. You key. Sparcle is never in the data path. No managed-hosting tier.

↓ PII-masked prompt only

7

OUTSIDE YOUR PERIMETER · OPTIONAL
LLM vendor of your choice (OpenAI · Anthropic · Azure · Bedrock · on-prem). Only PII-masked prompts cross the boundary; raw documents never leave your perimeter.

Your perimeter Platform layer · Sparcle ships, locked Vendor-swappable · you pick Customer-extensible · **your code** Outside perimeter (optional)

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 impl 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 4-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.

Sovereign enterprise AI — inside your perimeter, with your LLM, on your audit trail, ranked by your policy.

sparcle.app