FOR: DEFENSE / DIB · CUI · ITAR · CLASSIFIED-ADJACENT

AI inside the wire.

Enterprise AI for the Defense Industrial Base — air-gap deployable, ITAR-compatible, CUI-aware, no outbound telemetry.

> *Your contracts forbid sending CUI to a third-party cloud. Glean, Hebbia, Harvey, and Microsoft Copilot all require it. Your analysts and engineers still need fast cross-source search and agentic workflows. Today they get neither.*

CUI residency

"Where does CUI go when an analyst searches across SharePoint, Jira, and ServiceNow?"

Sparcle: Nowhere outside the CUI enclave. Bolt + Aeira deploy inside the network boundary you already maintain. **No outbound traffic to Sparcle. No telemetry, no phone-home, no vendor-side log aggregation.** The audit trail is yours.

ITAR + export control

"How do we prevent a non-US-person from inadvertently retrieving export-controlled tech data?"

Sparcle: 8-axis ACL with `country` and `office` axes built into the index. Documents tagged ITAR-controlled are pre-filtered at index time — a non-US-person's query never sees the candidate set. Every decision provable in the audit chain.

Air-gap operation

"Can your software run in an environment with no internet access at all?"

Sparcle: Yes. The trial sidecar is a single signed binary with embedded Postgres. Production Helm pulls only from your internal registry. **BYO LLM** for on-prem inference (Llama 3.3, Mistral, Qwen, custom). No phone-home, no auto-update — you control update cadence.

What ships today vs what ships during a 90-day pilot

Air-gap-deployable Rust workspace, no outbound network calls	SHIPPED
8-axis ACL with `country` + `office` axes	SHIPPED
BYO LLM — on-prem (Llama / Mistral / Qwen / custom) or sovereign cloud	SHIPPED
Per-tenant CMK via HashiCorp Vault or AWS KMS	SHIPPED
Per-tenant CMK via PKCS#11 HSM	ROADMAP
Sealed Merkle audit chain + standalone verifier binary	SHIPPED
103 connectors built; source-fidelity ACL live on 6 today, backfill per pilot	SHIPPED
Late-bind permission check on top-10 sources	PILOT
CMMC L2 / IL5 / FedRAMP authorization	NOT HELD

Why we're the only viable choice in classified-adjacent work

1. **Glean, Hebbia, Harvey, Microsoft Copilot are SaaS-only.** No version of any of them runs in an air-gapped enclave. If your contract prohibits SaaS, none of them can bid.
2. **No Sparcle-managed sub-processor, in any tier.** Every Bolt tier is self-hosted, so your CSO does not add Sparcle to the third-party risk register as a data processor; the software runs inside your perimeter and no data reaches Sparcle.
3. **Source-code escrow available at pilot tier.** If Sparcle disappears, your deployment survives. SaaS competitors' shutdown leaves you stranded mid-contract.

> **Recommended deployment:** any self-hosted Bolt tier — **Authorize**, **Backbone**, or **Certify**. All are fully customer-hosted inside your enclave, run on your own on-prem LLM, and send zero outbound traffic to Sparcle. There is no Sparcle-managed hosting tier; nothing runs on Sparcle infrastructure.

Brief us in 30 minutes. Demo in your own enclave in 60 days.

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

sparcle.app/defense · bolt@sparcle.app · v2 · 2026-07