

Productivity superagent. *Sovereign by construction.*

*One interface for every system you have access to — instant, identity-aware, within your boundary. Any integration, any tool, any agent, any LLM. **Do more with less. Less clicks, tabs, apps, time, LLM tokens and cost** — without trading privacy or sovereignty.*

Empower (Workforce) · **Govern** (Integrations) · **Audit** (Access).

FOR THE WORKFORCE

One palette, every system. Instant. Identity-aware. Productivity with or without tokens.

FOR THE CISO / CIO

BYO LLM, IdP, MCP. On-prem, VPC, or air-gap. In every self-hosted Bolt tier, no Sparcle component in the data path.

FOR AUDIT & COMPLIANCE

Sealed Merkle audit chain. Crypto-shred for right-to-erasure. Controls by construction.

- Self-hosted & air-gap-capable
- Patent-pending: ACL · audit chain · crypto-shred
- 3 USPTO provisionals · more in preparation
- No Sparcle servers in the data path (every self-hosted tier)
- Productive day one · with or without LLM tokens
- Identity-aware end to end · OIDC · SAML · MCP · A2A

FROM

Sparcle LLC

bolt@sparcle.app · sparcle.app

01 / 12

A BRIEF FROM

Brief · for a first conversation

Bolt + Aeira

Millions paid. Hundreds of tools. The workforce still loses *hours, every day.*

Hundreds of SaaS apps. Each promised easier work. Together — they made it harder, adding a context-switching tax on every role.

~28%

of a knowledge worker's week is spent **searching for information**. At \$100K loaded cost → ~\$28K/yr reclaimable per worker.

► MCKINSEY GLOBAL INSTITUTE

250+

SaaS apps per average enterprise — ~half see **no monthly use**.

► GARTNER RESEARCH

~60%

of business decisions made with **stale or partial information**.

► FORRESTER

\$4.4M

average cost of a single data breach. **Highest in healthcare & finance.**

► IBM COST OF A DATA BREACH 2025

€5.6B+

cumulative GDPR fines since 2018. **Enforcement keeps accelerating.**

► EDPB / GDPR ENFORCEMENT TRACKER 2025

~30%

of breaches involve a **third-party in the data path**.

► VERIZON DBIR 2025

Spending on tools went up. Tokens are sky-rocketing. Yet productivity, privacy, and compliance remain *more challenging than before* — and modern AI is making it worse.

Responsible AI adoption. With what you *already pay for*.

Productivity, sovereignty, governance. Every enterprise wants all three — the industry asks them to pick two.

PATH 1 • SAAS AI

Modern AI. *Lost sovereignty.*

- ✓ Modern AI productivity
- ✗ Your data, their cloud
- ✗ Vendor in the data path
- ✗ Privacy is an SLA promise
- ✗ Audit is logs you must trust

PATH 2 • ON-PREM ONLY

Sovereign. *And slow.*

- ✓ Sovereign data
- ✗ Dumb tools, little or no AI
- ✗ Workforce drag continues
- ✗ “Air-gap” means outdated
- ✗ Compliance via human process

PATH 3 • SPARCLE

Both. *No trade-off.*

- ✓ Modern AI productivity — with or without LLM tokens
- ✓ Your data, your perimeter — on-prem, VPC, or air-gap
- ✓ BYO LLM · no LLM-vendor lock-in. Self-hosted tiers keep Sparcle out of the data path entirely
- ✓ Privacy is cryptographic, not contractual
- ✓ Audit chain a regulator can verify independently

*For decades, knowledge workers across every industry have struggled with the same drag — **tools that don’t talk, context that doesn’t travel, decisions made on stale information.** Modern AI promised relief and quietly shipped a new tax: rising token bills and data leaving the perimeter. We built Bolt and Aeira on an **intelligent architecture** that lets every organization adopt AI as a daily driver — **without sacrificing data privacy, without exploding LLM token costs, and without re-buying what they already have.** Do the work that matters. Reduce cognitive fatigue. Stay sovereign.*

Superagent on top. Substrate *underneath.*

Bolt = the surface your workforce lives in. Aeira = the substrate that makes it defensible.

► BOLT PRODUCTIVITY SUPERAGENT

Access. Search. Automate. *Agentially.*

One interface for every system you have access to · multi-OS · multi-surface

◇ Access	One palette across local, cloud, Aeira, and enterprise indexes — only what your identity is allowed to see
◇ Any LLM	BYO model + keys. Admin gated. Lock which model the org uses, by role.
◇ Any tool	Any MCP server plugs in — Bolt is a hub. 8 enterprise auth modes.
◇ Any agent	Bidirectional A2A peer — orchestrate or be orchestrated. OpenAI-compatible.
◇ Automate	Schedule, watch, trigger — recurring reports, reminders, watch-and-respond, unattended
◇ Data privacy	You control. No sensitive data crosses the boundary. Audit, govern, restrict — org-wide.
◇ Anywhere	Wherever your workforce works — macOS, Windows, Linux, browser, mobile, command-line
◇ Your boundary	On-prem, VPC, or fully air-gapped on self-hosted tiers — data stays inside your perimeter.

► AEIRA ORG KNOWLEDGE, UNLOCKED

Sovereign by *construction.*

Your answers, buried across 40 systems — one corpus, access-controlled per identity

◇ One corpus	Finance, contracts, secure access-controlled corp data, docs, wikis, code, tickets, CRM, HR — plus your existing connectors
◇ ACL	Patent-pending 4-level pre-filter, at the index, not post-retrieval
◇ Identity	Visibility maps to your IdP groups — automatically. No manual permissioning.
◇ Encryption	Per-tenant CMK + envelope encryption + signed integrity
◇ Erase	Crypto-shred for HIPAA / GDPR / DPDPA right-to-erasure — works on WORM
◇ Audit	Sealed Merkle chain, KMS-signed — auditors verify independently
◇ Two modes	Instant retrieval (no LLM, zero token cost) or reasoned synthesis (agentic)

Productive with or without *LLM tokens.*

QUERY

“Find my Q4 deck”

Local + remote + Aeira / your corp → 0
tokens

QUERY

**“Now in Tokyo” · “EUR-
USD” · “Free meeting
room”**

=tz · =fx · =room utilities → 0 tokens

QUERY

**“Summarize last week’s
calls, draft a reply”**

Reasoning required → LLM tokens

Bolt’s **first-class integrations** — search, files, utilities, clipboard, apps, slash commands — carry **70–90% of daily work at zero LLM tokens**. The model is the *last resort*, not the first. **Fewer clicks. Less time. Less tokens. Smaller bill. Less PII surface.** Time reclaim alone pays for Bolt — token savings are the encore.

Every answer carries *its receipts*.

GENERIC

“Find my Q4 deck”

Q4 Sales Deck.pptx

Drive · Marketing folder

Updated 2 weeks ago

Approved

For your audience

Default pack: freshness, approval, audience.

HEALTHCARE

“Latest hypertension treatment guideline”

Hypertension Management — Tier 1 Guideline

Clinical Library · Cardiology

Clinical guideline

CME current

Authoritative source-of-record

Healthcare pack: evidence ladder, CME currency.

DEMOTED

“Expense policy”

Expense Policy v3 (2023)

Confluence · Finance space

Retired policy — do not cite

Regulated pack: retired policies sink below the cut.

Authority Policy SDK ships three reference packs out of the box — **Default** (universal signals), **Regulated** (industry compliance), **Healthcare** (clinical evidence ladder). Customers extend or write their own in Rust + YAML; trust scoring runs inside your perimeter, on the substrate you already control. *Your search. Your policy. Your code.*

Sensitive data, *protected at the call.*

TOOLS

See the *real values*.

Function calls receive unmasked data — so the action actually works.

THE MODEL

Sees *masked tokens*.

PII / PHI / financial values pseudonymized before any LLM call — in both directions.

THE AUDIT LOG

Stays *PII-free*.

Tokens are tenant-isolated and reversible only inside your perimeter.

Layered detection across **three pluggable engines**: **regex** for structured patterns (SSN, IBAN, credit card, MRN, employee IDs), **GLiNER / Microsoft Presidio / your own NER sidecar** for unstructured free-text PII and PHI, and **Tesseract or any OCR you already run** for image & document text. Even when using a frontier public model, sensitive values never reach it.

BYO everything. *In your perimeter.*

MODEL

BYO *LLM*

OpenAI, Anthropic, Gemini, Llama, local, your own — admin-gated by role.

IDENTITY

BYO *IdP*

OIDC, SAML 2.0, SCIM. Okta, Azure AD, Keycloak, Ping — or yours.

TOOLS

BYO *MCP*

Any MCP server plugs in. Bolt is also a host & A2A peer.

DEPLOYMENT

Self-hosted · *air-gap*

Helm chart. On-prem, VPC, or fully air-gapped. Self-hosted by default.

Self-hosted by default — All Bolt tiers, Authorize / Backbone / Certify, run in your perimeter with no Sparcle component in the data path. (There is no Sparcle-managed hosting tier; every tier is self-hosted.) Open protocols (OIDC, SAML, MCP, A2A, OpenAI-compatible) at every external boundary. **Bolt picks what you already have** — LLMs, embeddings, rerankers, PII engines, OCR. Nothing is replaced unless you want it replaced. **For procurement on self-hosted tiers: not a critical vendor on your TPRM list, no LLM concentration risk, no BAA needed for Sparcle.**

Cryptographic. *Not contractual.*

AUDIT CHAIN

Sealed *Merkle*. KMS-signed.

Ed25519-signed roots, rotated nightly.
Bitcoin-style integrity tree.

RIGHT-TO-ERASURE

Crypto-shred. *Works on WORM*.

Destroy the key → record is
unrecoverable. HIPAA / GDPR / DPDPA
defensible.

ACCESS CONTROL

ACL *at the index*.

Patent-pending 4-level pre-filter.
Restricted docs cannot leak via counts.

A regulator verifies any audit root using **only the published algorithm and the raw events** — no trust required in Sparcle code.
Evidence-grade, not SLA-grade.

Controls *by construction*.

Frameworks aligned. Standards adopted. Controls implemented — all inside your perimeter.

► FRAMEWORKS ALIGNED

What you can defend.

- ✓ **HIPAA / HITECH · HITRUST CSF** — PHI handling, audit, erasure
- ✓ **GDPR · DPDPA** — right-to-erasure (§15) by crypto-shred
- ✓ **SOC 2 · ISO 27001 / 27701** — security & privacy baseline
- ✓ **EU AI Act · NIST AI RMF · ISO 42001** — AI governance & transparency
- ✓ **PCI-DSS · GLBA · DORA** — financial data & operational resilience
- ✓ **MAS TRMG · OSFI · CERT-In** — data residency, multi-jurisdiction
- ✓ **FedRAMP / IL4 · CMMC · NIST 800-171** — gov / defense / CUI handling
- ✓ **ITAR / export-aware** — sovereign, air-gap-capable deployment

► STANDARDS ADOPTED

What you can verify.

- ✓ **Identity** — OIDC, SAML 2.0, SCIM
- ✓ **Crypto** — AES-256-GCM, Ed25519, KMS envelope
- ✓ **Primitives** — FIPS 140-3 eligible
- ✓ **API auth** — OAuth 2.1, HMAC-SHA256, RFC-9457
- ✓ **Observability** — OpenTelemetry, Prometheus
- ✓ **Open protocols** — MCP, A2A, OpenAI-compatible
- ✓ **Deployment** — Helm 3, OCI, Kubernetes

► CONTROLS IMPLEMENTED

What you can audit.

- ✓ **Identity-aware retrieval** — ACL at the index
- ✓ **PII / PHI pseudonymization** — at LLM and external boundaries
- ✓ **Human-in-the-loop (HITL)** — approval gates on risk-classed actions
- ✓ **Central admin hub** — provisioning, model & tool gating per role
- ✓ **Sealed Merkle audit chain** — KMS-signed roots
- ✓ **Per-tenant CMK** — crypto-shred for erasure
- ✓ **Sandboxed agents** — path / command allowlists
- ✓ **Rate limit · circuit breaker · DLQ** — per MCP
- ✓ **Cryptographically-verifiable provenance**

List is representative, not exhaustive. Detailed control mappings available on request. In every self-hosted Bolt tier, no Sparcle-hosted component sits in the data path.

We don't *have* a cloud.

DIMENSION	BOLT + AEIRA	GLEAN	MICROSOFT COPILOT	OPENAI ENTERPRISE
What it reduces	Clicks · tabs · open apps · time · LLM tokens · cost — all down	Adds a search surface; tokens per query	Adds a chat sidebar; M365-tier tokens per chat	Adds a web chat; tokens per message
Daily drivers	Unified surface — local + 1P & 3P apps, utilities, secure clips, notes, files, devices, AI, automation, and more	Enterprise search only	M365 chat sidebar	Web chat only
Pluggability	BYO at every layer — LLM, IdP, MCP, embeddings, PII, OCR	Some BYO at edges	Microsoft stack	OpenAI stack
Where the data lives	Customer infra — on-prem, VPC, or air-gap	Glean Cloud (VPC retrofit)	Microsoft Cloud (tenant)	OpenAI Cloud
LLM choice	BYO — any model (frontier, local, on-prem)	Glean-selected	Microsoft-curated	OpenAI only
Tokens cost	0 tokens on 70–90% of work — LLM only when reasoning is needed	Every query routes via LLM	Every chat = M365 tier tokens	Every chat = LLM tokens
PII at the LLM call	Masked — both directions	None native	Tenant scope only	Contractual only
Audit chain	Sealed Merkle · KMS-signed · auditor-verifiable	SaaS audit logs	M365 unified log	Vendor logs
Right-to-erasure	Crypto-shred (works on WORM)	Deletion (best-effort)	Deletion	Deletion
ACL enforcement	At the index (pre-filter)	Post-retrieval filter	M365 permissions	None
Air-gap deployable	Yes	No	No	No

Next steps.

Four shapes — from a 7-day free trial to a year-long design partner. Scoped, measurable, independently useful.

SHAPE 1 · FREE TRIAL

7 days · no commercials

Trial inside your boundary.

Plug Bolt into your **IdP via OIDC** (Microsoft 365, Google Workspace, Okta, Azure AD, any OIDC) — **data stays on device, you keep your AI keys**. Or sign in with Gmail / Outlook / Zoho via **Sparcle ID** for the quickest first look.

[sparcle.app/download](#)

► CISO + CFO + IT · TRIAL IN YOUR OWN PERIMETER

RECOMMENDED START

SHAPE 2 · PILOT

90 days · founding terms

Cohort. Quarter. Measurable.

Bolt to a small cohort (10–50 users), with **optional Aeira** for governance. Success metrics agreed up front — **token delta, time reclaimed, audit posture**. Founding-customer pricing.

► CIO + CFO + WORKFORCE LEAD · MID-TO-LARGE ENTERPRISE

SHAPE 3 · AEIRA EVAL

30–180 days · eval pricing

Aeira under what you run.

Slide Aeira's governance substrate beneath an existing AI workload. **Sealed audit, crypto-shred, ACL at the index**. Eval team only, no production change. **Discounted evaluation pricing** for the trial period.

► CISO + AUDIT + DPO · REGULATED INDUSTRIES

SHAPE 4 · DESIGN PARTNER

6–12 months · deep

Locked terms. Roadmap influence.

Multi-quarter partnership. **25% off list, locked 24 months, direct roadmap influence**, joint case study. For enterprises ready to anchor on Sparcle as their sovereign AI platform.

► CEO + BOARD LEVEL STRATEGIC ADOPTERS

Flexible, risk-free and collaborative. Our success depends on delivering the value and making you successful with Bolt and Aeira.
bolt@sparcle.app