ARCANA RESEARCH

Vendor Security Brief

For IT, security, and procurement review. Effective April 24, 2026.

Purpose. Confidential B2B research panel. Voluntary self-reported data on enterprise AI investment, adoption, and impact. No consumer data, no payment data, no PHI. Hosted entirely in the United States on SOC 2 Type 2-attested infrastructure.

01 DOMAINS TO ALLOWLIST

```
arcana-research.com
*.arcana-research.com
```

Suggested category: Business / Research / IT.

Outbound from your network: HTTPS only (TCP 443).

02 DATA SCOPE

WE DO COLLECT

- Work email, name, employer, job title
- Self-reported research responses (AI investment, adoption, vendor use)
- IP address, user-agent, session timestamps

WE DO NOT COLLECT

- Consumer or end-user data
- Financial accounts, payment cards, SSNs
- Health, biometric, or government IDs

03 SECURITY POSTURE

- TLS 1.2+ in transit; AES-256 at rest
- bcrypt password hashing (cost factor 10)
- Password policy rejects common / breached entries and email-equivalent passwords
- Login rate-limit: per-IP + per-email (anti credential-stuffing)
- Server-side sessions, httpOnly + Secure cookies, 7-day TTL
- Daily cron purges expired sessions and rate-limit rows
- Single-use, time-bound invite tokens
- Audit logs retained 90 days minimum
- IR runbook with 72-hour notification; annual pen test from 2026
- No advertising trackers, no cross-site pixels

04 SUBPROCESSORS (US-HOSTED)

Provider	Function	Region	Compliance
Vercel	Application hosting, edge network	US	SOC 2 Type 2 · ISO 27001
Turso (libSQL)	Application database; password hashes and session records	US	SOC 2 Type 2
Supabase	Secondary storage for portal content	US	SOC 2 Type 2 · HIPAA-eligible
Resend	Transactional email delivery	US	SOC 2 Type 2
PostHog	First-party product analytics (US Cloud)	US	SOC 2 Type 2 · HIPAA-eligible
Inngest	Background job orchestration	US	SOC 2 Type 2
Anthropic	LLM inference for research synthesis	US	SOC 2 Type 2 · zero data retention by contract
Google (Gemini)	LLM inference for research synthesis	US	ISO 27001/27017/27018 · SOC 2/3

05 COMPLIANCE

SOC 2: Type 1 readiness in progress; Type 2 audit window 2026

GDPR / UK GDPR: SCCs available; DPA at /legal/dpa

CCPA / CPRA / VA / CO / CT: Full DSR workflow

Vendor questionnaires: CAIQ Lite available; SIG Lite on request

06 RETENTION & AGGREGATION

Account data: until deletion or 24 months inactive

Identified responses: 24 months

Aggregated / de-identified: retained for the program

Security logs: 90 days

Min cohort for publication: n ≥ 10

CONTACT

FULL REFERENCE