Architecture overview

Schema-per-tenant isolation and agent/API flow

Trustholm Architecture Overview (Summary)

Vendor origin

- - Global legal entity: Trustholm Pty Ltd (Australia)
- - European founder-led product; EU/EEA data plane and contracting via enterprise onboarding

Tenant isolation

- - Each tenant: dedicated PostgreSQL schema (tenant_{code})
- - Portal users: JWT TenantId must match resolved tenant (403 on mismatch)
- - Agents: X-Tenant-Code + X-Agent-Key polling credentials

Regional data planes (home region per tenant at provision time)

- - Australia (launch): api-aus.trustholm.com / portal-aus.trustholm.com
- - European Union (pilot/enterprise): api-eu.trustholm.com / portal-eu.trustholm.com
- - Vanity portals: {tenantCode}.trustholm.com pinned to tenant home region via DNS

Script flow

1. Author in PowerShell IDE → approval → signing policy check 2. Execution queue dispatches to agent 3. Security audit records publish, approve, run events 4. Optional: external agentic tools via POST /api/Governance/execution-intent

Audit planes

- - Security audit table: privileged actions (export via /api/audit/export)
- - HTTP request logs: operational telemetry with tenant_id enrichment

Deployment profiles

- - Shared multi-tenant SaaS (regional)
- - DedicatedDatabase (enterprise isolation profile)
- - Self-hosted / air-gapped (Enterprise bundle)

Honest gaps (see product evidence map)

- - WORM / hash-chain audit immutability: backlog
- - Native Microsoft Sentinel connector: backlog
- - MCP transport for agentic gate: roadmap (REST v1 shipped)

Marketing site (www.trustholm.com): trial signups only; no tenant production data.