

FOUNDING DESIGN-PARTNER PILOT

Turn machine-identity metadata into an accountable exposure map.

A fixed-scope 60-day engagement for one consequential agent workflow in one business unit. PermitGraph traces agent and workload access and delivers a repeatable evidence package. The default customer-run mode keeps raw metadata inside the customer's environment.

INVESTMENT	DURATION	SCOPE	RECORD LIMIT
\$4,000	60 days	1 business unit	2,500

The outcome

- A validated inventory of AI agents, service principals, workload identities, credential metadata, resources, and access paths for the agreed scope.
- A prioritized exposure register with accountable owners, recommended controls, and human-validation status.
- A repeat scan, executive readout, machine-readable evidence package, ROI baseline, and production decision memo.

Delivery plan

WEEK 1	Source map + safe run	Confirm scope, owners, up to three sources, field mapping, exclusions, and zero-custody or agreed-transfer delivery mode.
WEEK 2	First exposure report	Run the scanner customer-side by default, review critical paths, and establish the approved finding register.
WEEKS 3-5	Validate + tune	Resolve ownership, tune false positives, confirm accepted corrections, and define the remediation baseline.
WEEKS 6-8	Repeat + decide	Run the second scan, measure change, deliver the executive package, and make a production conversion decision.

Included in the fixed scope

UP TO THREE MAPPED SOURCES AWS IAM, Entra, GitHub, MCP tool registries, and Supabase use customer-supplied metadata adapters, not hosted collectors. MCP still needs an approved registry and action map; voice and custom registries need an agreed field map.	TWO SCAN CYCLES First assessment plus a repeat scan after validation or agreed corrections.
OWNERSHIP WORKSHOP One working session to assign owners, validate lineage, and resolve ambiguous access paths.	BUYER-READY EVIDENCE Prioritized register, executive readout, JSON evidence, integrity digest, ROI baseline, and production requirements.

DECISION FRAME

Success is measurable. The security boundary is explicit.

The default delivery mode keeps raw metadata inside the customer's environment: run PermitGraph locally, review the findings, and share only an approved evidence package. Any raw-metadata transfer is a separately agreed exception.

Pilot success criteria

01	SOURCE ONBOARDING	Valid metadata for the agreed sources can be prepared and mapped into the customer-run scanner in under two customer hours.
02	TIME TO FIRST REPORT	The first report is delivered within one business day after a complete, valid scan is available for review.
03	ACCEPTED CORRECTIONS	At least three owner, credential, or access-path corrections are accepted by the customer.
04	MEASURABLE CHANGE	The repeat scan shows the status and risk change for validated findings.
05	DECISION	A production conversion, extension, or stop decision is made within 14 days of the final readout.

Data and security boundary

ZERO-CUSTODY DEFAULT The customer runs PermitGraph locally. Raw exports stay in its environment; only customer-approved findings or evidence are shared.	METADATA ONLY No passwords, token values, private keys, client secrets, JWTs, database rows, Storage objects, or application payloads.
NO INFRASTRUCTURE MUTATION The pilot reports findings and recommended controls. It does not revoke, rotate, grant, or change production access.	NO TRAINING RIGHT BY DEFAULT Customer source data remains customer-owned. PermitGraph receives no model-training right unless separately agreed in writing.

If Pith Strategies will receive raw metadata, the parties must first agree in writing on confidentiality, encrypted transfer, permitted operators, retention and deletion, incident handling, liability, and any required security or privacy exhibit. The public demo does not persist scan submissions; the separate pilot-request form stores only business contact and fit information.

Out of scope

- Secret custody or password vaulting	- Autonomous remediation	- Runtime enforcement
- Workforce identity governance	- Penetration testing	- Compliance certification

READY FOR A FIT CHECK?	permitgraph-agent-security.andrew7carlin.chatgpt.site
Andrew Carlin / Pith Strategies	pithstrategies@gmail.com

Commercial structure: \$4,000 fixed, proposed as 50% at kickoff and 50% at final readout. Final scope, payment schedule, and legal terms are controlled by a mutually signed order form.