IMPLEMENTATION PLAN

Distributed workers across your estate

What gets stood up, in what order, and who does each part.

Pattern A DMZ and a worker in every environment. Evidence stays where it lands.

For Multi-cloud enterprises with residency or egress constraints

IRON FORT YOU TOGETHER

The control plane is built as in Pattern 2. The difference is that you run a collector in every environment you have, and you provide the storage it writes to. Plan this per environment rather than as one project — each has its own network owner and its own change window.

BEFORE YOU START

- An inventory of every environment in scope: cloud accounts and data centres alike.
- For each, a network owner who can place a workload in a DMZ and allow its egress.
- For each, storage you control — object storage or a filesystem — and the key that protects it.

1

Inventory the estate TOGETHER

- List every environment: AWS accounts, Azure subscriptions, Google Cloud projects, data centres.
- For each, name the network owner and the storage it will write to.
- Decide what is genuinely in scope. Every environment you add is a worker to run, so scope honestly rather than exhaustively.

DONE WHEN

A list of environments, each with an owner, a runtime and a storage target.

2

Control plane IRON FORT

- We build your dedicated control plane as in Pattern 2, with the same allowlist and sign-in.
- Register each planned worker and issue a key unique to it.
- Confirm no evidence artefact will be stored here — only findings, status and pointers.

DONE WHEN

The control plane is reachable and every worker has an identity.

3

First worker, one environment TOGETHER

- Deploy a ScanOps worker into a DMZ in your least sensitive environment first — a VM, a Kubernetes pod, or a plain container, whichever that environment already runs.
- Give it read-only credentials for that environment and a path to its storage.
- Confirm it connects out to the Iron Fort endpoint successfully, and that evidence lands in your storage, not ours.

DONE WHEN

One environment collects end to end, and you can point at where the evidence sits.

4

Roll out the remaining environments YOU

- Repeat per environment. The pattern is identical; the network conversation is not, so allow for each one separately.
- Keep keys distinct per worker. A shared key removes the only thing that tells two environments apart.
- Set retention and legal hold on each storage target — they are yours to set and yours to defend.

DONE WHEN

Every environment on the inventory is collecting.

5

Scope, collect, populate TOGETHER

- Record the organisation and its systems across all environments; install the framework.
- Run the first full collection and reconcile findings against what each environment owner expects.
- Bulk-upload existing policies and set review cycles.

DONE WHEN

One coverage figure spans the whole estate, and each environment owner recognises their part of it.

6

Prove the boundary TOGETHER

- Walk your security team through an evidence item end to end: where it was collected, where it is stored, what left the environment.
- Document the answer. This is the artefact that satisfies the residency question in future reviews.
- Schedule recurring reviews and generate the first assessor report pack.

DONE WHEN

Your security team has signed off the data-flow, in writing.

Sequence, not schedule. The phases are ordered by dependency. Elapsed time depends on your change process, your approvals and how much of the estate is in scope, so this plan does not guess at it. Ask us and we will estimate it against your specifics.

Iron Fort Solutions · goironfort.com/reference-architecture