

MARKETING BROCHURE · 16 PAGES

Sovereign and air-gapped AI

Choose jurisdiction, infrastructure, custody, and network boundaries for the work.

VISUAL BRIEFING

SOVEREIGNTY, SECURITY, INFRASTRUCTURE, AND MISSION OWNERS

ENGLISH



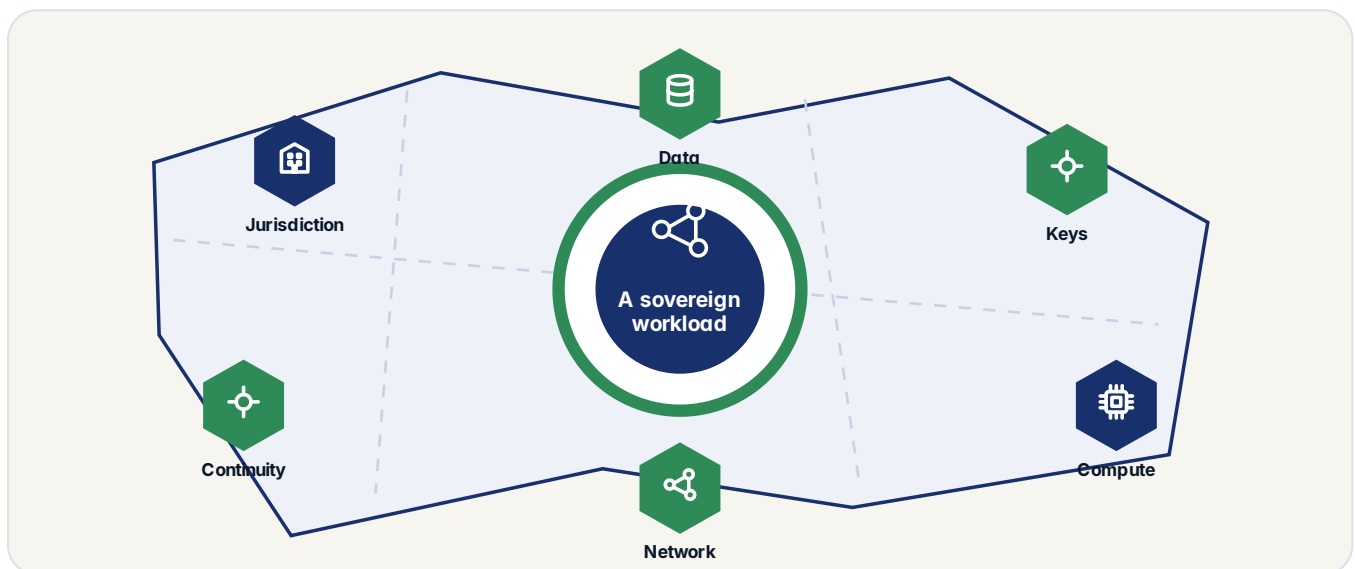
Turn sovereignty from a slogan into an operating decision.

M05

THE PROPOSITION

Control that can be demonstrated

Deployment uses three operating postures: managed participation in Dweve's public Mesh, a licensed platform on hardware you control, or fully air-gapped operation with no outbound network. The operating responsibility changes without inventing a different product architecture.



How to read this visual: follow a sovereign workload through the proposition.

MECHANISM

Read the promise against the operating reality

Managed customers use Fabric, its business API and Agent SDK on the public Dweve Mesh. A licensed deployment adds direct operation of Core and the platform products on customer-controlled infrastructure. Key custody, updates, logs, product access, and source rights follow that boundary.

Most people open managed Fabric in a browser and start without an infrastructure project. Organisations that need direct product operation inside their own perimeter move to a licensed deployment. Workflow and evidence contracts remain portable, while product access, keys, patches, logs, and operating responsibility change.

- Jurisdiction
- Data
- Keys
- Compute

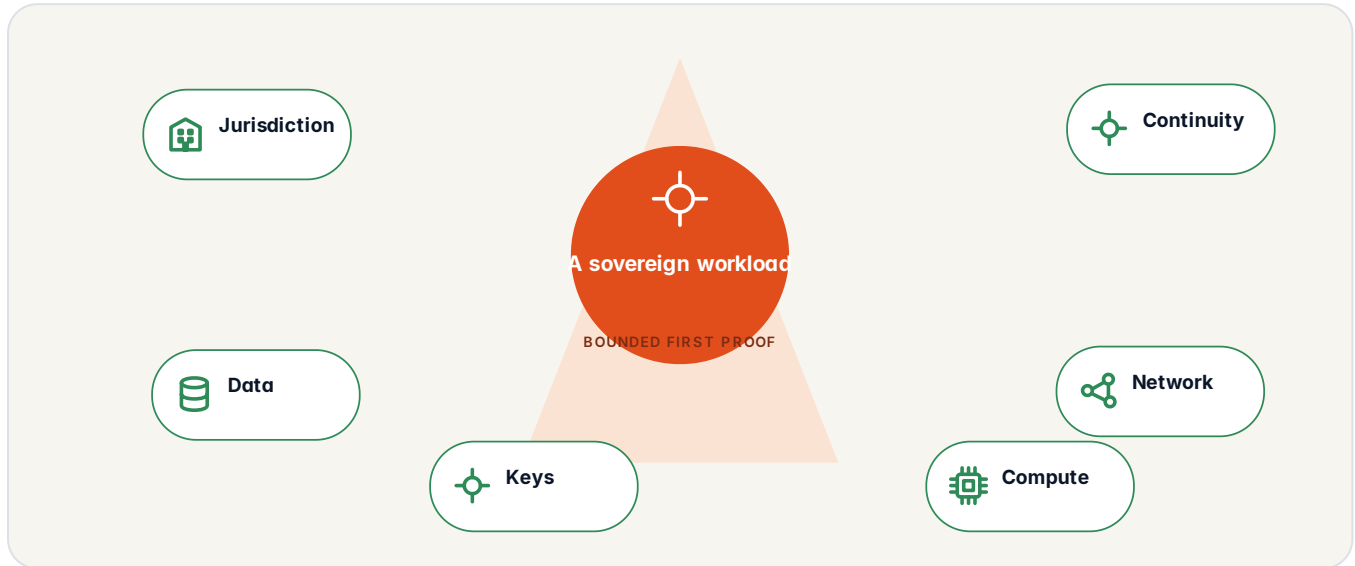
QUESTION TO CARRY

Which part of this proposition changes the outcome people receive today?

USE AND FIT

Where this proposition can earn its place

Start with responsibilities that have a real owner, useful sources, and a consequence worth improving.



How to read this visual: follow a sovereign workload through use and fit.

DECISION

Separate useful scope from attractive distraction

Start in managed Fabric: open a browser, sign in, and ask. If your organisation later needs direct product operation inside its own perimeter, use a licensed transition plan that carries the workflow and evidence contracts into customer-controlled infrastructure.

Choose managed Fabric on the public Dweve Mesh, direct licensed operation on your infrastructure, or an isolated licensed perimeter. Workflow and evidence contracts remain portable; product access, keys, patches, logs, source rights, and operational responsibility change.

- Jurisdiction
- Data
- Keys
- Compute

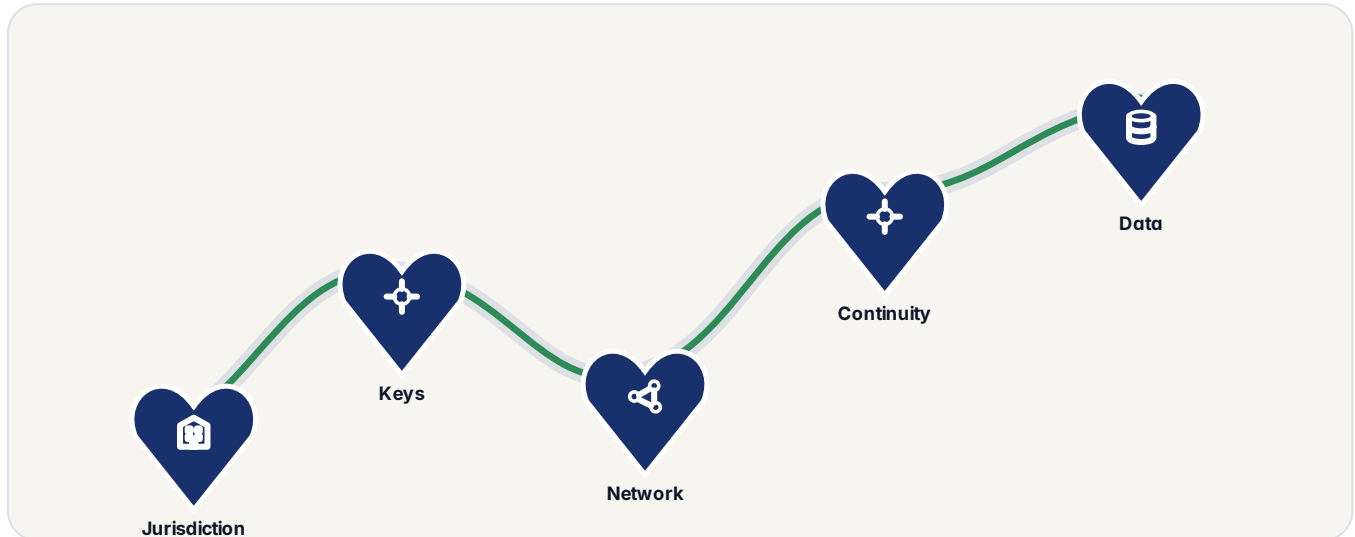
QUESTION TO CARRY

Where does this earn a place, and where should it deliberately not be used?

THE PATH

From first question to an informed decision

A focused engagement should make the next decision easier, not create a larger promise.



How to read this visual: follow a sovereign workload through the path.

WHY THIS SHAPE WORKS

The workflow, operating boundary, evidence, and decision criteria are considered together from the start.

MECHANISM

Make every stage earn the next one

Ask a question on a browser at home, or on a machine in a locked room with no internet at all. The answer that comes back is the same, down to the last word. So is the little list that tells you where it came from. Nothing about how it works changes when it moves.

Shuttle is a hardware-target option inside the air-gapped posture. It runs the same binaries as every other posture. The FPGA backend in Core handles the compute path; the rest of the stack is unchanged.

- Jurisdiction
- Keys
- Network
- Continuity

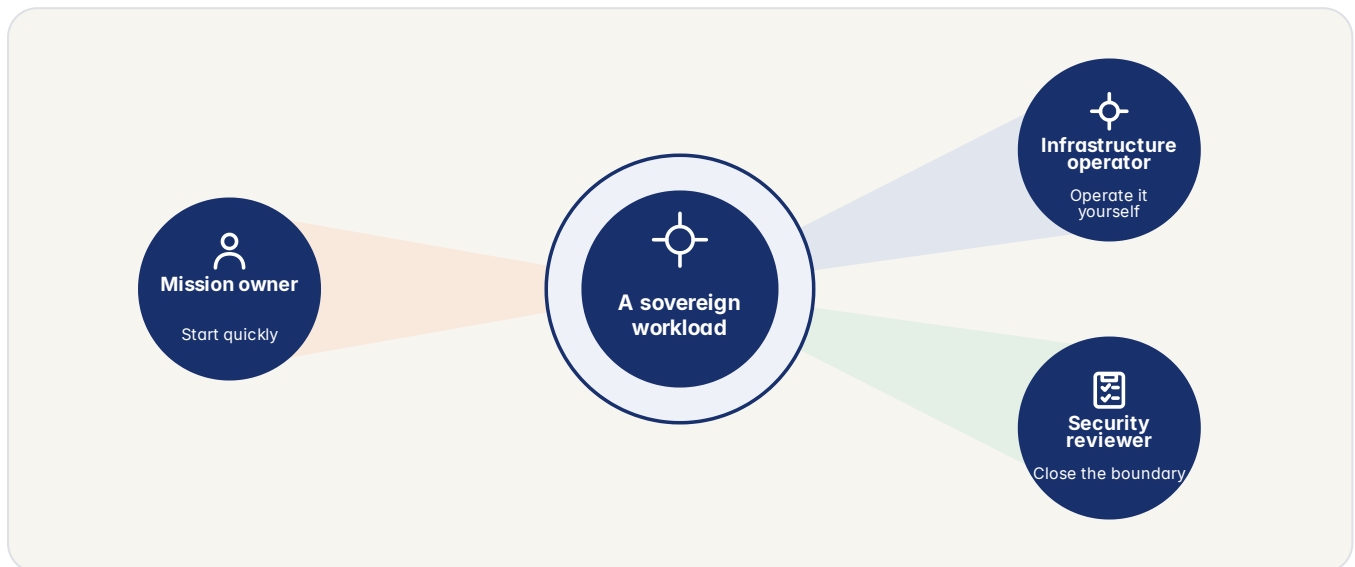
QUESTION TO CARRY

What evidence must exist before the scope is allowed to grow?

THE VALUE PICTURE

One outcome, seen from three responsibilities

Good AI work must make sense to the person using it, the team operating it, and the people reviewing it.



How to read this visual: follow a sovereign workload through the value picture.

PRIMARY READER

Sovereignty, security, infrastructure, and mission owners

The first conversation.

DECISION SUPPORTED

Turn sovereignty from a slogan into an operating decision.

The next useful step.

DECISION

Read the same outcome from several responsibilities

For customers who want the compliance posture of licensed deployment without building an operations team. Dweve engineers handle installation, patching, monitoring, and incident response on hardware inside your perimeter. The runbook hands over at cutover, with optional ongoing management.

You receive the licensed platform products plus Helm charts, Terraform modules, Docker Compose files for local development, and the agreed operations material. Your team operates them; Dweve deployment engineering and escalation support are available by agreement.

- Start quickly
- Operate it yourself
- Close the boundary
- Jurisdiction

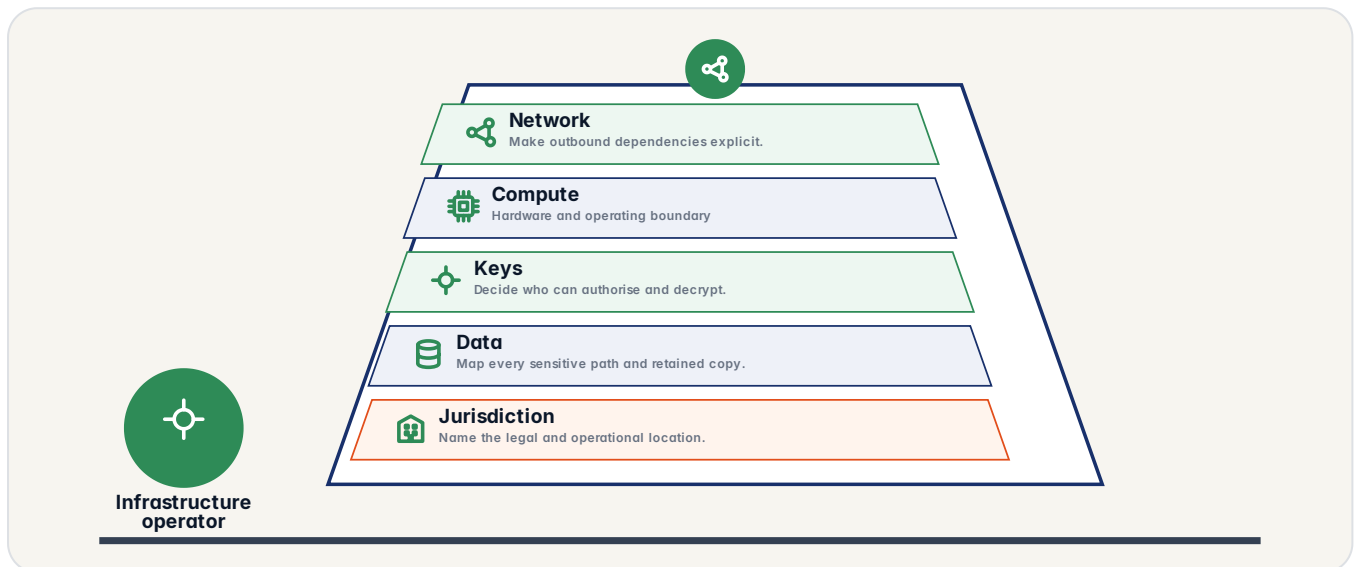
QUESTION TO CARRY

Can the same result satisfy its user, operator, and reviewer?

THE OPERATING MODEL

Control follows the work, from outcome to exit

A credible proposition connects the visible result to the less visible responsibilities underneath it.



How to read this visual: follow a sovereign workload through the operating model.

MECHANISM

Name the controls behind the simple interface

The Loom model is defended against extraction, adversarial attacks, integrity violations, and abuse across 10 threat types. Compiled binaries carry protection interpreted weights cannot match: integrity verification with SHA3-256 and BLAKE2b plus digital signatures, statistical adversarial detection, extraction protection with query-pattern analysis and response noise, and access control. For BYOK external models you hold the keys, so their security is yours to manage.

Choose managed Fabric on the public Dweve Mesh, direct licensed operation on infrastructure you control, or a physically isolated licensed installation.

- Jurisdiction
- Data
- Keys
- Compute

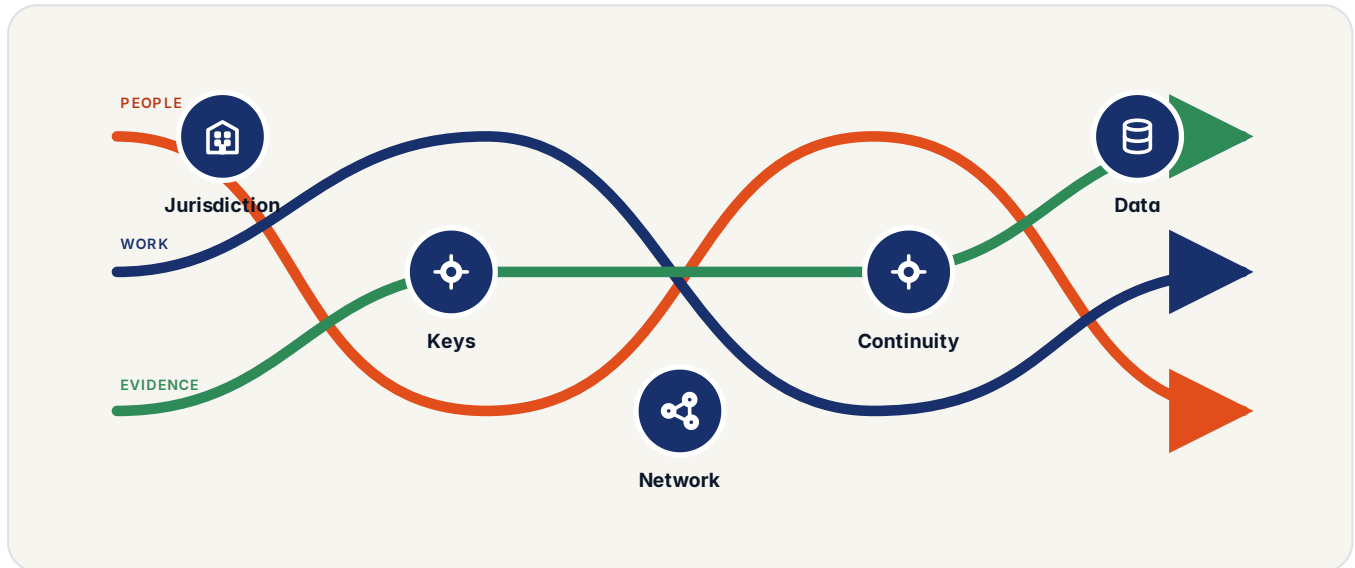
QUESTION TO CARRY

Who owns each control when the interface appears simple?

THE RESPONSIBILITY FLOW

People, platform, and evidence move together

The work becomes easier to govern when each stage leaves a clear hand-off.



How to read this visual: follow a sovereign workload through the responsibility flow.

DECISION

Keep every hand-off attached to an owner

Workflow and evidence contracts are designed to move, but a change of access model still requires an explicit technical and commercial transition.

The access model decides who operates the products, who holds the keys, and where the boundary sits. Workflow and evidence contracts remain portable, but rights are not identical.

- Jurisdiction
- Keys
- Network
- Continuity

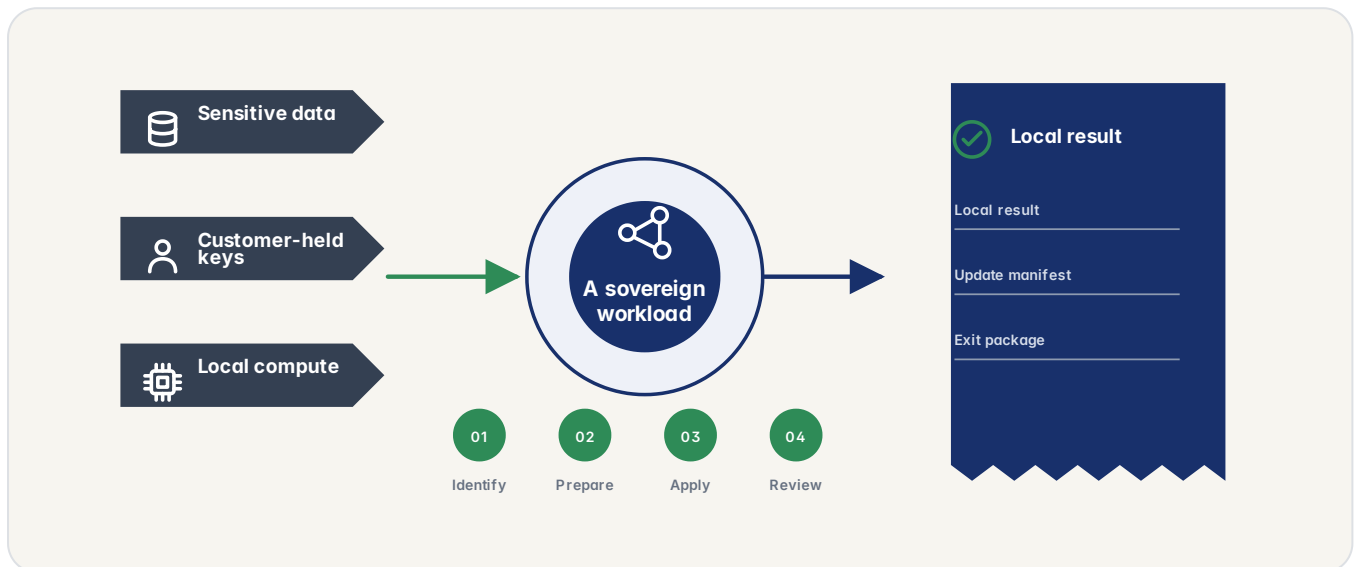
QUESTION TO CARRY

Is every hand-off visible, bounded, and assigned to an owner?

SOURCE TO RESULT

Every useful outcome begins with an authoritative basis

The work stays explainable when source identity, transformation, decision, and hand-off remain visible between systems.



How to read this visual: follow a sovereign workload through source to result.

MECHANISM

Keep the basis visible as the work changes form

Managed Fabric requires no customer installation. Direct operation of Core and the platform products begins with a licensed deployment and an explicit transition plan.

Licensed and air-gapped installs keep running with no kill-switch. The capability is already inside your perimeter, so it stays yours to operate.

- Identify
- Prepare
- Apply
- Review

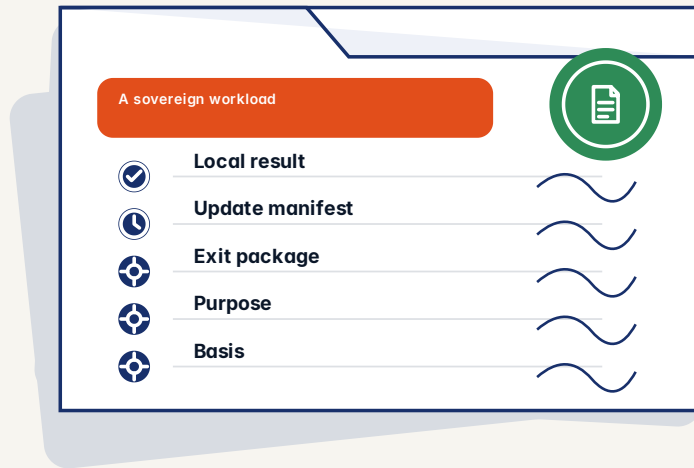
QUESTION TO CARRY

Can the result still be connected to the exact basis that shaped it?

EVIDENCE PACKET

The record should answer the next difficult question

Capture enough to explain the result, inspect authority, investigate failure, and make the next decision without rebuilding the story from memory.



How to read this visual: follow a sovereign workload through evidence packet.

DECISION

Preserve the record needed by the next question

Threat snapshot, standing order, decision trace, and officer receipt form one signed packet. Oversight can replay it in isolation without reconnecting the deployed system.

Traces from an air-gapped environment are bit-identical to traces from Fabric. An auditor with the AION verifier binary replays any trace, on any machine, without internet.

- Purpose
- Basis
- Authority
- Action

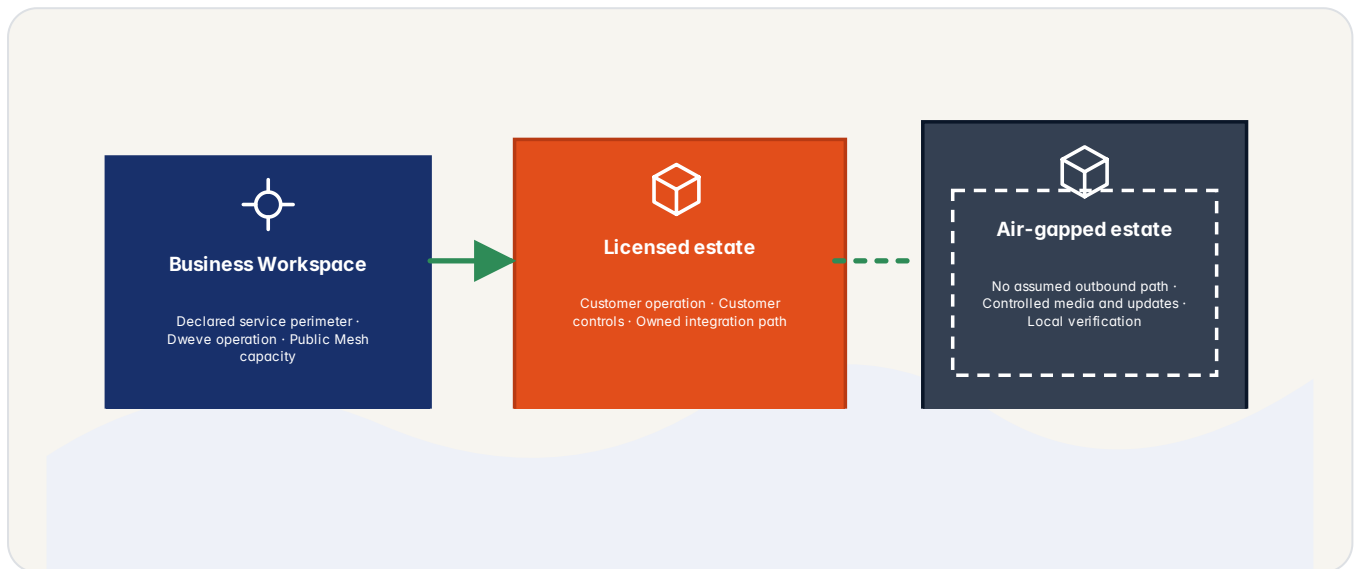
QUESTION TO CARRY

Does the retained record answer the next difficult question without reconstruction?

DEPLOYMENT CHOICE

Choose the operating posture around the work

Location is only one dimension. Decide who operates, who holds keys, which dependencies exist, how updates arrive, and what continuity requires.



How to read this visual: follow a sovereign workload through deployment choice.

MECHANISM

Compare operating responsibility, not location alone

Every security review asks the same five things. Can an assistant be tricked? Where does the data go? Is personal data protected? Who holds the keys? Will the encryption last? Dweve answers each one by construction, not with posture added later. Security and privacy are core principles, so the procurement file is a retrieval, not a scramble. One platform, not seven tools, with EU-only operations.

Before you commit to where the workload runs, four questions decide whether the deployment story holds. Here they are, answered plainly.

- Begin through managed Fabric
- Run on customer infrastructure
- Close the environment
- Jurisdiction

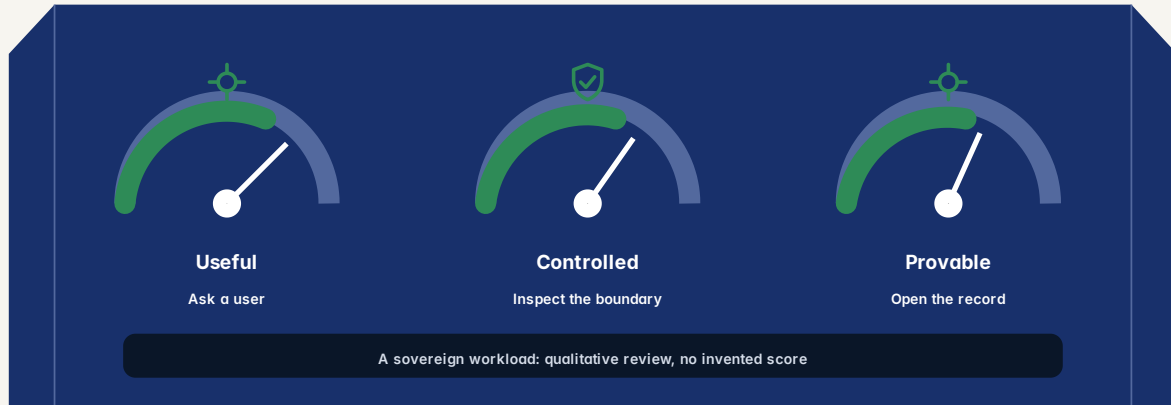
QUESTION TO CARRY

Who holds infrastructure, keys, updates, logs, recovery, and the exit path?

WHAT TO LOOK FOR

Three signals that the proof is earning trust

Progress is a useful outcome under understood control, supported by reviewable evidence.



How to read this visual: follow a sovereign workload through what to look for.

DECISION

Use signals that can change the next decision

Policy evaluation in Lattice and proof generation in AION are pure functions of their inputs. Both run with no network access.

Binaries, model weights, charts, and every dependency bundle into a signed archive, delivered on encrypted physical media through a documented chain of custody. The import script validates checksums before unpacking. Licence validation is offline-signed. No network egress of any kind after install.

- Useful
- Controlled
- Provable
- Jurisdiction

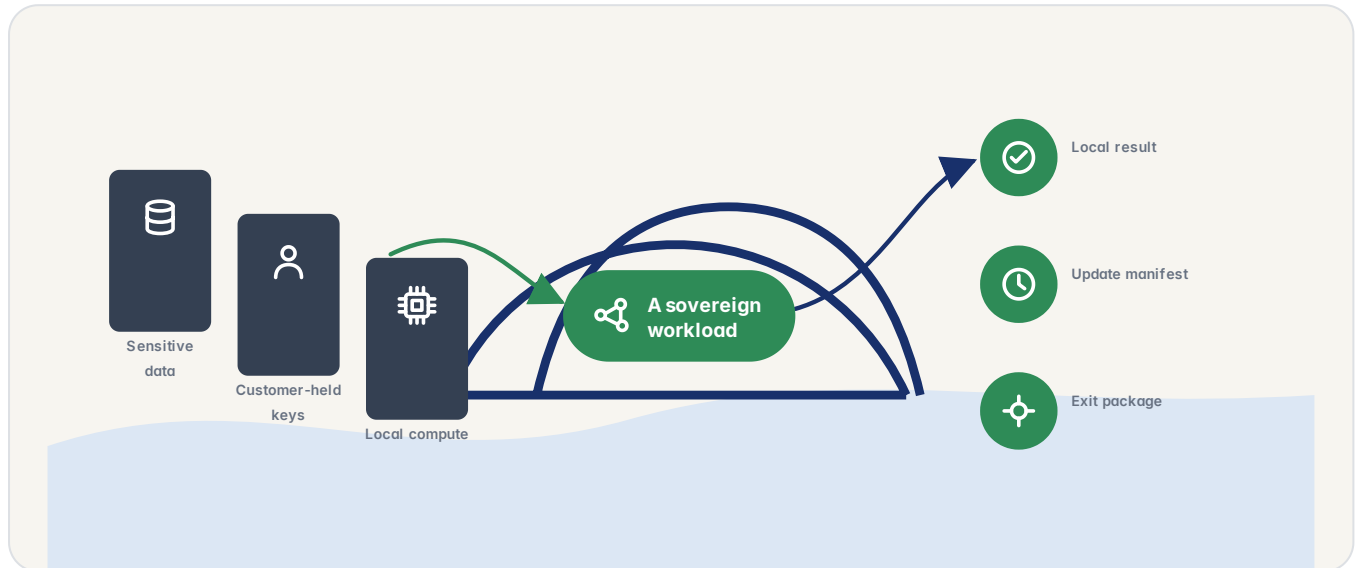
QUESTION TO CARRY

Which signals would change the next decision rather than merely impress the room?

HONEST LIMITS

Design failure before the first success demo

Visible failure is more useful than a polished result whose limits remain unknown.



How to read this visual: follow a sovereign workload through honest limits.

MECHANISM

Design the failure before presenting the success

Deterministic inference removes non-reproducible bugs and closes whole vulnerability classes at design time. There is no patch backlog to chase, because the failure mode was never reachable in the first place.

The energy saving is a consequence of binary compute. XNOR and POPCNT on FPGA fabric are orders of magnitude more efficient than floating-point matrix multiply on a GPU.

- Network loss
- Key unavailable
- Supplier loss

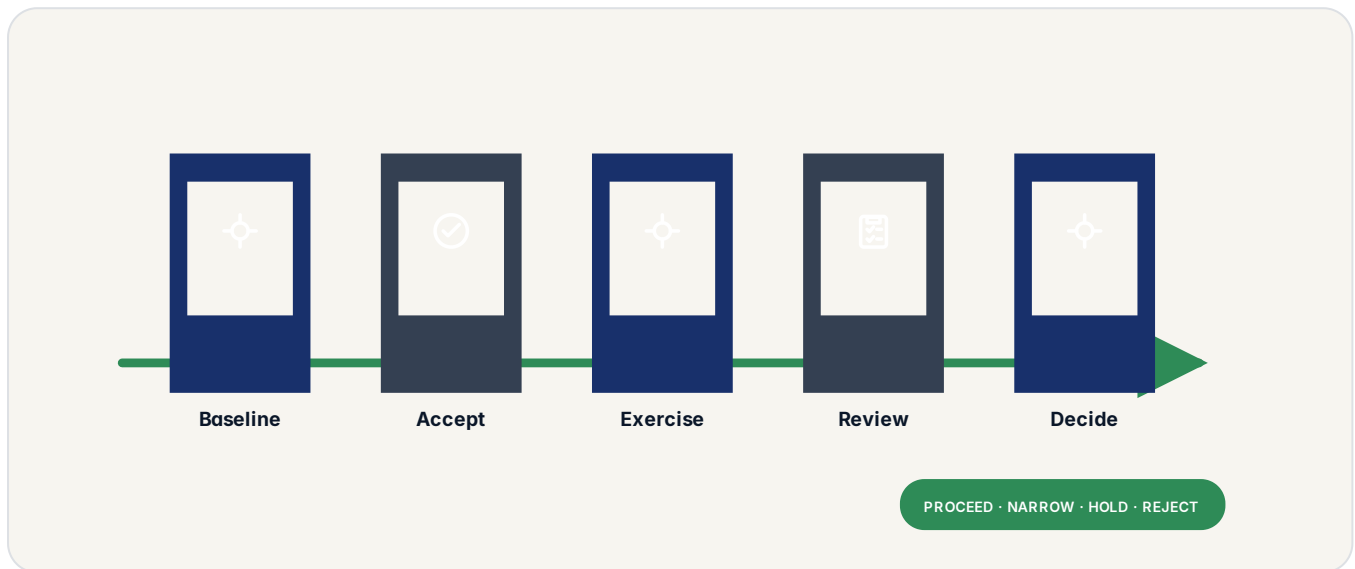
QUESTION TO CARRY

What happens when a source, permission, target, model, or supplier is unavailable?

ACCEPTANCE PATH

A proof should close with a decision, not applause

Agree the decision path before the demonstration so a strong or weak result can change what happens next.



How to read this visual: follow a sovereign workload through acceptance path.

DECISION

Close the proof with an owned decision

The local development path. One file, one command, the full stack up including a local object store and message queue. Not for production.

The production path. An umbrella chart with independently versioned subcharts for inference, router, gateway, monitoring, and ingress. Each subchart can be disabled.

- Baseline
- Accept
- Exercise
- Review

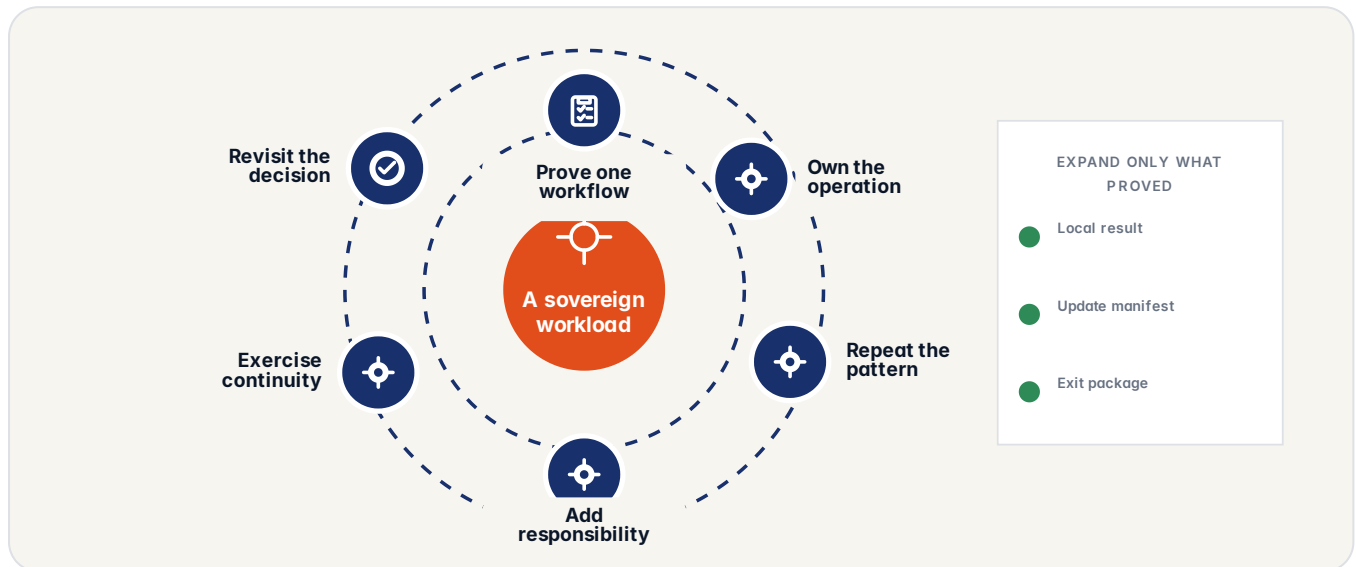
QUESTION TO CARRY

Are success, counter-metrics, failure cases, and stop conditions agreed first?

ADOPTION

Expansion is a sequence of owned choices

Move from one bounded result to a repeatable operating capability without making the scope vague.



How to read this visual: follow a sovereign workload through adoption.

MECHANISM

Expand only what proved reusable

The operating requirements and product rights differ across access models. This is what you are signing up for beyond the price.

No workflow rebuild is required, but the access boundary changes. Managed customers use Fabric and its business surfaces; licensed customers operate the products directly.

- Prove one workflow
- Own the operation
- Repeat the pattern
- Add responsibility

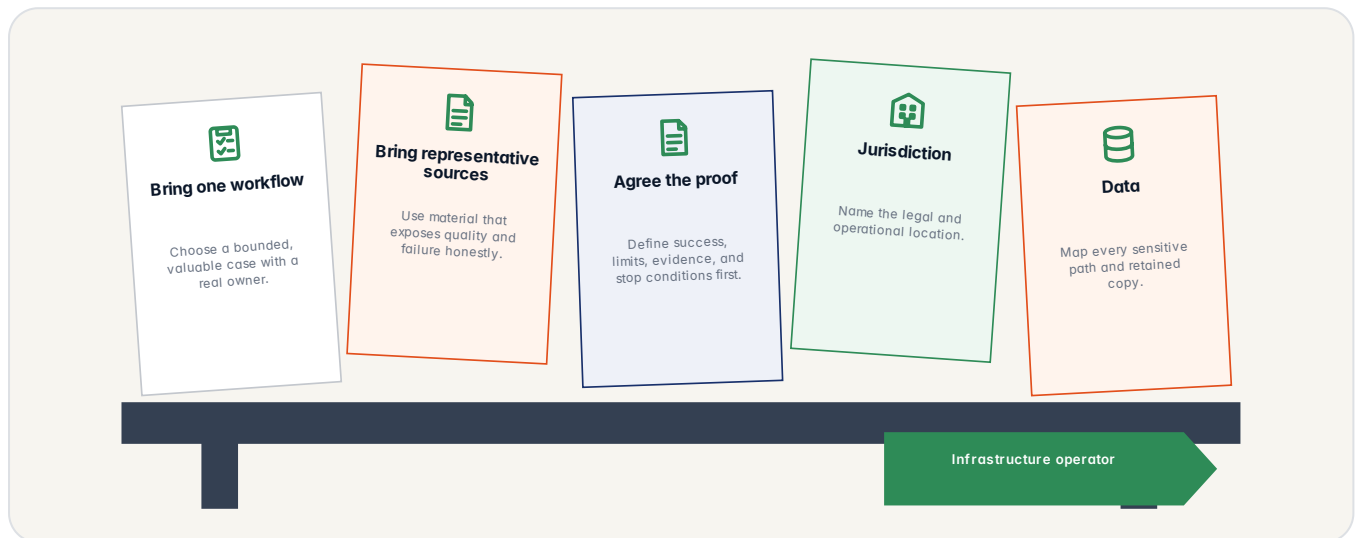
QUESTION TO CARRY

What can be reused safely, and what requires a new decision and proof?

WHAT TO PREPARE

Bring the ingredients for a useful first session

A small amount of real context produces a better conversation than a broad catalogue of hypothetical features.



How to read this visual: follow a sovereign workload through what to prepare.

KEEP IT BOUNDED

Sensitive production data is not required for the first conversation. Bring representative material and the rules that define a useful result.

DECISION

Bring enough reality to make the session useful

The licence token is a signed data structure, verifiable with a public key embedded at build time. No network call required.

Dweve is built for organisations that need security and privacy as core principles, not retrofitted controls. Binary AI security against prompt injection, jailbreaks, and model extraction. Context-aware PII detection. NIST-selected post-quantum cryptography. Bring Your Own Key for every external provider. EU-only operations, with all data stored within EU borders and GDPR Article 25 compliance by design.

- Bring one workflow
- Bring representative sources
- Agree the proof
- Jurisdiction

QUESTION TO CARRY

Which real sources, rules, owners, and examples will make the first session honest?

THE INVITATION

Continue with the question that matters

Scope a briefing, demonstration, or proof around the workflow and decision that matter to your organisation.

dweve.com/contact

ONE MAINTAINED PUBLIC ROUTE

Current contact choices stay on the website

CONTINUE ONLINE

dweve.com/contact

Current route and contact choices

START A CONVERSATION

Continue through the current contact page

Scope a workflow or ask a technical question, then use the contact page to begin.

START	dweve.com/contact Use the maintained public contact route
BRING	One bounded question Workflow, audience, decision, and desired evidence
CHOOSE	Briefing · demonstration · PoV Select the smallest useful next step
VERIFY	Current scope and terms Confirm availability, pricing, and responsibilities before commitment

MECHANISM

Turn the brochure into one bounded next step

Pick the path that fits. Every inbox reaches the same team; the right start depends on where you are: curious about the product, ready to scope a deployment, or here for a technical or legal matter.

Terraform state lives in your own backend. Each module outputs the connection strings and endpoints the Helm chart needs. No remote state access by Dweve.

- Start: dweve.com/contact
- Bring: One bounded question
- Choose: Briefing · demonstration · PoV
- Verify: Current scope and terms

QUESTION TO CARRY

What is the smallest useful next conversation Dweve should prepare?