Dweve
Weaving Intelligence

ENGLISH EDITION · JULY 2026

MARKETING BROCHURE · 16 PAGES

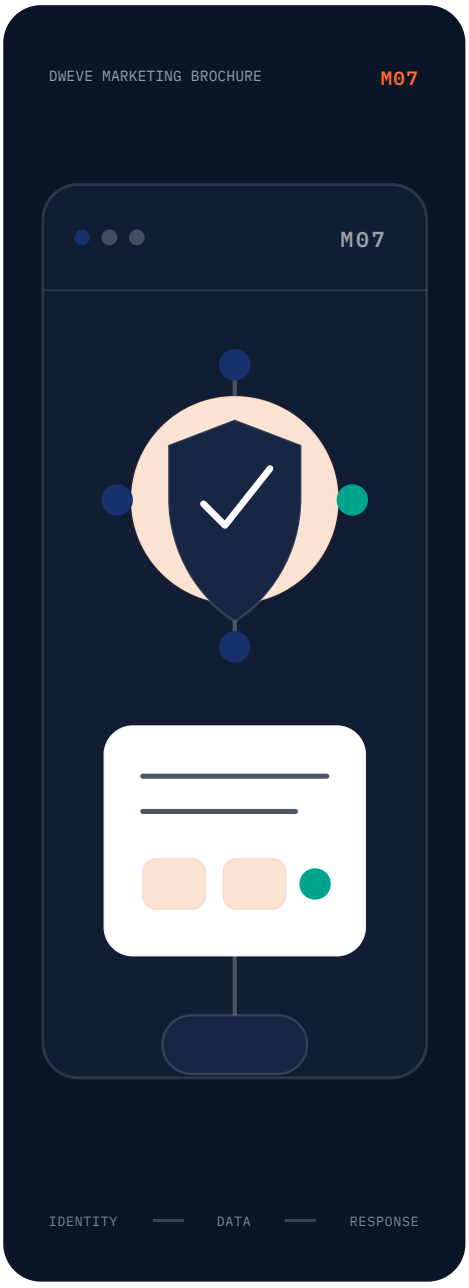
# Security and governed AI

Design authority, data handling, execution, and review into the workflow.

VISUAL BRIEFING

SECURITY, RISK, PRIVACY, GOVERNANCE, AND DELIVERY LEADERS

ENGLISH




Bring security, governance, and delivery into the same picture.

M07

THE PROPOSITION

# A bounded path to an outcome

What the executive brief actually claims, line by line, for the person who has to sign it off and defend it later: one platform instead of seven tools, answers you can explain, data that stays put, hardware you already own, and no lock-in at the foundation.


How to read this visual: follow a governed action through the proposition.

BOUNDARY

## Read the promise against the operating reality

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.

One platform, not seven tools. The same system handles the assistant, the personal-data protection, the key management, and the audit trail, so there is one supplier to assess, one contract, and one place the data lives.

- Identity
- Authority
- Data
- Execution

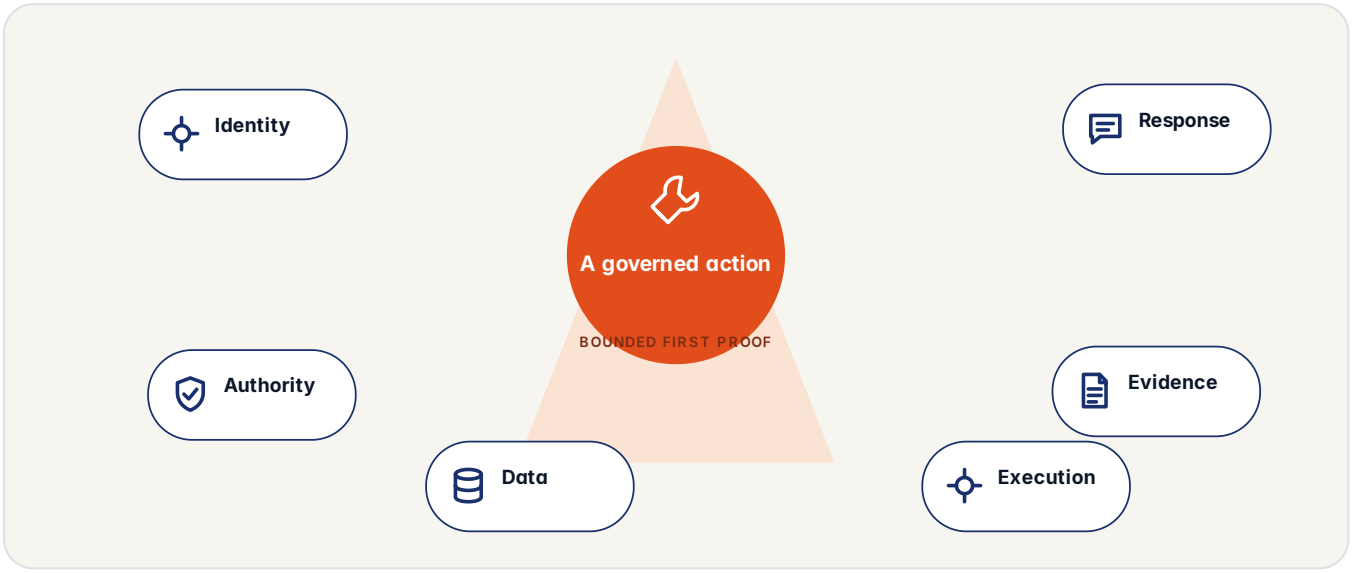
QUESTION TO CARRY

**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 governed action through use and fit.

CONTEXT

## Separate useful scope from attractive distraction

EU-only operations. All data stays within EU borders, with no non-EU subprocessor chain and no non-EU customer acceptance. On-premise deployment is available for full control, so the answer to where does our data go is a place you choose.

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.

- Identity
- Authority
- Data
- Execution

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 governed action through the path.

WHY THIS SHAPE WORKS

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

BOUNDARY

## Make every stage earn the next one

Secure by construction. We prefer architectures that make entire vulnerability classes impossible over patching regimes that catch them after the fact. Deterministic inference removes a class of non-reproducible bugs. Security and privacy are built in from the ground up, not added as an afterthought.

All data stays within EU borders, with no non-EU subprocessor chain and no non-EU customer acceptance. On-premise deployment is available when you want the servers in your own building, so where does our data go is a question you answer, not us.

- Identity
- Data
- Evidence
- Response

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 governed action through the value picture.

PRIMARY READER

## Security, risk, privacy, governance, and delivery leaders

The first conversation.

DECISION SUPPORTED

## Bring security, governance, and delivery into the same picture.

The next useful step.

CONTEXT

## Read the same outcome from several responsibilities

Sometimes people try to fool a computer into doing something it should not, the way a stranger might tell a clever story to get into your house. This has a guard at the door who has heard all the stories before. When a trick comes in, the guard stops it before anything happens. You do not have to spot it yourself. That is the guard's job, day and night.

You want to try this and you want to know it is safe. That is fair. Here is the short version, with no technical talk. Your information stays in Europe. It is locked away so other people cannot read it. The system is not used to learn about your private life. And if anyone tries to trick it, it is stopped before anything happens. You do not need to set anything up. The safety is already there.

- Identity
- Data
- Evidence
- Authority

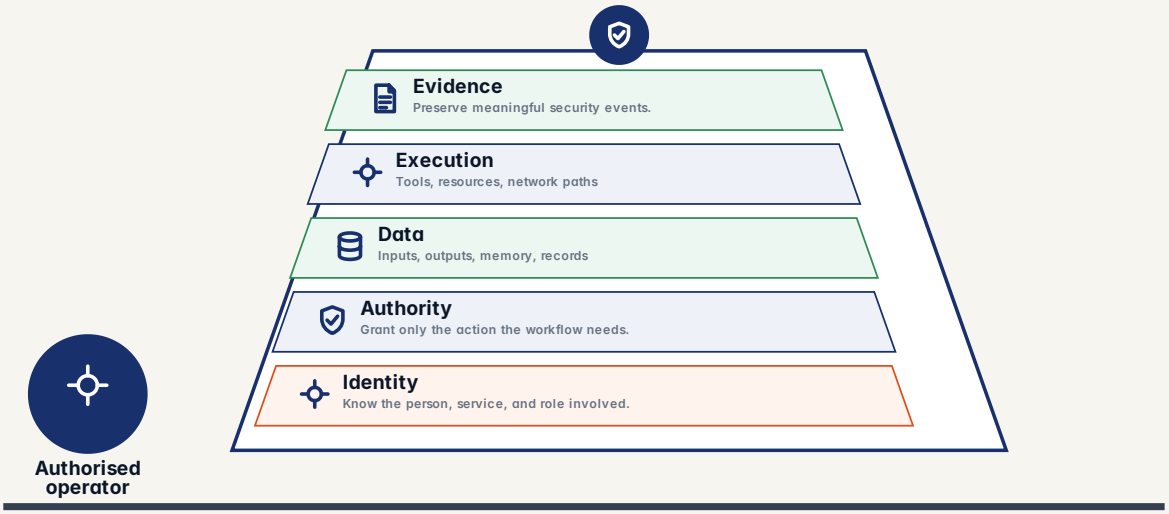
QUESTION TO CARRY

**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 governed action through the operating model.

BOUNDARY

## 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.

A typical AI stack stitches together a separate tool for the assistant, the personal-data scanner, the key vault, the audit log, and the residency control. Five contracts, five attack surfaces, five places the data sits. Dweve does all of it as one platform, so the security review assesses one supplier, one contract, and one jurisdiction, and the keys stay yours throughout.

- Identity
- Authority
- Data
- Execution

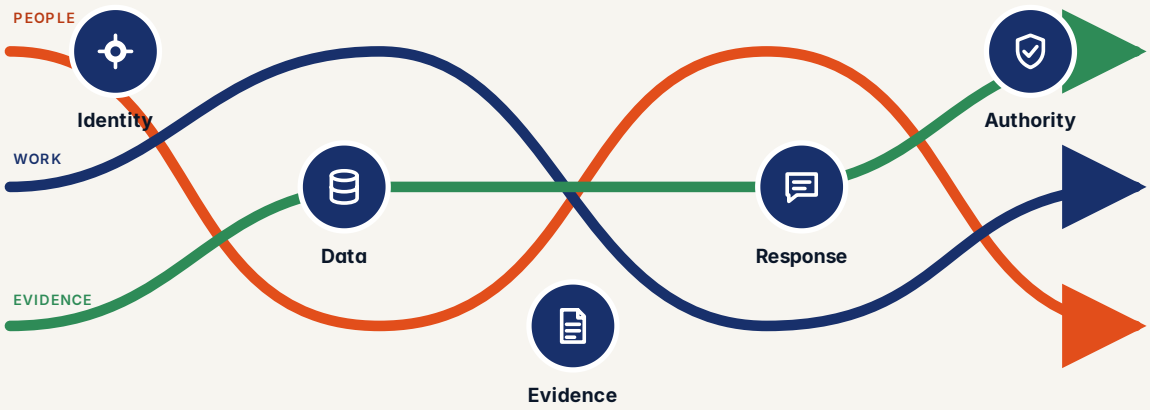
QUESTION TO CARRY

**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 governed action through the responsibility flow.

CONTEXT

## Keep every hand-off attached to an owner

You do not need to know how any of this works. You only need to know it is safe. So here are the things people worry about, each with an everyday example you already understand, like a front door, a locked drawer, or keeping your post in the country.

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.

- Identity
- Data
- Evidence
- Response

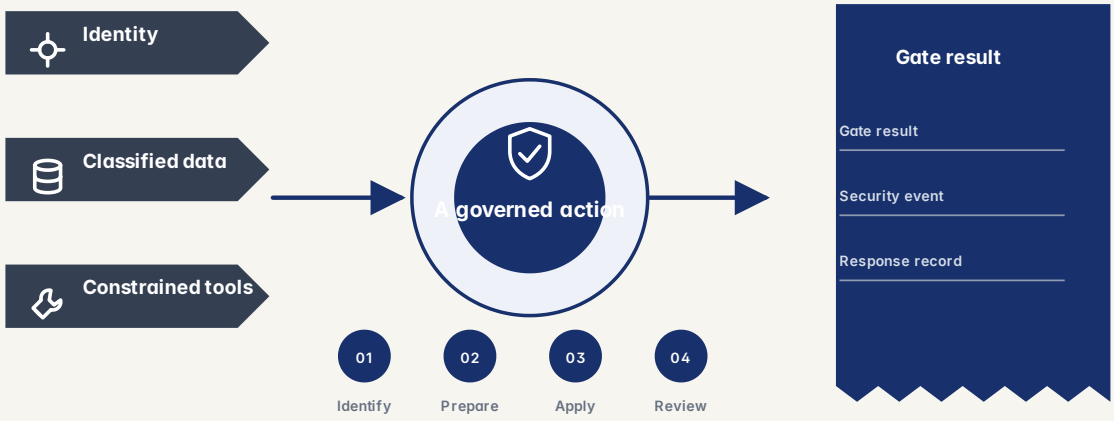
QUESTION TO CARRY

**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 governed action through source to result.

BOUNDARY

## Keep the basis visible as the work changes form

Think of your information like your post. You would not want it shipped to a country you have never been to, where nobody can tell you what happens to it. So it does not leave Europe. It stays under European rules, the same rules that protect you everywhere else, and a person here can always tell you where it is.

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.

- 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 governed action through evidence packet.

CONTEXT

## Preserve the record needed by the next question

And if you ever have a question, you do not have to be a computer expert to get an answer. A real person can explain it to you in plain words.

Deterministic inference removes a class of non-reproducible bugs: the same inputs return the same outputs, so an incident can be replayed exactly rather than guessed at. Complete audit trails record usage, cost, and key lifecycle for compliance reporting, and defence in depth means each layer assumes the one above it can fail and is built to fail closed.

- Purpose
- Basis
- Authority
- Action

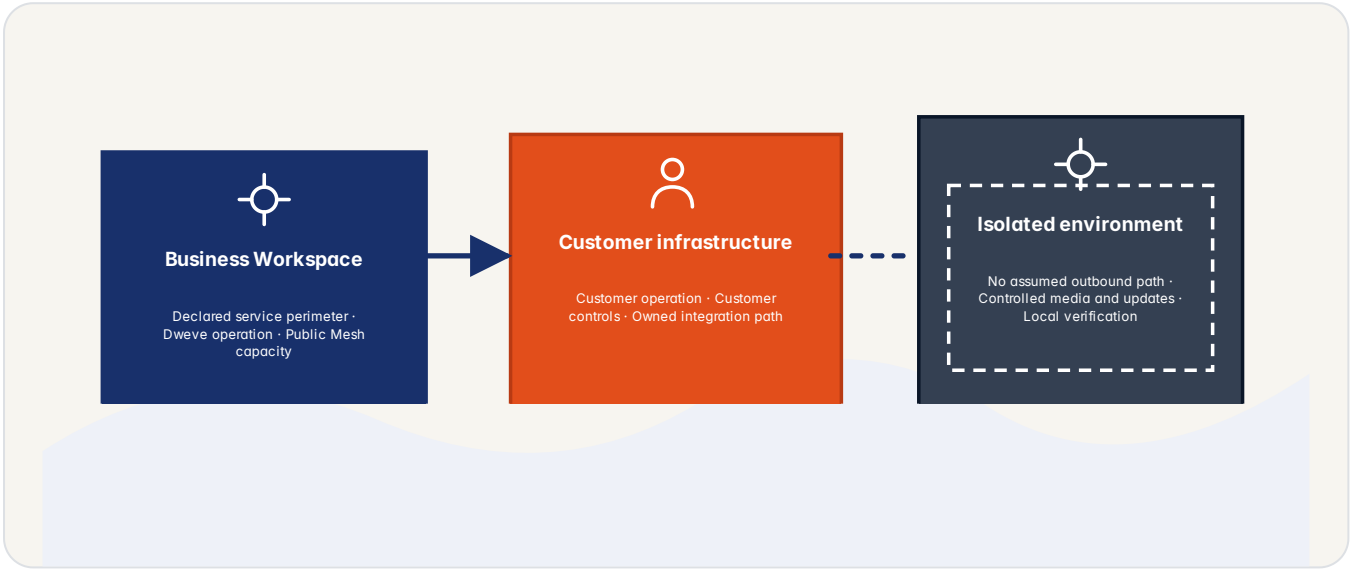
QUESTION TO CARRY

**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 governed action through deployment choice.

BOUNDARY

## Compare operating responsibility, not location alone

Two questions decide procurement: where does it run, and which rules does it satisfy. It runs on hospital or company hardware, in an EU-pinned cloud region, or fully air-gapped, with no re-platforming between options. GDPR, the EU AI Act, NIS2, DORA, and the Cyber Resilience Act are design constraints the platform satisfies by construction, not posture added after the review gets harder to pass.

Zero trust. No implicit trust based on network location. Every request is authenticated and authorised against explicit policy. Lateral movement across tenants, services, or environments requires fresh authorisation.

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

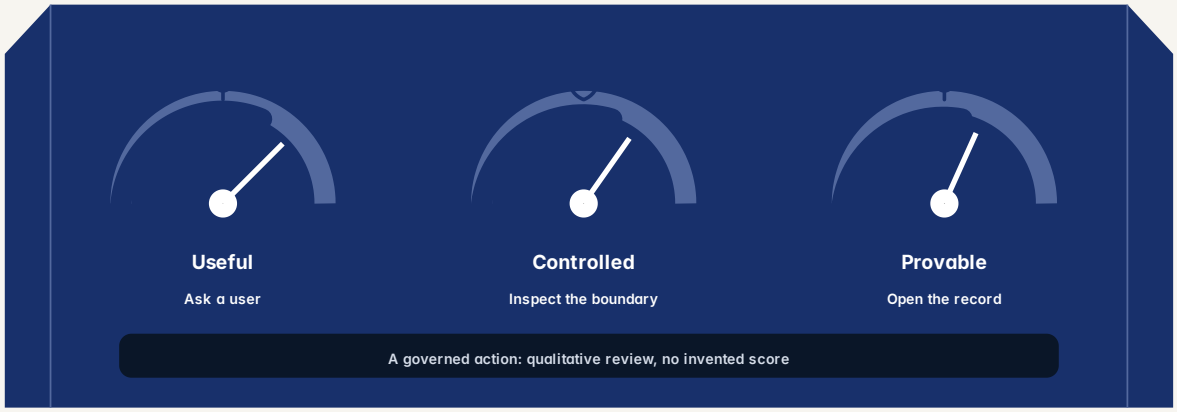
QUESTION TO CARRY

**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 governed action through what to look for.

CONTEXT

## Use signals that can change the next decision

100% EU-based infrastructure with all data stored within EU borders and no non-EU subprocessor chain. TLS 1.3 with perfect forward secrecy in transit, AES-256 with PBKDF2HMAC at rest, and GDPR Article 25 compliance by design. On-premise deployment is available for full control, with no external API calls.

Defence in depth. No single control carries the load. Transport security, at-rest encryption, least-privilege identity, network segmentation, runtime isolation, and continuous audit logging each assume the layer above them can fail. An attacker who breaks one layer meets another that was designed to fail closed.

- Useful
- Controlled
- Provable
- Identity

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 governed action through honest limits.

BOUNDARY

## Design the failure before presenting the success

The procurement pack is a retrieval, not a scramble, because the frameworks are design constraints rather than questionnaires answered after the fact. GDPR and the EU AI Act, including general-purpose AI, are core compliance. NIS2, DORA, and the Cyber Resilience Act are met architecturally, built to satisfy security-by-design, vulnerability handling, and operational-resilience requirements from the ground up.

Some tools add safety later, like fitting a lock after a break-in. This one was built with the locks already on, from the first day. You do not have to switch anything on.

- Denied action
- Data crossing
- Tool misuse

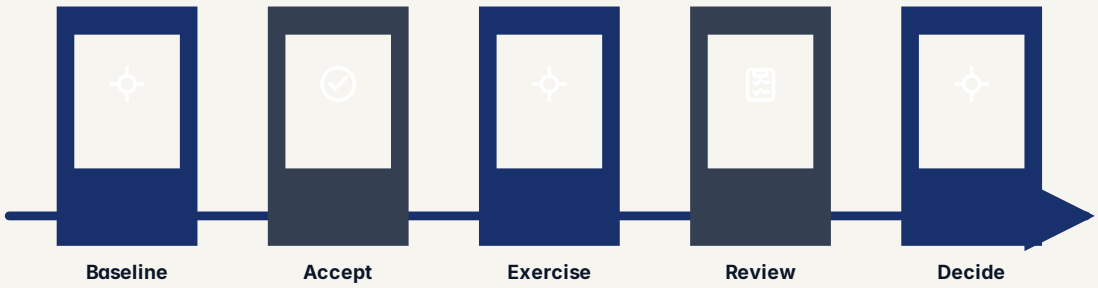
QUESTION TO CARRY

**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.




PROCEED · NARROW · HOLD · REJECT

How to read this visual: follow a governed action through acceptance path.

CONTEXT

## Close the proof with an owned decision

Your information stays in Europe, close to home, under European rules. It is not shipped off to a computer in another country where nobody can tell you what happens to it.

Context-aware detection of 17 PII categories with false positive prevention. Multi-pattern validation and Named Entity Recognition support GDPR compliance. Nine anonymisation techniques, from redaction through differential privacy to T-closeness, with privacy budget tracking and reversible anonymisation. EU-only operations, with no non-EU customer acceptance.

- Baseline
- Accept
- Exercise
- Review

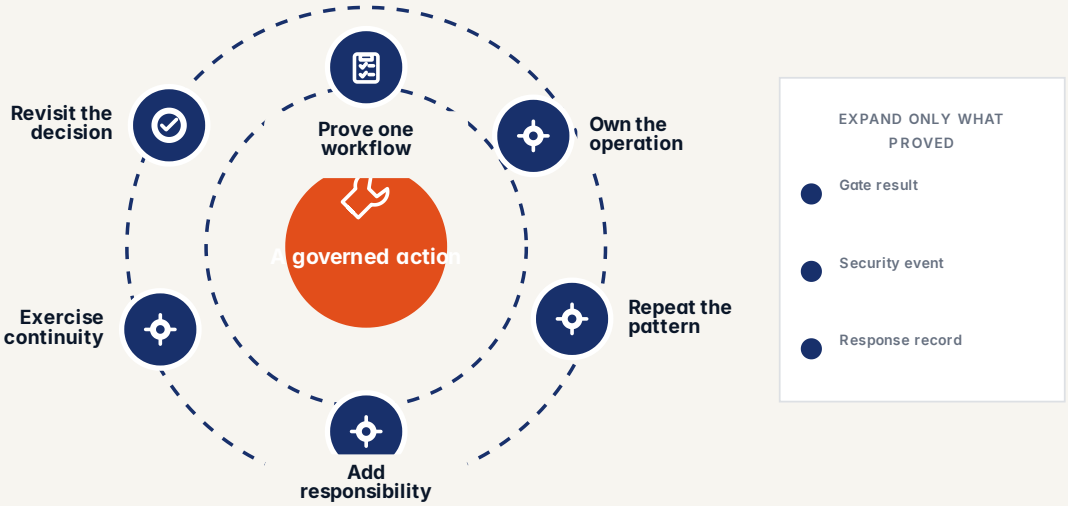
QUESTION TO CARRY

**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 governed action through adoption.

BOUNDARY

## Expand only what proved reusable

Private details are spotted and kept in a locked drawer. The assistant can do its job without leaving your personal information lying around for anyone to read.

SPHINCS+ adds a hash-based fallback. Larger signatures, but no lattice assumption required. A break of lattice cryptography does not leave Dweve deployments without a quantum-resistant option.

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

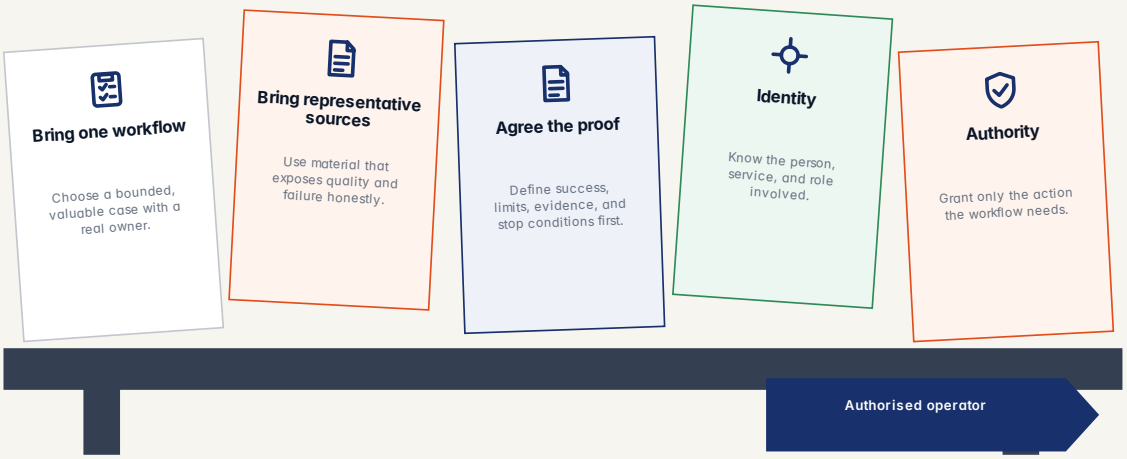
QUESTION TO CARRY

**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 governed action 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.

CONTEXT

## Bring enough reality to make the session useful

Binary AI security runs at four configurable analysis depths. Choose the right balance of speed and coverage for each deployment context: high-throughput APIs stay at Basic, regulated workloads step up to Advanced or Paranoid. The binary neural detector runs independently at below 1ms regardless of the selected level.

Bring Your Own Key for external LLM providers. Fernet encryption (AES-128 CBC plus HMAC-SHA256), PBKDF2HMAC key derivation at 100,000 iterations, and automatic 90-day rotation. AI-specific rate limiting across seven dimensions with model-specific token pricing for Loom and all BYOK models, and real-time cost tracking.

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

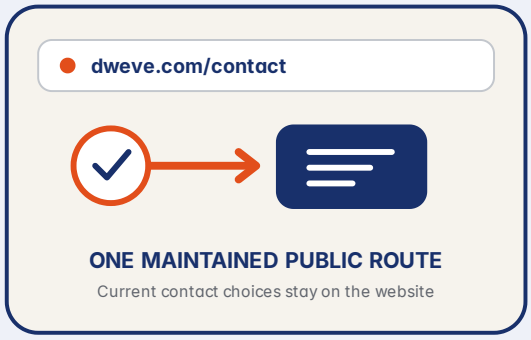
QUESTION TO CARRY

**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.




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 |

BOUNDARY

## Turn the brochure into one bounded next step

Think of a doorman who looks at everyone before they come in. If a message tries to talk the assistant out of its rules, it is stopped at the door before anything happens.

The five risks closed by design, EU data residency, and one platform instead of seven tools. Contact us and we will walk through the procurement file with you.

- 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?**