



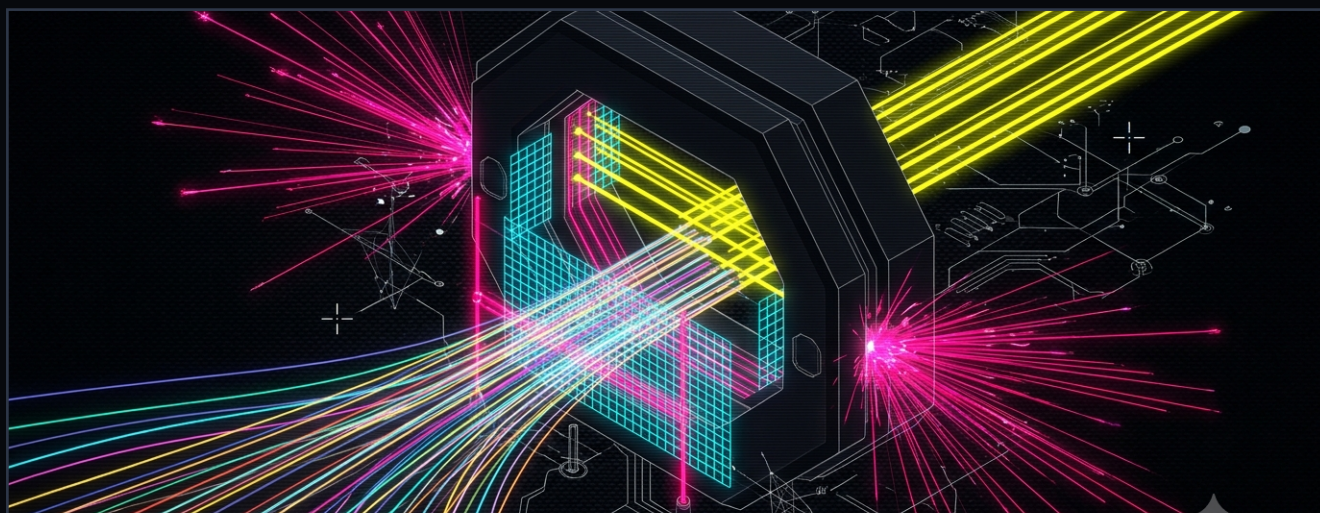
WORKFOUNDRY / INGRESS SHIELD

Ingress Shield

Pilot Guide v6.0

Webhook Boundary + Agent Preflight

**A controlled pilot for declared connections
before authority widens.**





01 // OVERVIEW

Two surfaces. One deliberate boundary.

Ingress Shield is a controlled pilot for approved developers. It separates declared webhook traffic from read-only connection checks, so each can be understood without implying permission to act.

WEBHOOK BOUNDARY**Protect the route**

Protect and observe declared webhook traffic on a reviewed route. Verify the request, bound the delivery, and retain redacted operational evidence.

AGENT PREFLIGHT**Check before action**

Use a bounded, account-scoped, read-only MCP interface to inspect a proposed webhook or AI-agent connection before any separately reviewed decision.

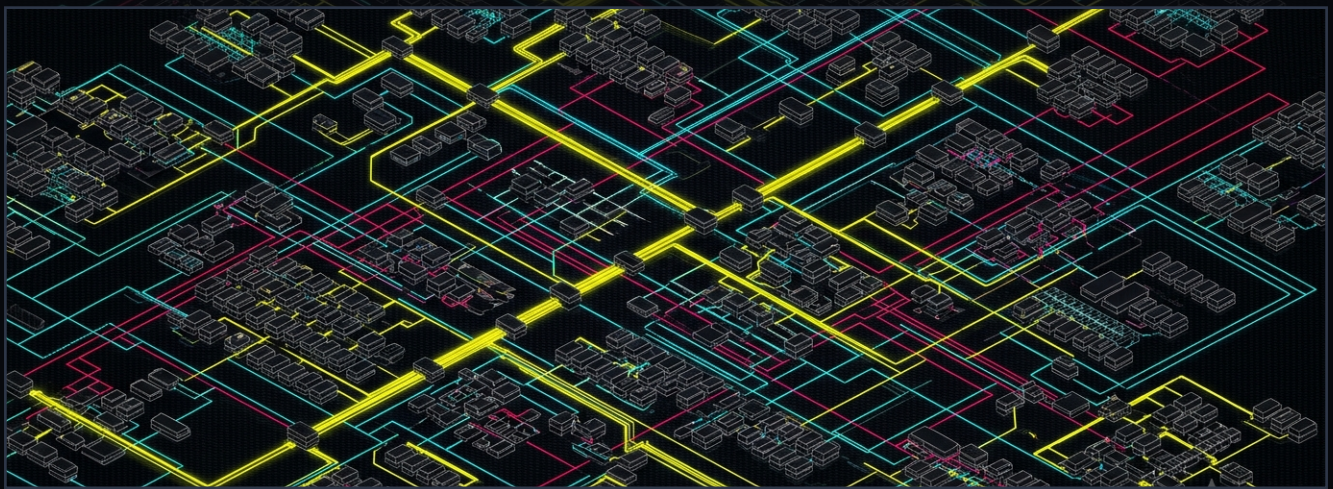
What this guide does and does not cover

It explains the public pilot, its two surfaces, illustrative use cases and the public-safe route into review. It does not create an account, grant access, request credentials, promise availability, or approve a business-critical workload.

02 // WHY THIS EXISTS

Connections should not arrive with ambient authority.

An AI agent or third-party webhook can introduce fragile hand-offs, unexpected formats, credential exposure, or an assumption that a compatible connection is automatically approved.



Declare the connection

Check the contract

Review authority
separately

Observe with redacted
evidence

The core principle is simple: a connection can be made explicit and checked without being given permission to run. A compatibility result is evidence for review, not a security guarantee or an operational approval.



03 // WEBHOOK BOUNDARY

Declared traffic. Bounded delivery.

Webhook Boundary is the Ingress Shield surface for declared webhook traffic on a reviewed route. It exists to make the first traffic path deliberate, narrow and reviewable.

Declared source
profile

Exact route and
method

Validate and
normalise

One sandbox
receiver

Redacted receipt

01

Input

Only the agreed source profile and JSON request shape are accepted.

02

Delivery

Accepted traffic goes only to one predeclared HTTPS sandbox destination with bounded retry.

03

Evidence

Outcomes retain reason code, timestamp and digest rather than payload logs.

04

Not included

No arbitrary relay, self-service destination manager, credential store, or production delivery platform.



04 // WEBHOOK BOUNDARY CONTROLS

Make the route explicit before it can affect anything downstream.

The pilot uses a declared boundary rather than a general-purpose integration surface.

SOURCE**Source**

Signed-request verification and declared-source checks.

SHAPE**Shape**

Exact route and method, JSON validation, and body-size limits.

FRESHNESS**Freshness**

Stale-request and replay rejection.

LOAD**Load**

Per-source rate and concurrency limits.

FORMAT**Format**

Declared field mappings normalise accepted JSON into one consistent event.

EVIDENCE**Evidence**

Redacted outcome, retry count, timestamp and digest only.

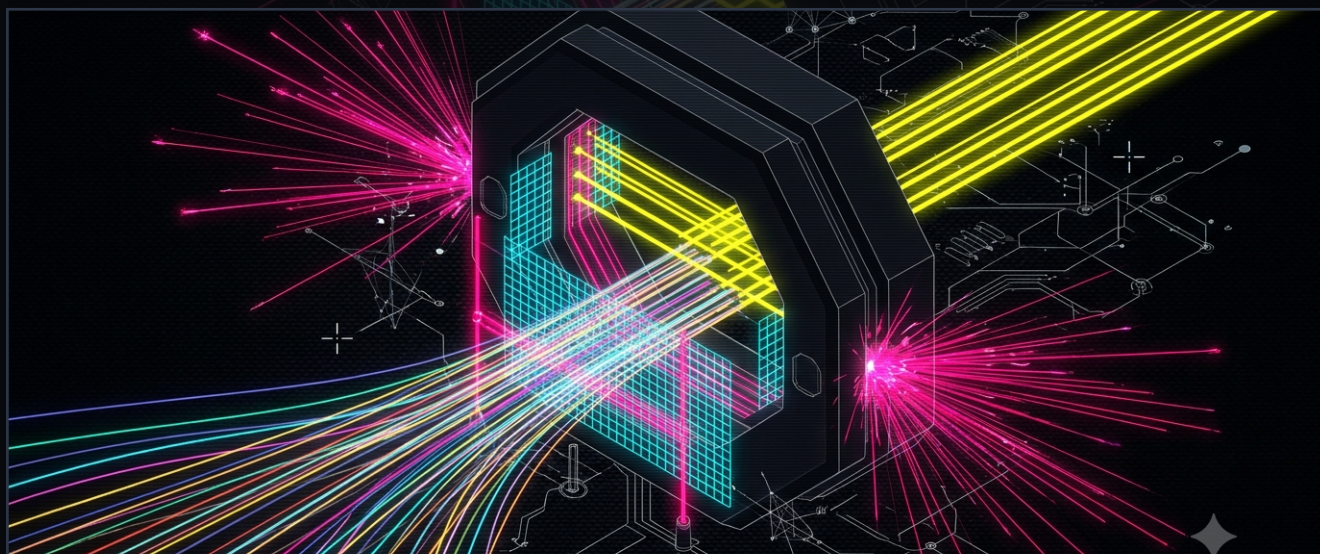
Raw bodies, destination responses and credentials are not written to receipt history. These controls reduce a declared integration risk; they do not amount to a universal security promise.



05 // SANDBOX DELIVERY

A sandbox is an explicit review boundary, not a marketing label.

The first delivery is deliberately boring: one named source, one reviewed route, one predeclared HTTPS sandbox receiver, and evidence that does not become a payload log.



Webhook source

Webhook Boundary

Sandbox receiver

Redacted receipt

The pilot has no contractual uptime guarantee or SLA and is not approved for business-critical live workloads. Adding a destination or broadening scope is a separate human review decision.



06 // AGENT PREFLIGHT

Useful to an agent. Not authority for an agent.

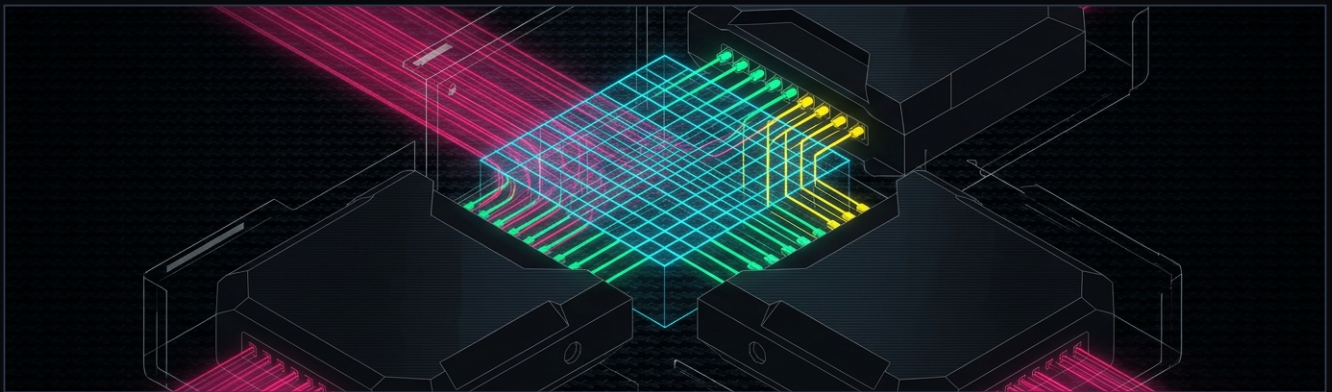
Agent Preflight is the Ingress Shield surface for bounded, account-scoped, read-only connection checks using the Model Context Protocol (MCP).

CAN**Inspect a declared draft**

Check declared inputs and outputs, compare safe drafts, receive a starting plan, and read the caller's own bounded result or explanation.

CANNOT**Widen authority**

It cannot access secrets, configure destinations, sign policy, queue or execute work, activate workflows, or make arbitrary network calls.



A read-only tool check is intentionally separate from permission to run work. It helps a person or approved agent understand a declared connection before a sensitive system is involved.



07 // SYNTHETIC EXAMPLE

Catch a mismatch before it becomes an action.

This example is synthetic. It illustrates an incompatible hand-off; it does not describe a framework integration, automatic repair, or execution.

customer.created/v1

Agent Preflight

payment.cleared/v1

CONNECTION RESULT**INCOMPATIBLE**

The declared producer cannot satisfy the required consumer event. The useful result is not a silent rewrite. It is a bounded next action: correct the expected schema, add the missing field, insert an explicit adapter, or request human review.

Compatibility is not authority.

A compatible result would still not grant a destination change, credential use, request send, deployment, or workflow execution.



08 // TOOL-CHAIN PREFLIGHT

Make each hand-off visible.

A useful preflight maps the connection between tools before one tool is asked to run on the next tool's assumptions.

01

Map every hand-off

Record fields, types, meaning, requiredness and limits.

02

Find the gap

Identify missing inputs, stranded outputs, or incompatible types and meanings.

03

Propose a visible fix

Add a field, correct the schema, remove an unused output, or name an explicit adapter.

04

Review separately

A draft can be corrected and re-checked without becoming production authority.

Agent Preflight can explain a draft. It cannot silently rewrite it or infer that the caller has authority to operate the connection.



09 // REPAIR SAFELY

Fix the mismatch. Keep the authority separate.

A correction should be visible, reviewable and re-checkable while the connection remains a draft.

Name the failed
hand-off

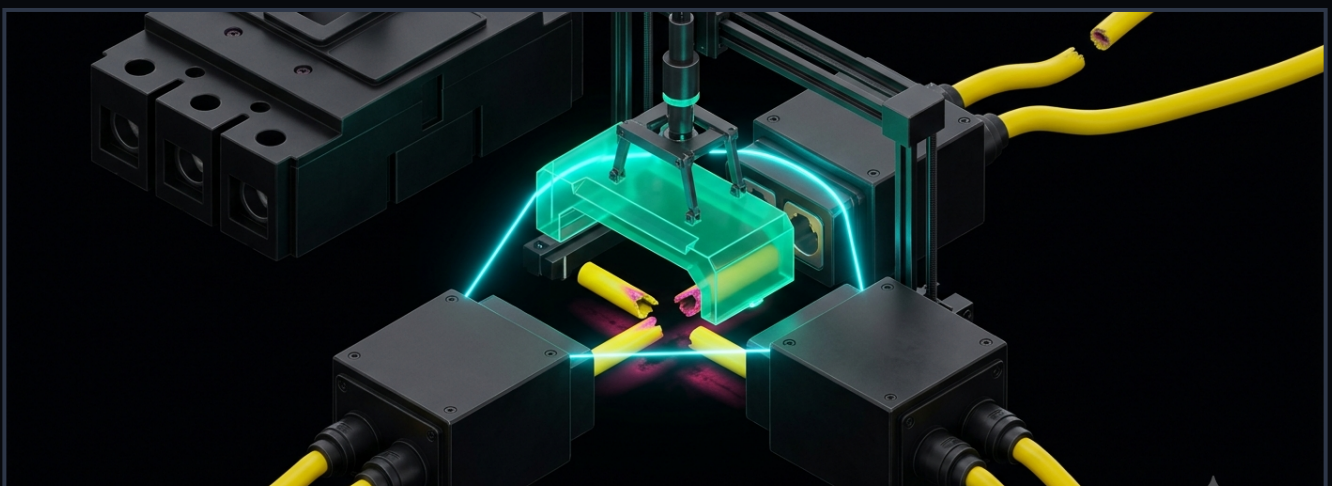
Correct the declared
contract

Re-check the draft

Review operational
change separately

A safe repair identifies the producing tool, receiving tool and the exact point that does not fit. It distinguishes a missing field from the wrong data type, different meaning, or an output that no later tool uses.

Make the correction visible in the workflow draft. A compatible draft is not permission to use credentials, send a request, configure a live destination, or execute work.





10 // WHERE IT FITS

Choose the job before choosing the tool.

Webhook Boundary and Agent Preflight work beside delivery and integration platforms. They are not a replacement for a general production delivery stack.

DELIVERY PLATFORMS**Operate the path**

For general delivery, routing, retries, monitoring and production event infrastructure, use a dedicated webhook platform.

INTEGRATION PLATFORMS**Operate the workflow**

For many SaaS or API integrations, credentials, synchronisation, and execution workflows, use an integration platform.

INGRESS SHIELD**Declare, bound and check before authority widens**

Webhook Boundary supports a reviewed sandbox or pre-production route. Agent Preflight checks a declared connection before action. Neither is an arbitrary relay, a self-service destination manager, or an execution API.



11 // REQUEST A CONTROLLED PILOT

Start public-safe. Agree the boundary before onboarding.

Pilot applications are manually reviewed. Describe the connection, not the secrets behind it.

Include

- [] Your name and organisation or project
- [] Whether you need Webhook Boundary or Agent Preflight
- [] Declared source, target, route, expected format and intended outcome
- [] The HTTPS sandbox receiver you control, where relevant
- [] Expected non-production use and the operational question you want answered

Do not send

Credentials, signing secrets, private keys, personal data, confidential payloads, or private endpoints by email.

Email ingress-shield@workfoundry.co.uk with a public-safe outline. WorkFoundry agrees scope, data boundary and secure onboarding separately.

ATOM FLUX IS THE LOCAL-FIRST OPERATING SUBSTRATE BENEATH GOVERNED SOFTWARE.
LAMINA IS AN EMERGING PRODUCT DIRECTION, NOT A FINISHED HOSTED SERVICE.