

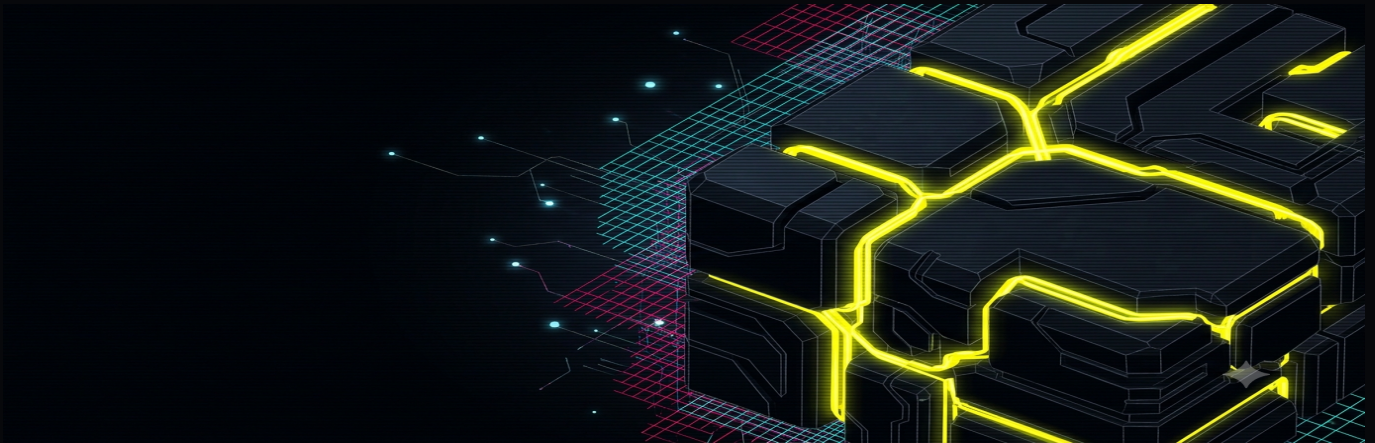


PRODUCT OVERVIEW // CONTROLLED PILOT

Atom Flux Ingress Shield

Safeguarding AI-agent connection checks and inbound webhook integrations.

Ingress Shield helps teams inspect a proposed connection before it reaches sensitive systems. It separates read-only preflight from permission to run work, keeps onboarding deliberately bounded, and returns redacted operational evidence rather than payload logs.



THE CUSTOMER PROBLEM

AI agents and third-party webhooks can introduce three linked operational risks: unbounded tool authority, exposure of credentials or payloads, and fragile integrations that fail when an upstream format changes.

UNBOUNDED AGENT AUTHORITY

Agents must not receive ambient access to production databases, terminals, deployment controls, secrets, or route configuration.

CREDENTIAL AND PAYLOAD EXPOSURE

Raw authorization values and customer payloads must not become routine logs, diagnostics, or public records.

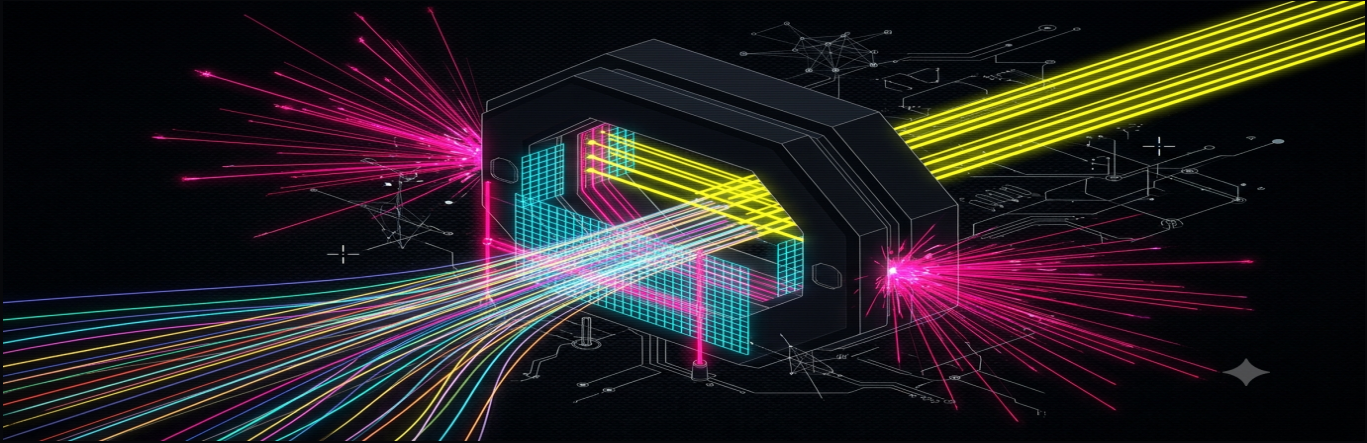
INTEGRATION FRAGILITY

Schema drift and unexpected formats should be caught at a declared boundary before they create downstream failures.



PRODUCT 1 // INBOUND WEBHOOK SECURITY

A bounded traffic plane for declared integrations.



For an approved pilot, the gateway verifies a declared source, applies route and format checks, normalises accepted JSON into a consistent event shape, and delivers only to a predeclared HTTPS sandbox destination. It is not an arbitrary relay and it does not grant execution authority.

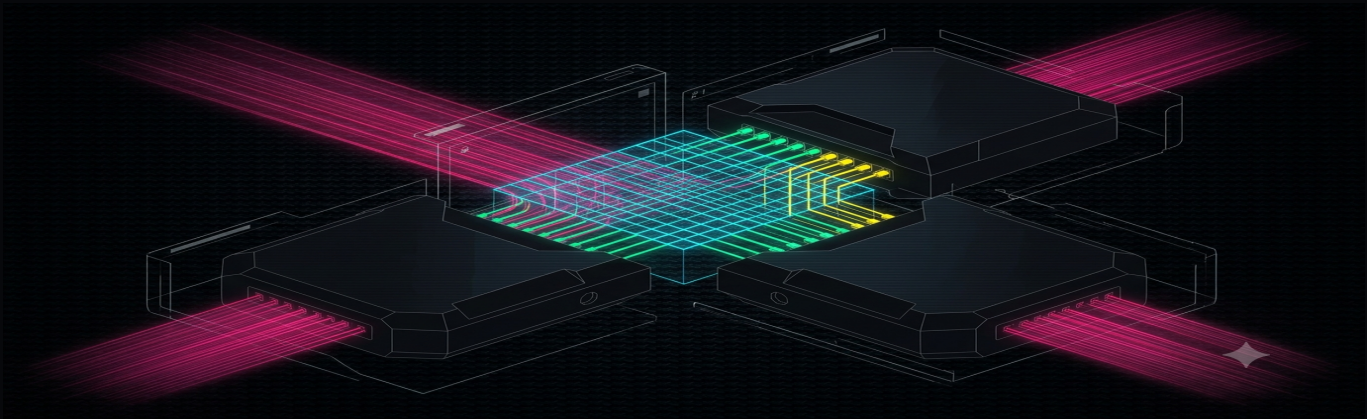
PILOT BOUNDARY

CONTROL	PILOT BOUNDARY
Request shape	Declared JSON request and source profile only
Authentication	Declared signature validation; no secret disclosure
Delivery	One predeclared HTTPS sandbox destination; bounded retry
Evidence	Redacted outcome, reason code, timestamp and digest only
What it never does	No arbitrary destination, secret retrieval, deployment, or execution



PRODUCT 2 // HOSTED MCP PREFLIGHT

A read-only AI-agent entry point.



Approved coding and agent clients connect to the hosted Model Context Protocol endpoint at <https://ingress.workfoundry.co.uk/mcp>. The interface supports bounded, account-scoped, read-only preflight and discovery. It is deliberately separate from permission to run work.

WHAT AN APPROVED CLIENT CAN DO

READ-ONLY ACTION	OUTCOME
Check a tool connection	Identify whether declared inputs and outputs fit together, including missing information.
Check a workflow draft	Receive a bounded compatibility report without starting work or reserving execution capacity.
Compare or scaffold a safe draft	Review safe differences or receive an unsigned starting draft for human review.
Review a multi-seam readiness pack	Bring related declared checks into one ordered, redacted result: what fits, what stopped, and the next human-review action. It cannot approve, deploy, or run the change.
Read caller-owned status	Retrieve a bounded result or corrective explanation for an account-owned request.

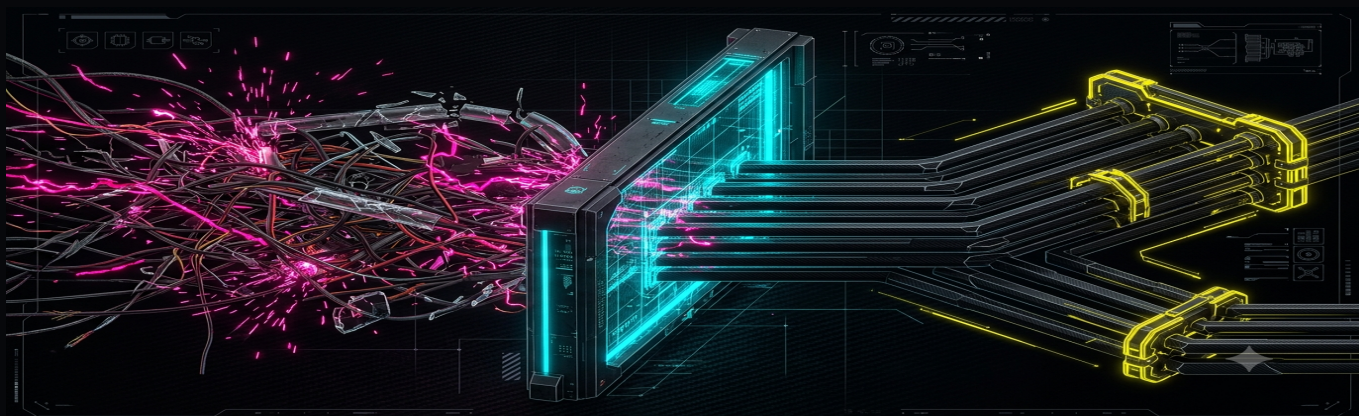
NO-AUTHORITY GUARANTEE

The hosted MCP cannot access secrets, configure webhook destinations, sign policies, queue or execute work, activate a workflow, or make arbitrary network calls.



ONBOARDING // EXPLICIT BOUNDARIES

Start with evidence, not operational risk.



Ingress Shield uses a controlled, review-led pilot path. The first step is a public-safe description of a connection or sandbox use case. WorkFoundry then agrees the scope, data boundary, and secure onboarding separately.

LOW-RISK PILOT PATH

1. DISCOVERY

Describe a public-safe webhook or agent-tool connection. Do not send credentials, private keys, personal data, or confidential payloads.

2. OBSERVE AND PREFLIGHT

Use sandbox or pre-production traffic and read-only checks to surface drift, mismatches, and operational constraints before any broader change.

3. HUMAN REVIEW

Any change beyond the controlled pilot remains a separate human decision with its own scope, authority, and rollback requirements.

REQUEST A CONTROLLED PILOT

For a public-safe conversation about a webhook or AI-agent connection-checking use case, contact ingress-shield@workfoundry.co.uk. Pilot applications are reviewed manually. This brief describes a controlled pilot; it is not an SLA, open self-service offer, or business-critical production-workload approval.