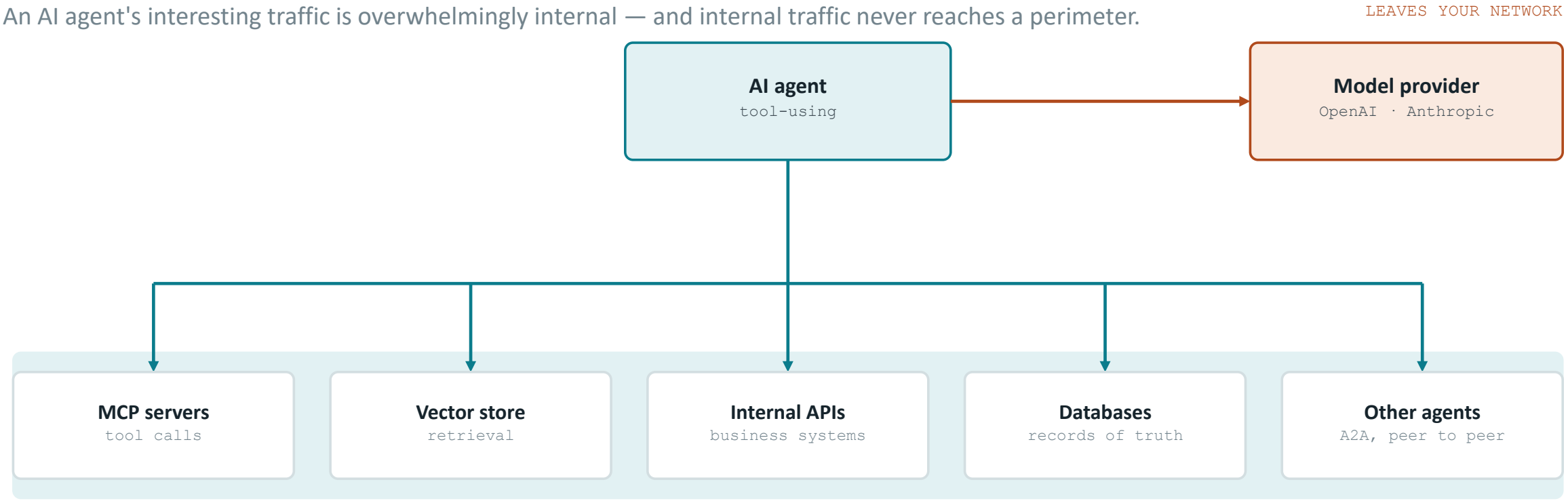
THE SHAPE OF THE PROBLEM

One flow leaves your network. The rest never do.

An AI agent's interesting traffic is overwhelmingly internal — and internal traffic never reaches a perimeter.



"If an adversary is able to take control of an AI agent's behavior, they effectively gain the same level of access as the agent."

MITRE ATLAS 2026.07, technique AML.T0112.000 — Local AI Agent

TWO DIFFERENT CONTROL PLANES

Two questions. Only one of them is a content question.

DATA GOVERNANCE

“Is what is being said acceptable?”

Read the prompt, the response, the tool call. Decide whether the content is safe, compliant and grounded.

This is what Prisma AIRS does, and it does it well.

ACCESS GOVERNANCE

“Should this conversation exist at all?”

Decide whether this specific workload is authorised to reach that specific service — before any path between them exists.

This is what NetFoundry does.

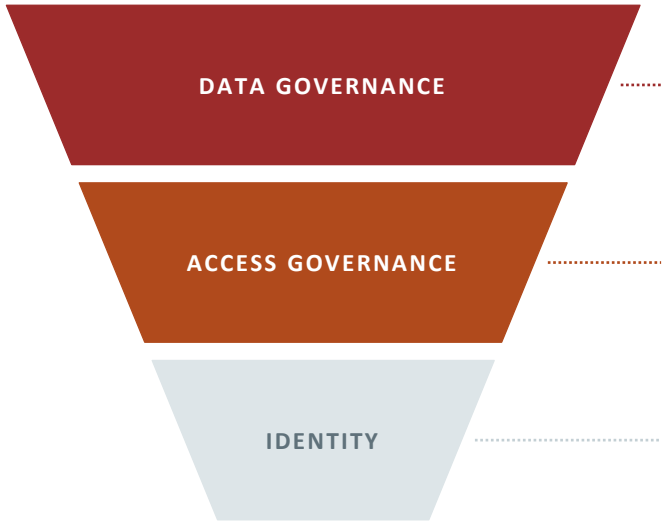
Neither one can do the other's job — and the order matters.

Inspection operates on whatever an agent can already reach. Authorisation is the only control that changes the size of that set. Every service an agent can reach is a classification, retention, residency and audit obligation — so access governance is what makes data governance tractable, and what makes it enforceable.

THE GOVERNANCE STACK

“Identity first Connectivity’ shrinks scope of Data Governance

CURRENT STATE IP-based segmentation

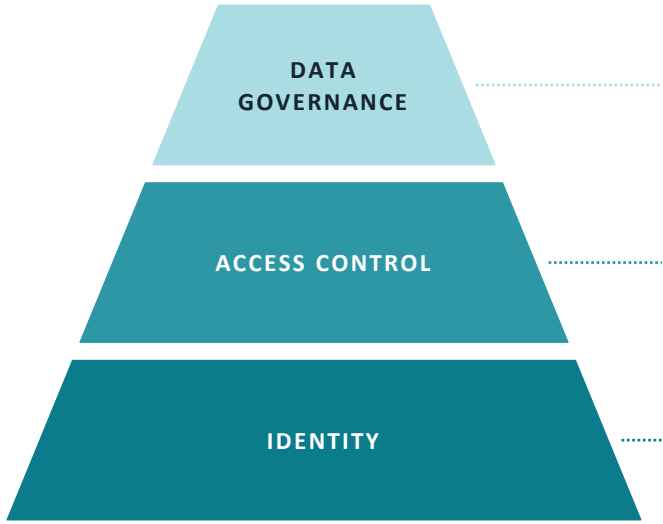


Costly Inspection
Everything reachable must be inspected and over 95% of it is encrypted

Complex Ops
VLANs · VRFs · ACLs · NAT

Weak Identity
IP address + port

WITH NETFOUNDRY identity-based access



Optimized Inspection
Only permitted flows to inspect

Simplified Ops
Authenticated and authorised only

Strong Identity
x509 per workload, checked every connection

KEY PAIN POINTS

- Identity is an IP address — reassigned, NAT'd, spoofable
- **82%** of intrusions are malware-free: attackers log in
- **44%** name network complexity a top-three segmentation barrier
- **90%** segment · only **35%** microsegment — reachability stays broad
- Same appliance: **60 Gbps** firewall only · **2 Gbps** inspecting TLS
- **29 minutes** to move laterally · **247 days** to detect and contain

VALUE DRIVERS

- Identity is x509 — cryptographic, verified every connection
- Deny by default — no policy, no path, no listening port
- Data governance inspects **only** authorised flows
- No decryption needed — authorisation is on the certificate
- Ransomware contained **21%** faster with microsegmentation — **33%** at $1B+ firms
- Average breach cost **–$226K** with strong IAM, **+$177K** when over-privileged

CrowdStrike GTR 2026 · Akamai Segmentation Study 2025 (n=1,200) · IBM Cost of a Data Breach 2026 · Check Point QF 9200 datasheet, Jul 2026 · CyberRatings.org 2025 — every figure links to its source

What Prisma AIRS does well, and we do not do at all

If you have already bought this, keep it. We are not asking you to replace any of it.

Prompt and response inspection

Prompt injection, toxic content, malicious code and URLs, custom topic guardrails, contextual grounding for hallucinations.

Data loss prevention

Sensitive-data detection with masking, and database query regulation on the model's generated SQL.

Model supply chain

Scanning 35+ model file types for deserialization threats, neural backdoors, unsafe formats and invalid licences.

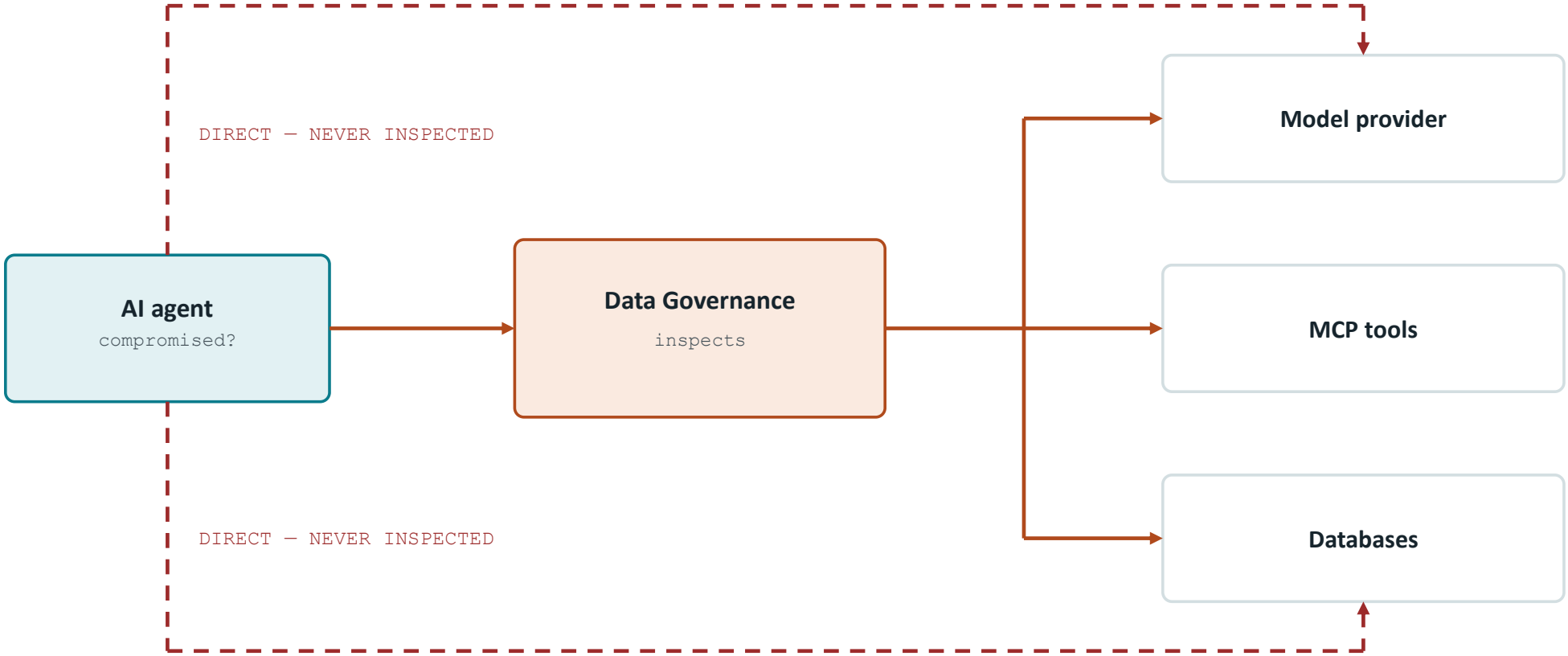
Continuous red teaming

50+ attack techniques across 500+ scenarios, mapped to OWASP, NIST and MITRE ATLAS.

Palo Alto Networks product documentation, docs.paloaltonetworks.com/ai-runtime-security — verified 25 Aug 2026

‘Data Governance’ is a chokepoint only if it is the only route

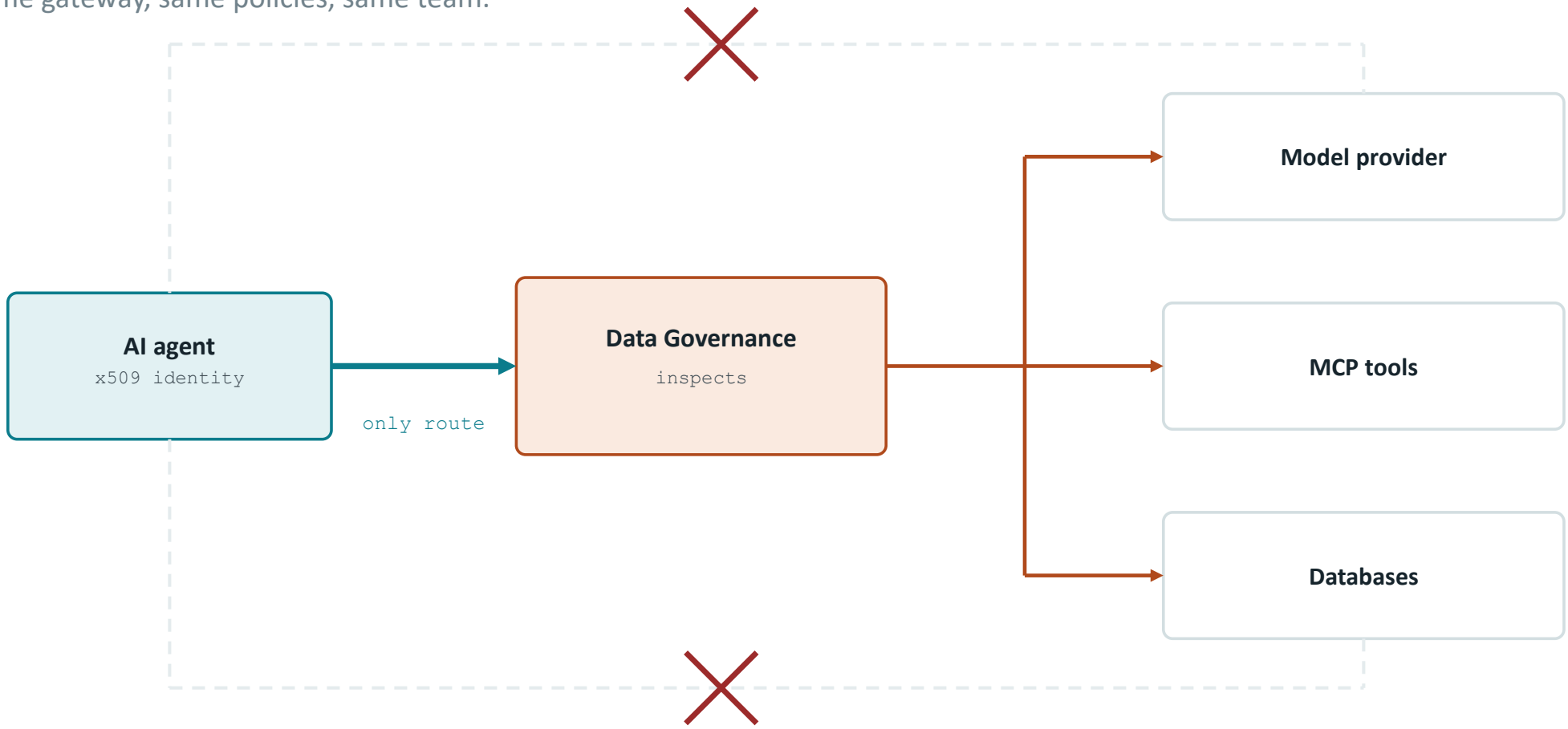
Deploy the governance stack, leave the network as it is, and it governs the traffic the agent chose to send through it.



WHAT NETFOUNDRY CHANGES

Make it the only route

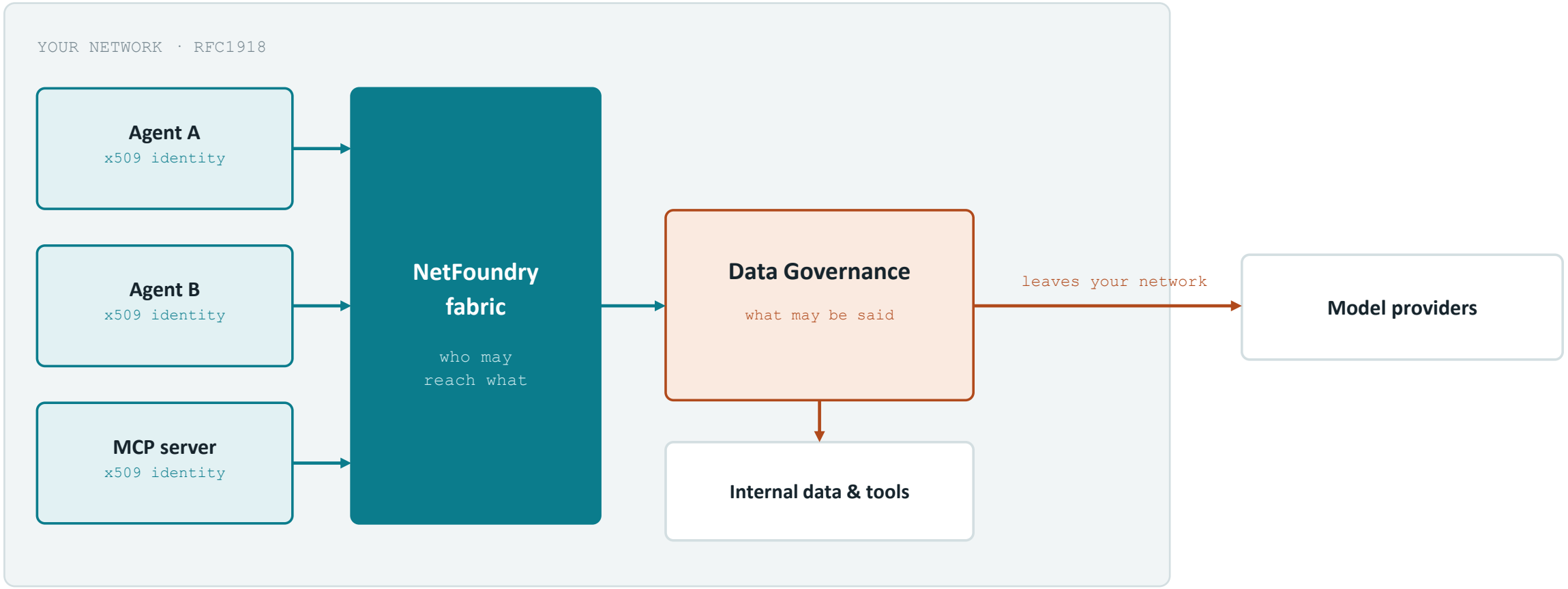
Same gateway, same policies, same team.



Your coverage number becomes 100% by construction, not by discipline.

THE COMBINED ARCHITECTURE

Both layers, doing the job each is actually good at



ONLY authenticated and authorized agents reach the data governance layer — and nothing else. Data governance is ‘brute force’ and expensive, NetFoundry reduces scope of data governance to only permitted flows.

THE DIVISION OF LABOUR

Who owns which control

CONTROL	PRISMA AIRS	NETFOUNDRY
Prompt & response inspection	**Owns it — injection, toxicity, grounding**	None. Not attempting it.
Data loss prevention	**Owns it — detection and masking**	None.
Model supply chain	**Owns it — 35+ file types scanned**	None.
Workload identity	Idira issues SPIFFE SVIDs — a separate product	**x509 on every connection, mutual TLS**
Who may reach what	Zone, IP, tag on an IP, App-ID signature	**The identity itself — dial and bind policy**
Default posture	Inspect, then permit or deny	**No policy, no path — allow-list only**
Reachability of the inspection point	Depends on configuration	**Architectural — no alternate route exists**
Runs with nothing leaving your estate	Control plane is SaaS on both AIRS paths	**Self-hosted and air-gapped supported**

Compiled from published vendor documentation on both sides. Full evidence base with verbatim quotes available on request.