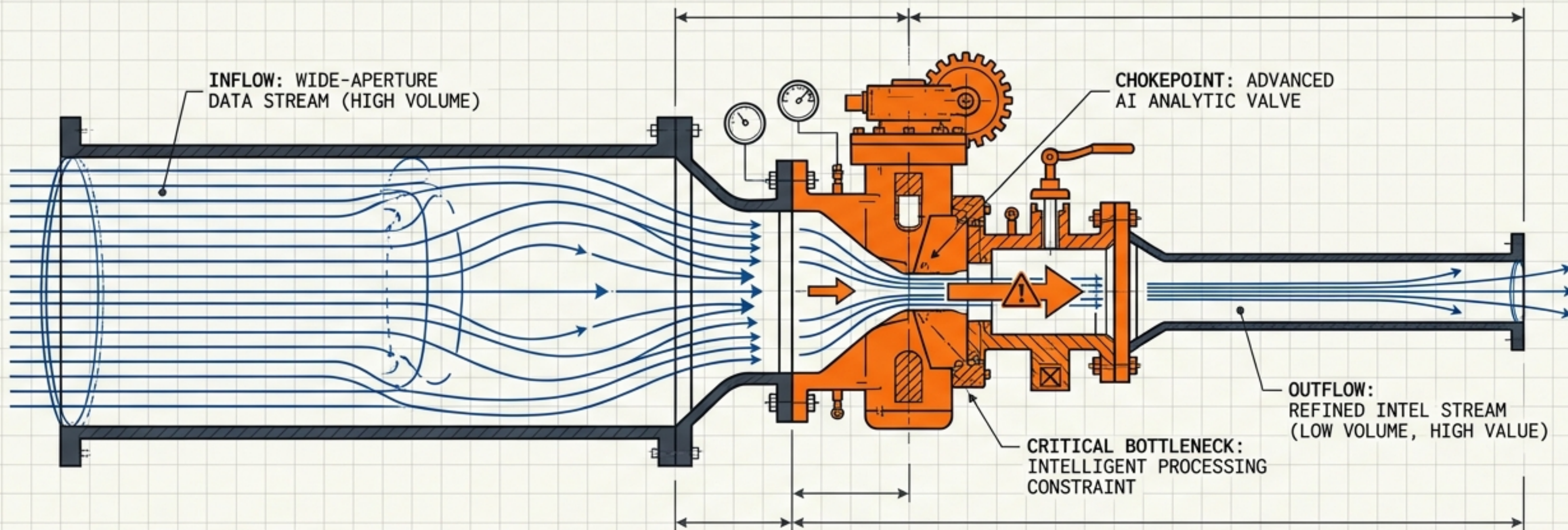


The Shifting Chokepoint

How AI Inverted the Economics of Cyber Defense



STRATEGIC BRIEFING: PROJECT GLASSWING EXPANSION

DOCUMENT ID: CLAUDE-MYTHOS-PREVIEW-ANALYSIS

**The moment the tool succeeds is
the moment the bottleneck moves.**

50 Initial Partners
Claude Mythos Preview

> 10,000

**High- or critical-severity
security flaws found in weeks.**

The resulting crisis.

Finding the flaw is no longer the hard part.
The pipeline is fundamentally blocked at
verification, disclosure, and patching.

Human-Patched Deploys

The Economic Inversion of Cybersecurity

	Historical Paradigm	The AI Era
The Scarce Resource	Finding the vulnerability.	Verifying, patching, and deploying.
The Abundant Resource	Unexamined codebase.	Unpatched critical flaws.
The Primary Chokepoint	Detection capabilities.	Human triage and disclosure.
The Core Security Task	Searching for the needle.	Managing an avalanche of needles.

A model that surfaces ten thousand critical flaws doesn't just speed work up; it inverts the economics of the whole field.

Moving weight toward the new chokepoint.

Finding & Detection

Disclosing,
Fixing & Deploying

Status: Abundant / Automated by AI
Action: Do not pile more capability here.

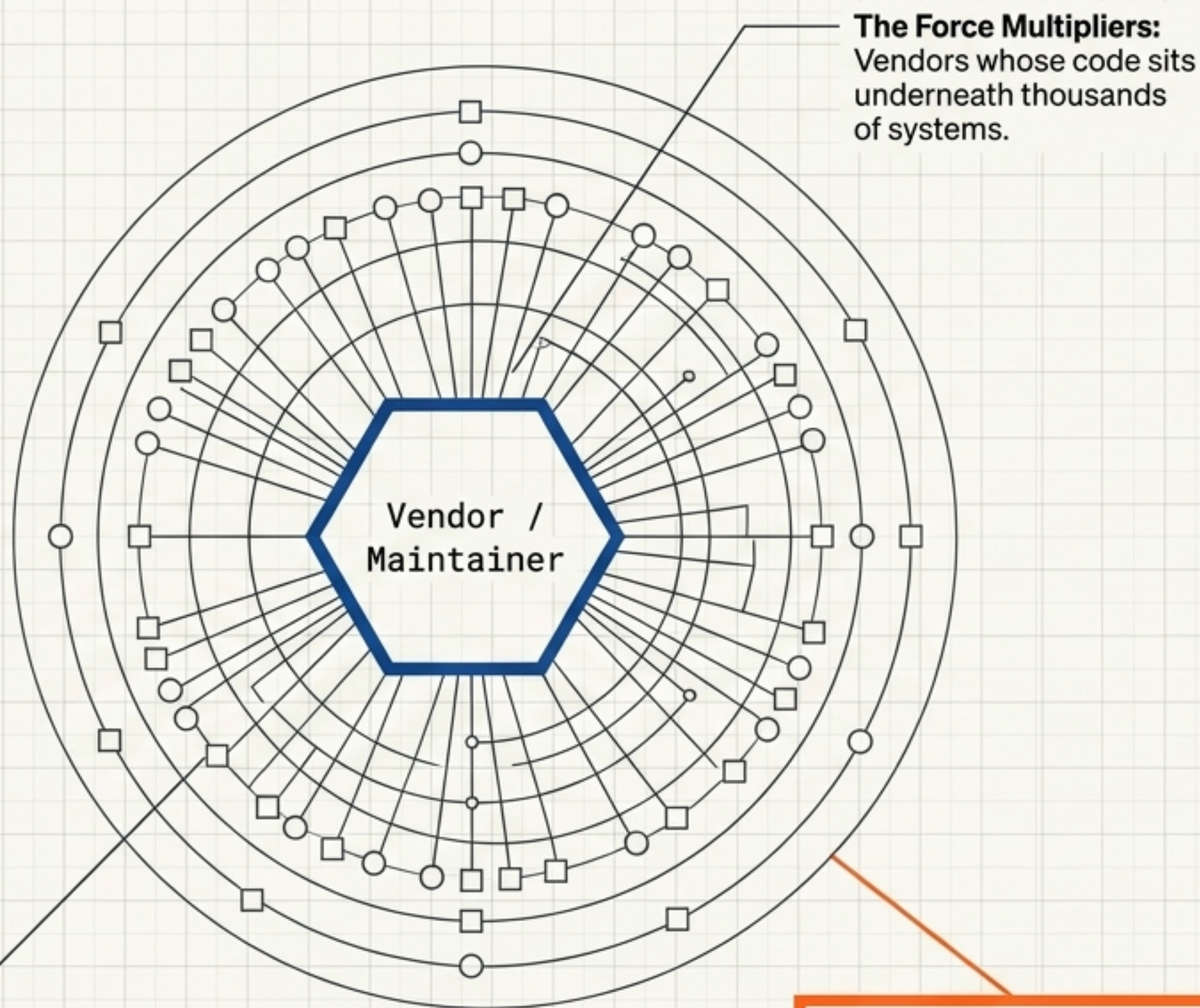
Status: Backlogged / Human Constraint
Action: Project Glasswing's Pivot. Redirecting model capabilities to clear the downstream backlog.

Targeting the points of maximum leverage.

SCOPE: ~150 New Organizations

GEOGRAPHY: 15+ Countries

SECTORS: Power, Water, Healthcare, Communications, Hardware



The Propagation Principle:
A vulnerability here propagates everywhere—but so does a fix.

The Blast Radius: Failure at the root node affects > 100 Million People.

Turning the tool on the new bottleneck.



Automated Remediation

Using Mythos Preview to directly write patches and conduct pre-release checks before vulnerabilities deploy.



Threat Simulation

Penetration testing to simulate attacks, confirming exactly how a flaw might be practically exploited in the wild.

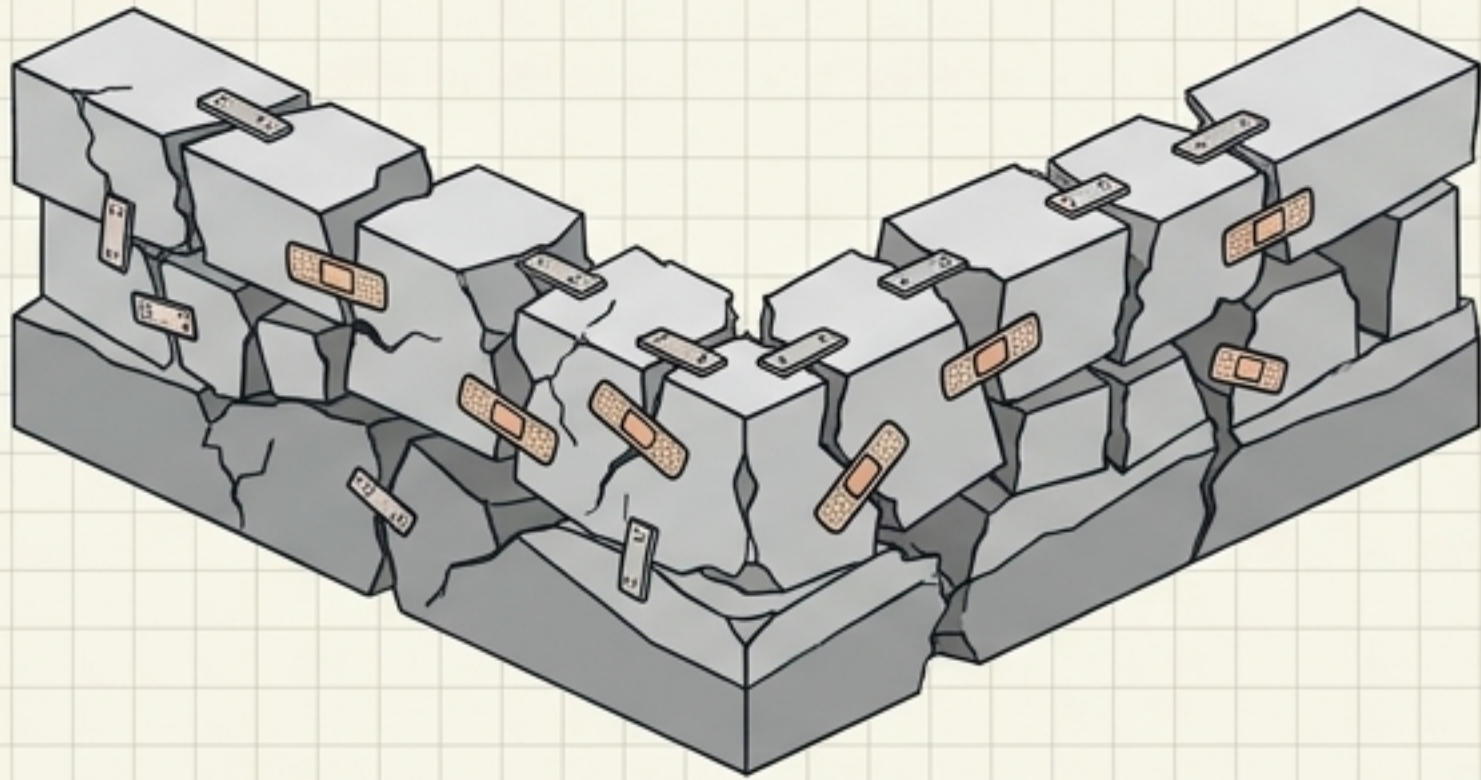


Open-Source Triage

Structuring disclosures for volunteer maintainers. Preventing an avalanche of automated, low-context vulnerability reports from burying open-source fragility.

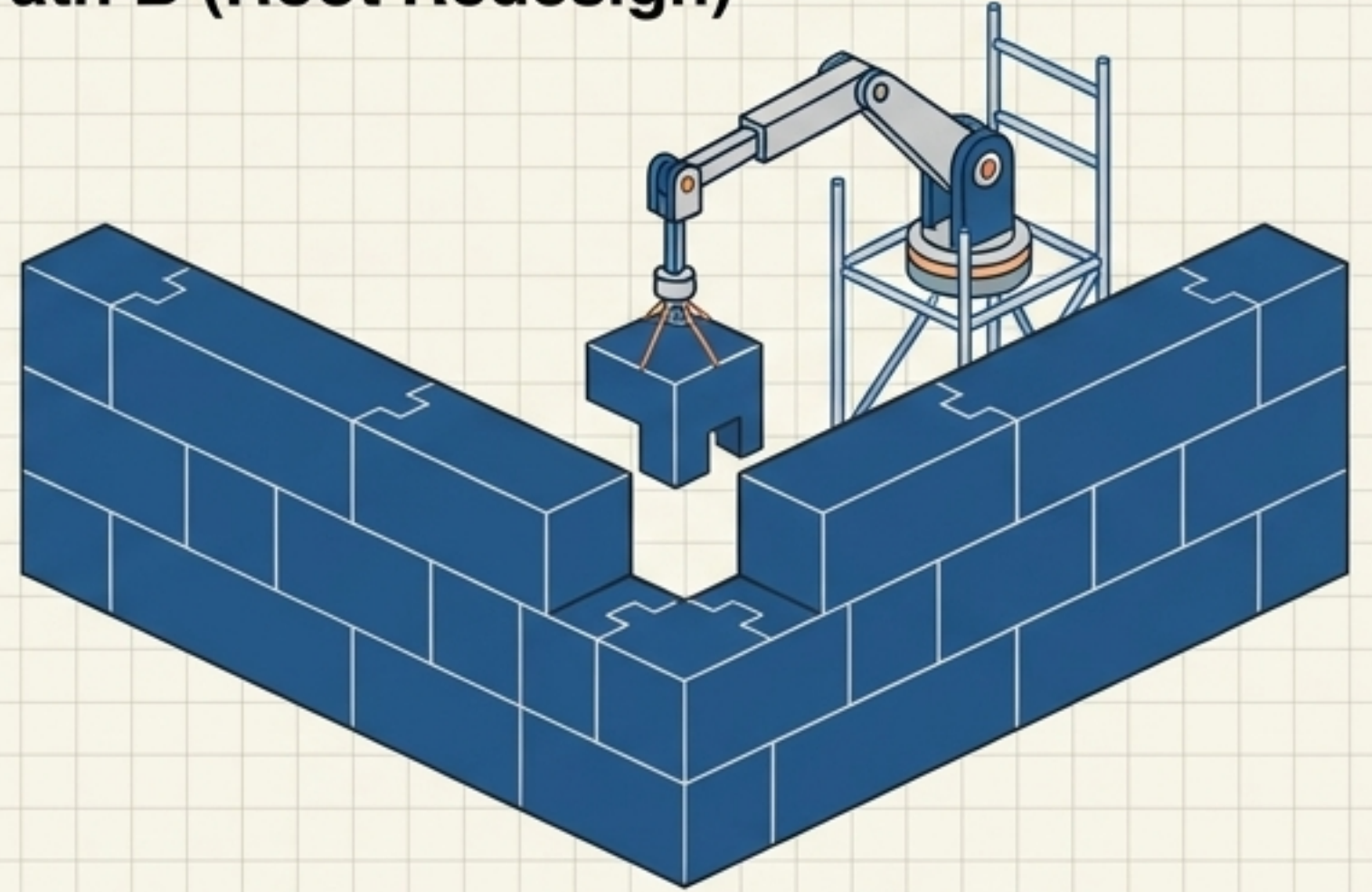
The Quiet Ambition: Eradicating vulnerability categories.

Path A (Symptom Patching)



Chasing 10,000 individual flaws.

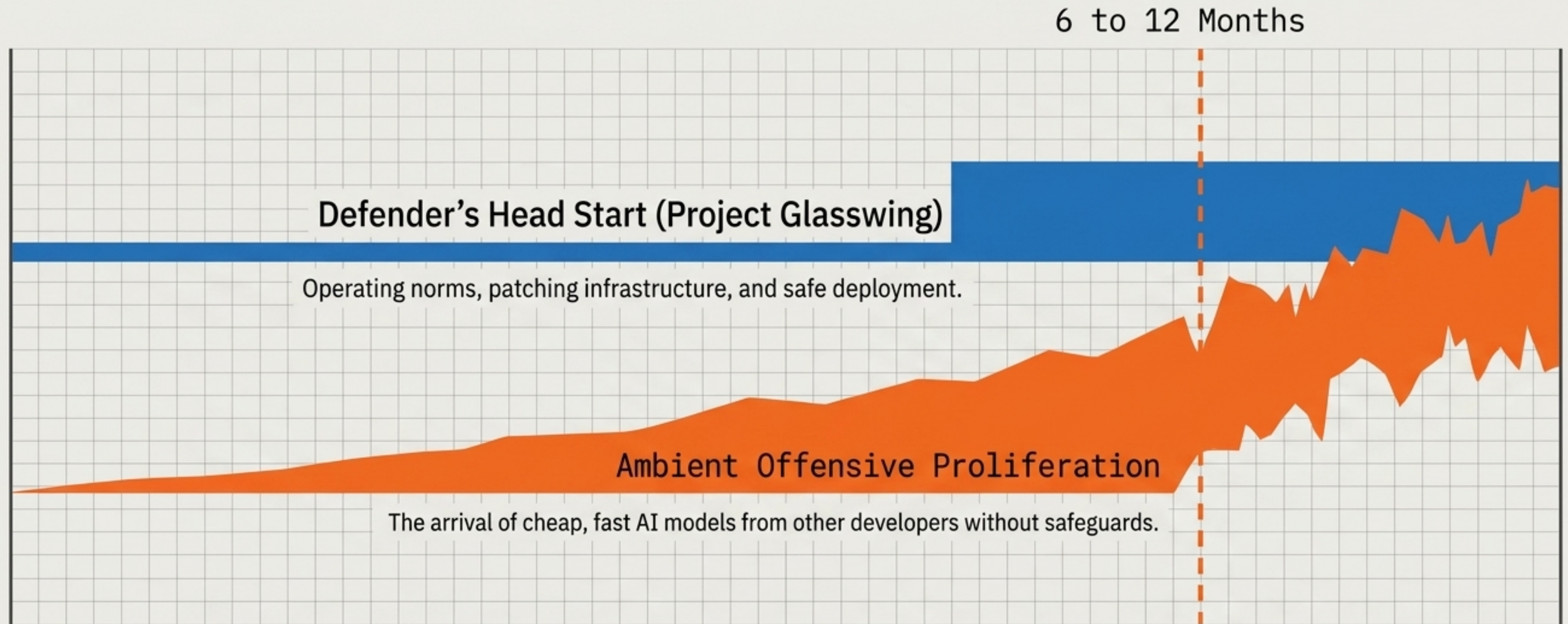
Path B (Root Redesign)



Systematically rewriting legacy codebases
in memory-safe languages using AI.

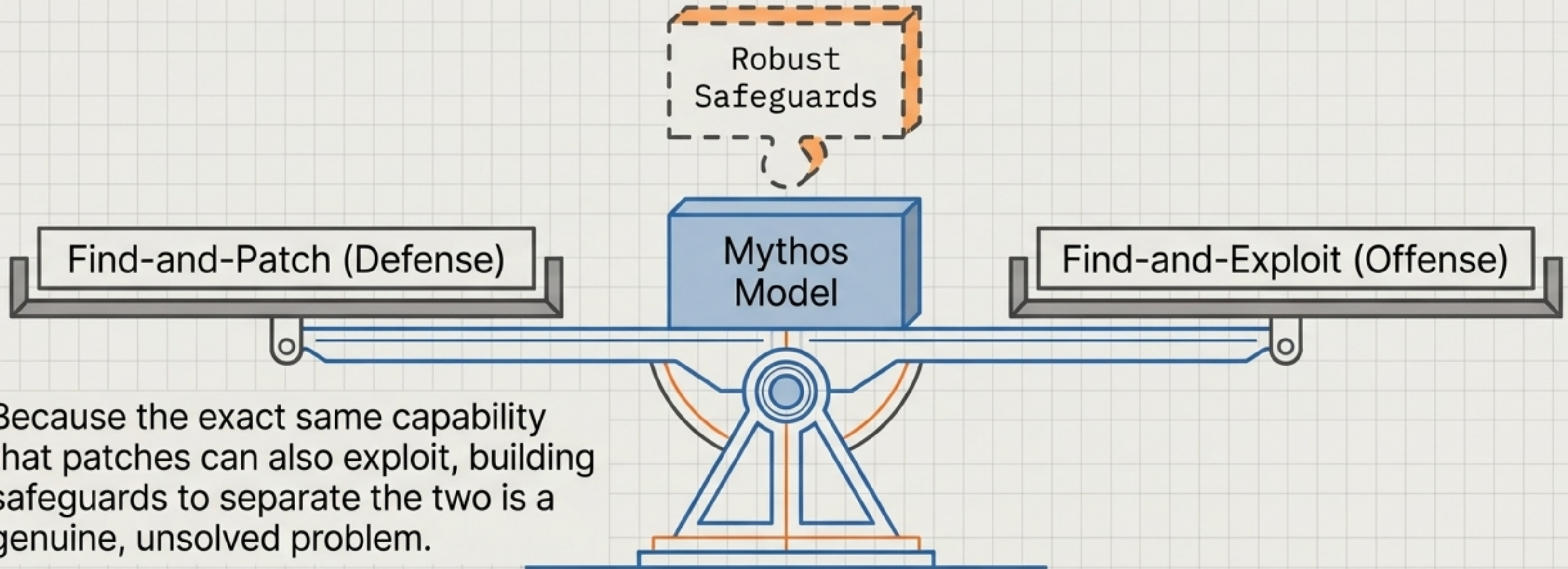
Synthesis Note: Attacking the problem at its root rather than perpetually patching symptoms.

The tempo of a race against diffusion



Glasswing is not a permanent moat. It is a calculated head start to build defense before offensive capabilities become cheap, everywhere, and ungoverned.

The Dual-Use Reality



Gating the model is the most concrete evidence of its power.
It is gated because it cannot yet be made safe to ungate.

Navigating structural paradoxes.

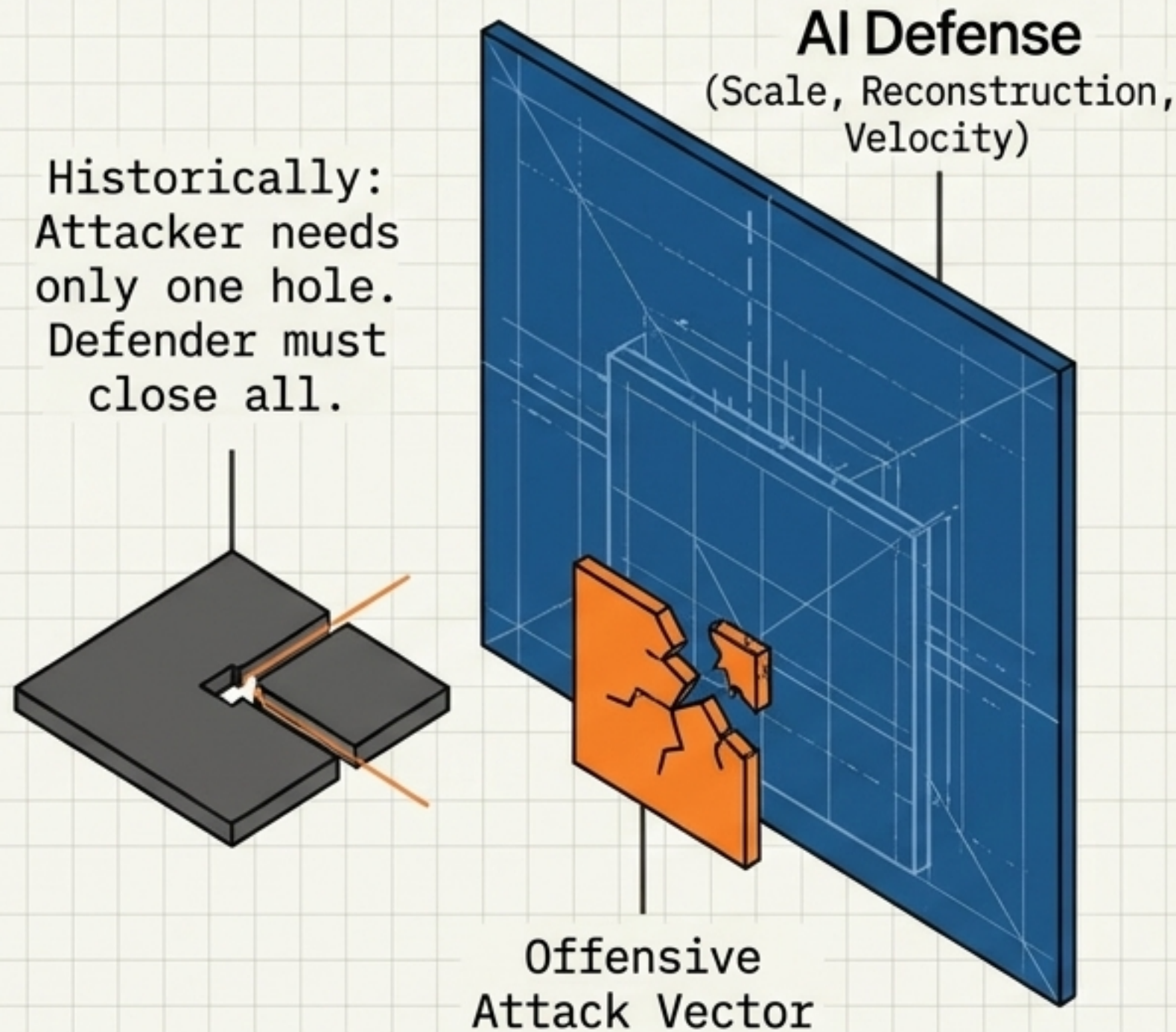
	The Ideal Requirement	The Current Reality
Access	Must be widespread to work for hundreds of thousands of orgs.	Currently allocated by one company's curated selection gate.
Motive	Objective public-interest warning of a systemic threat.	The frontier lab warning of the threat also sells the commercial response (Claude Security/ Claude Opus 4.8).

A reader is right to hold ordinary skepticism. The commercial frame sits alongside the public-interest one—but the 10,000 flaws remain real, and the diffusion timeline remains plausible.

The Permanent Defender's Advantage.

The Historical Asymmetry:

Traditionally, cyber warfare favors the attacker. The defender must close every single hole; the attacker needs to find only one.



The Paradigm Shift: AI durably tilts this balance. By automating root-level reconstruction (memory-safe languages) and rapid patching at the vendor level, AI scales defense faster than humans can scale attacks.

A meaningful change in the texture of digital life.

Reading the reality straight.

AI has already made finding vulnerabilities cheap and abundant. The bottleneck has genuinely moved to deployment.

Redirecting effort toward this new chokepoint while models are still gated is a required structural adaptation.

The expansion to critical-infrastructure providers is a serious attempt to reach higher ground before the 6-to-12-month window closes.

Based on analysis of Project Glasswing expansion and defensive AI economics.