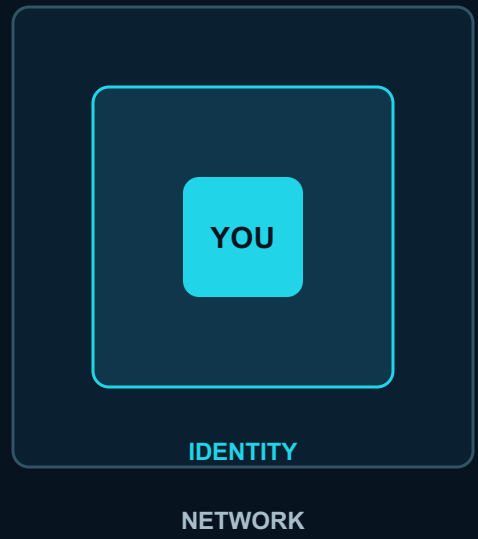
LAYER9i

Person-Controlled Internet Presence

A person-controlled Internet Presence



Identity, routing and trusted Internet delivery designed as one system

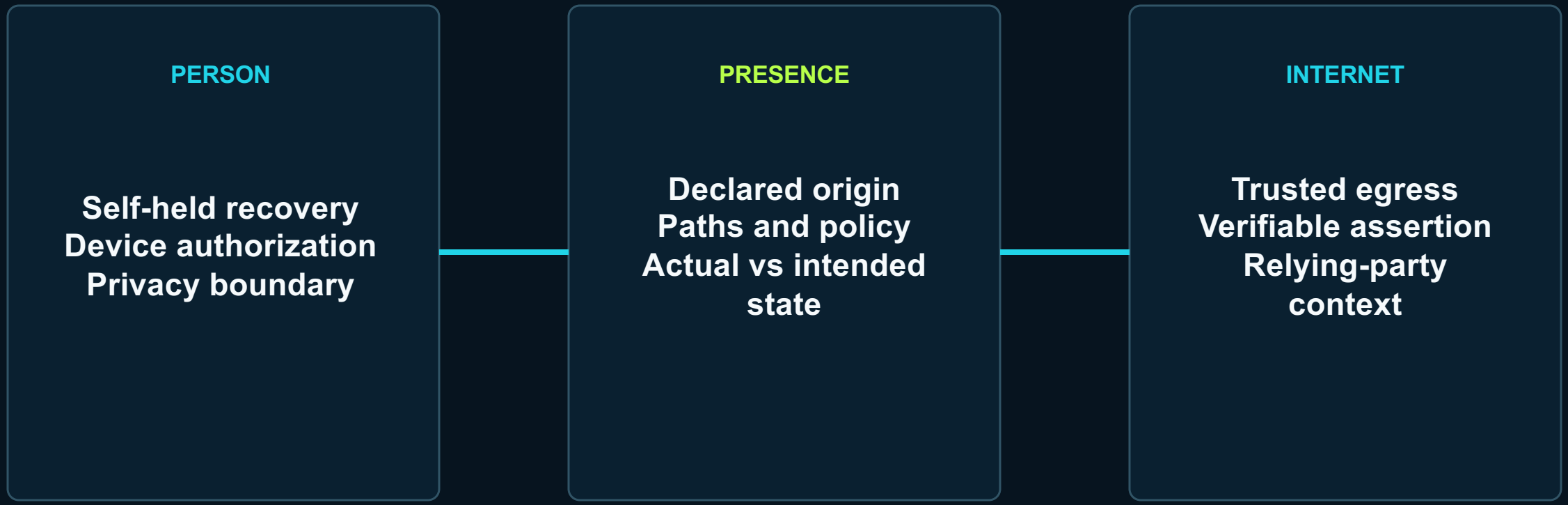
The internet recognizes connections, not people

Identity, network path and trust are managed by separate products

01	**Identity stops at sign-in**	A service can know who authenticated without knowing whether the network path still reflects that person’s intent.
02	**A public IP is borrowed context**	Travel, carrier changes and cloud egress alter how services see a person.
03	**Routing remains infrastructure work**	Users choose locations and tunnels, then troubleshoot failures with little explanation.
04	**Non-agent devices fall outside**	Travel devices, appliances and legacy hardware often cannot run a modern client.

The product unit is a persistent Presence

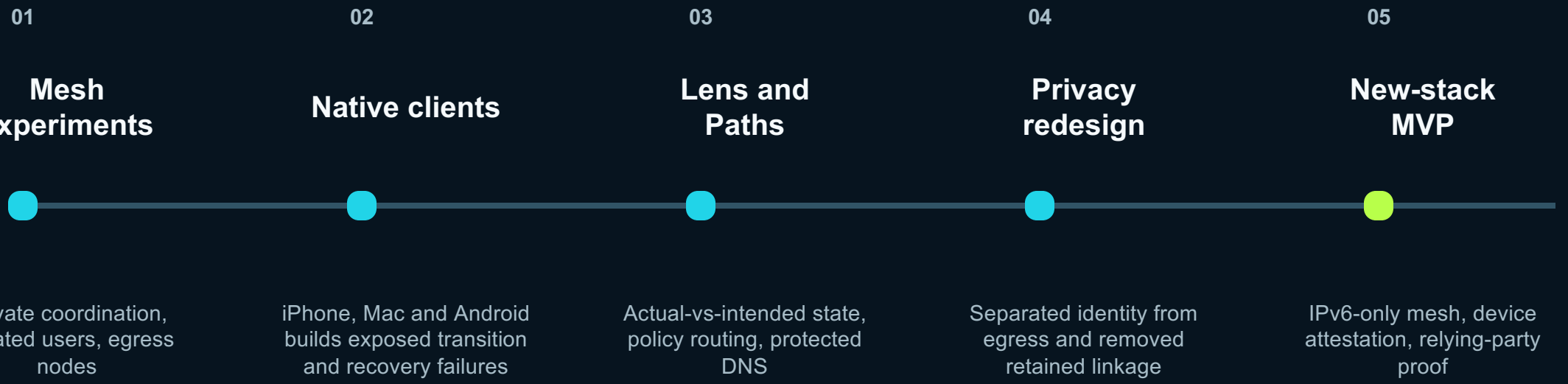
A Presence carries identity, authorized devices, intended routes and recovery across networks



One durable model across devices and networks

Atlas evolved through real network failures

Each phase narrowed the product from tunnel control toward person-controlled trust



The architecture changed when evidence contradicted assumptions

Evidence exists at the protocol and system level

Technical traction is real; commercial traction has not started

23 / 23

backend and contract test files passed

Closure candidate, Aug 31

2 keys

verified across live key rotation

Independent relying party

16 / 16

operational checks passed after DNS correction

Aug 13 baseline

4 regions

public IPv6 configured and outbound verified

NY, Toronto, London, control

Measured gaps

- **iOS state update missed the 5-second target**
- **Mac stability test ended after a false recovery trigger**
- **Several scorecard measures remain unmeasured**

Pre-revenue • no claimed customers • no claimed partnerships

Current state: a live trust core, with the client gate open

The September rebuild preserved proven infrastructure and retired the old Presence API

LIVE + VERIFIED

- **IPv6-only personal mesh**
- Device-bound identity sessions
- Pairwise relying-party identifiers
- Toronto egress without retained identity linkage
- Bank demo verifies published keys

HISTORICAL / RETIRED

- **Former /api/presence/* backend**
- Old enrollment and recovery flows
- Legacy Paths signing service
- Builds 723–725 as active clients

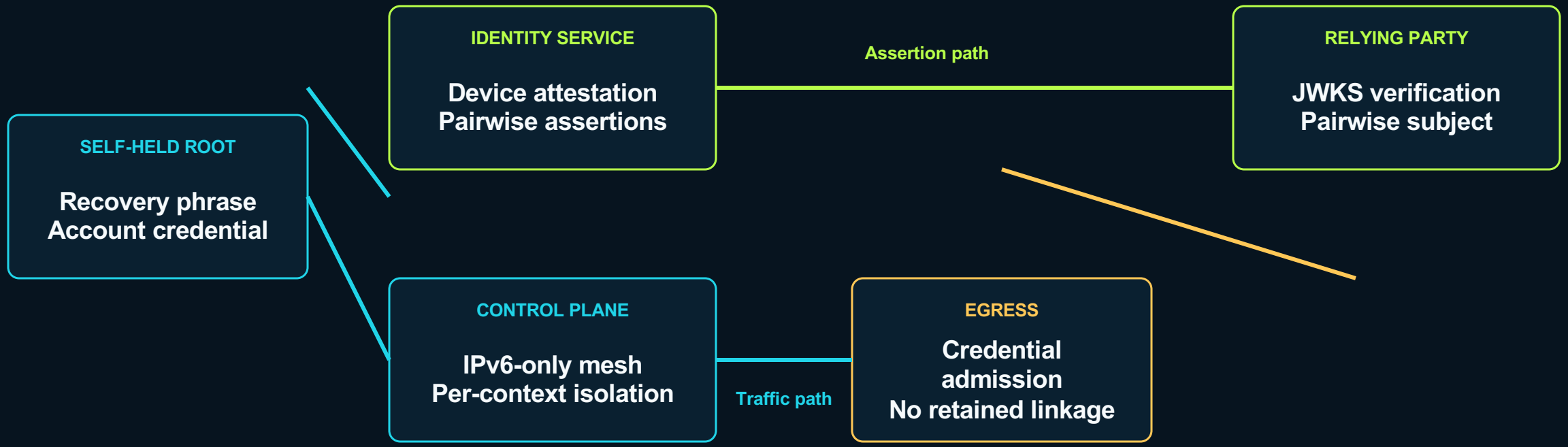
OPEN GATE

- **New macOS client end to end**
- Real-device recovery continuity
- Physical-device matrix
- Edge routed session proof

Investor reading: the core thesis has working evidence, while the product remains before launch

Current architecture separates identity from traffic delivery

The egress can authorize a device without holding the subscriber’s identity label



The ISP layer turns Presence intent into Internet delivery

Atlas treats addresses, routes and egress reputation as product inputs

1	**TRUSTED IP DELIVERY**	Authorize a device, assign a route, verify the observed egress and explain mismatches.
2	**IPv6 FOUNDATION**	Use IPv6-first coordination and dual-stack egress while treating IPv4 as scarce infrastructure.
3	**EGRESS CONTROL**	Regional, private and future residential-grade origins can carry different trust and reputation properties.
4	**POLICY + LENS**	Map destination policy to intended egress, compare actual state and surface a human-readable answer.
5	**OPERATIONS**	Health checks, safe failover, credential revocation and bounded observability protect service continuity.

Today: rented egress. This raise: owned prefix. ARIN allocation is not claimed.

Lens explains the gap between intention and reality

Policy becomes useful when the person can see what happened and why

INTENDED

Everyday	Toronto
Work	New York
Banking	Home origin

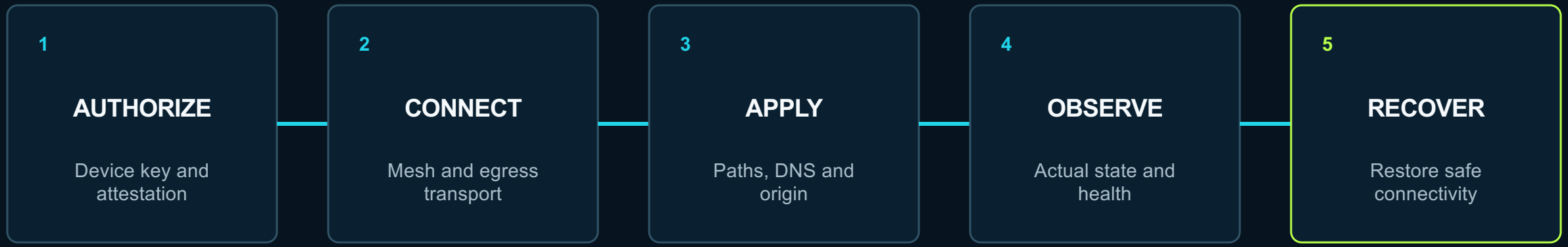
OBSERVED

Current egress	Toronto
Matched rule	Everyday
Status	Intended = actual

AI assistance remains bounded: detect drift, explain evidence, propose an action, require authorization

The client and agent make trust portable

One device contract hides platform-specific network machinery



Supported design targets

macOS first on the new stack

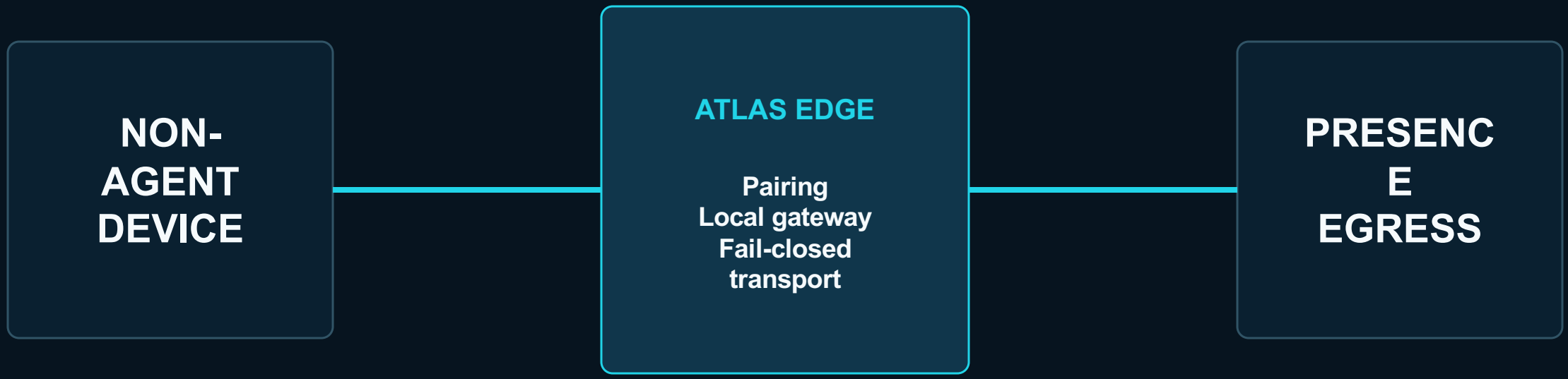
iPhone and Android follow the same contract

Windows in closed download-portal test

Current launch gate: the new macOS client has not completed end-to-end proof

Atlas Edge extends Presence to devices without an agent

A small connector can carry policy and egress for downstream hardware



Hardware evidence

Display and crash fixes verified

Open proof

Complete handshake and routed session

Next association model

Four words + device public key

Observability must diagnose without building a surveillance trail

Atlas is redesigning what each system can know, retain and join

KEEP

Health verdicts

Config versions

Credential status

MINIMIZE

Current endpoints

Short operational logs

Failure evidence

EXCLUDE

Browsing history

Identity at egress

Central raw capture

Known debt

Legacy logs and backup copies exposed more linkage than the target architecture allows

Roadmap principle: prove service health while making identity-to-traffic linkage unavailable by design

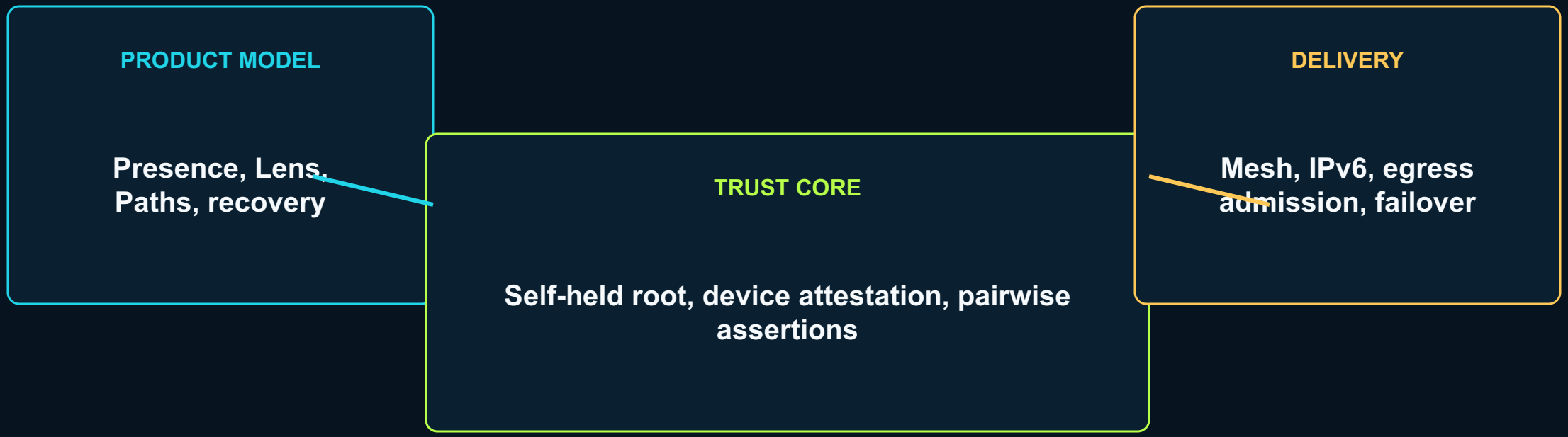
Atlas joins layers that the market sells separately

The differentiator is the continuity of person, policy and network presentation

CATEGORY	PRIMARY JOB	GAP ATLAS TARGETS
Consumer VPN	Encrypted egress and location	No durable identity or intended-vs-actual Presence model
Mesh networking	Private device connectivity	Network identity usually stops inside the mesh
Zero Trust / SWG	Enterprise access and inspection	Administrator-controlled posture, not person-controlled presentation
Identity / device trust	Authenticate user and device	Does not normally control public egress or destination routing
Atlas / Layer9i	**Person-controlled Internet Presence**	**Identity, egress, policy, recovery and explanation in one contract**

The moat is a trust architecture plus operational learning

Value compounds as each layer becomes independently verifiable and harder to correlate



Evidence loop

Failure capture | architecture correction | verified proof

No patent, partnership or exclusive network asset is claimed

Business model: recurring trust and delivery services

A staged hypothesis, not current revenue

INDIVIDUAL

Subscription

Presence, clients, core egress and Lens

First monetization hypothesis

PREMIUM ORIGIN

Add-on

Dedicated or higher-trust egress, advanced routing

Requires supply and reputation proof

TEAMS / DEVELOPERS

Per seat + usage

Relying-party verification, policy and reporting

Later expansion after consumer proof

Pricing, unit economics and willingness to pay remain unvalidated

Status: pre-revenue • no customer or revenue metrics claimed

Go-to-market starts with people who feel network identity break

The initial wedge rewards technical proof and high-intent feedback

1	**TRAVEL + REMOTE**	Need a stable, explainable Internet origin across networks
2	**PRIVACY-CONSCIOUS BUILDERS**	Want control without a provider joining identity to destinations
3	**SMALL TEAMS**	Need trusted devices and predictable egress without a full enterprise stack

Founder-led private beta → instrument reliability → validate willingness to pay

Roadmap: prefix first, then a paid Presence

No customer charge until Atlas-origin IPv6 is visible to a third party

NOW

First colo + transit + RPKI
Atlas IPv6 on the wire
macOS new-stack E2E

Product proof

NEXT

iPhone + Android parity
Edge routed-session proof
Service reliability baseline

Platform proof

THEN

Invited paid Presence
Blind-signature issuance
Independent relying parties

Commercial proof

SCALE

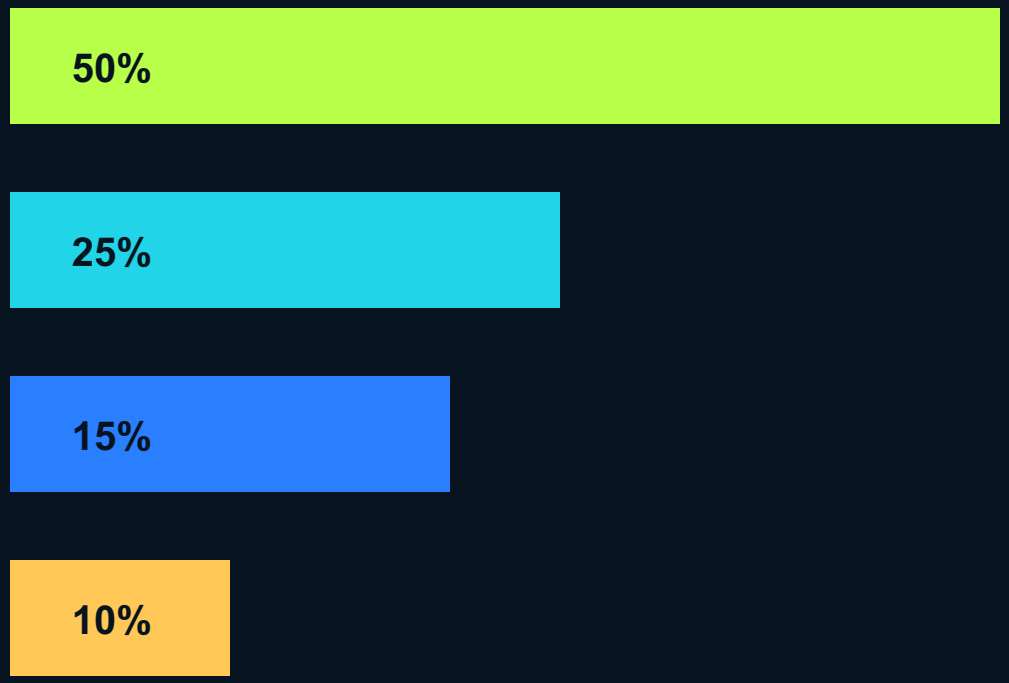
Windows and broader Edge
Multi-region capacity
Operational automation

Delivery scale

Launch criteria stay evidence-based: real devices, observed routing, measured recovery and explicit privacy boundaries

Use of funds: stand up the first Atlas prefix

SAFE $400k-$750k • $6M-$8M post-money cap • one POP, not a team



FIRST PREFIX

Colo, cross-connect, transit, Atlas v6, RPKI

CLIENT + PRODUCT

macOS E2E, mobile parity, Lens, recovery

SECURITY + TRUST

Review, key lifecycle, blind-sig design

MARKET VALIDATION

Invited testers, sandbox commerce, founder-led

Exact amount and cap are set in Stripe Atlas before any signed note

The ask: fund the first Atlas-origin IPv6 prefix

YC post-money SAFE via Stripe Atlas. No customer payment until a looking glass shows our v6.

CAPITAL

$400k-$750k • $6M-$8M cap • one cage, port, and v6 path

EXPERTISE

ISP ops, IP reputation, identity architecture — and a wire into Treasury

MILESTONE FOR THE ROUND

Third-party lookup shows Atlas IPv6. One person, one Presence, pairwise proof.

Terms on layer9i.com/atlas/one-pager/ • Stripe Atlas SAFE