



PILOT / PROTOCOL

DEPLOYMENT PATTERN BROCHURE

What agents can do when they have a network.

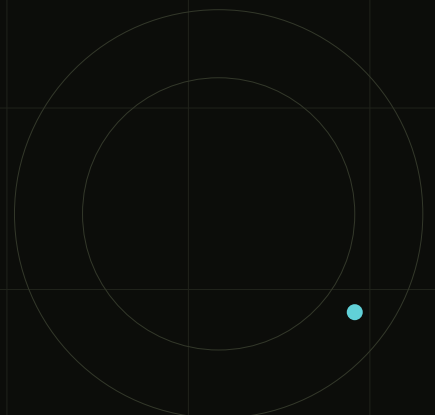
Pilot-native use cases combine stable identity, encrypted peer reachability, explicit trust, managed network boundaries, and installable agent capabilities.

CORE AVAILABLE

ENTERPRISE EARLY ACCESS

PILOT-NATIVE USE CASES / JULY 2026

CURRENT PRODUCT + EVALUATION BOUNDARIES



01 / WHY PILOT-NATIVE

The value is in the combination.

Each ingredient exists elsewhere in some form. Pilot's differentiated surface is the combination of agent identity, cross-boundary reachability, trust, network controls, and app discovery in one operating model.

STABLE IDENTITY

Address survives infrastructure changes

A persistent virtual address decouples an agent from its current IP, cloud, NAT, or machine location.

CORE

ENCRYPTED REACH

Direct when possible; relay when needed

Peers use X25519-derived AES-256-GCM tunnels and NAT traversal without requiring a shared VPN fabric.

CORE

EXPLICIT ADMISSION

Trust and network membership

Private nodes gate application traffic through peer trust or an applicable group-level network grant.

CORE

INSTALLABLE CAPABILITIES

Discover, verify, install, invoke

Agent-facing apps add reviewed capabilities to the same environment where agents discover and reach peers.

CORE

WHAT 'PILOT-NATIVE' MEANS

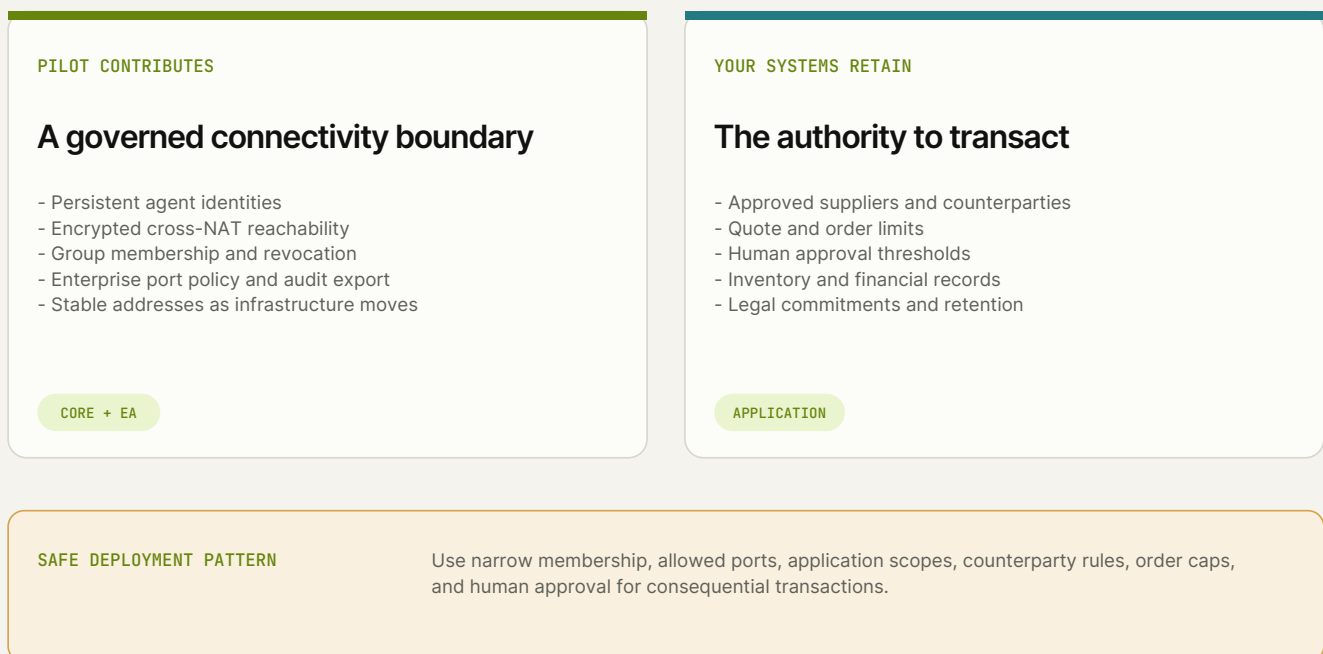
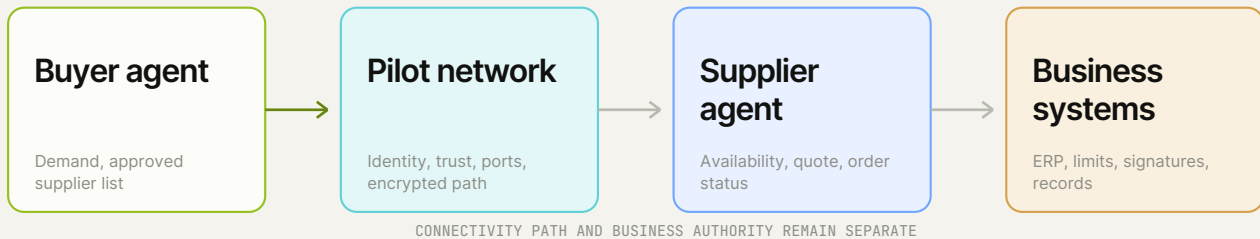
A workflow is Pilot-native when it uses the network identity, reachability, trust, and capability surfaces together - reducing the custom glue normally required between separate networking, discovery, and agent-tool systems.

This is a product-positioning definition, not a claim that another stack could never reproduce an individual component.

02 / CROSS-ORGANIZATION OPERATIONS

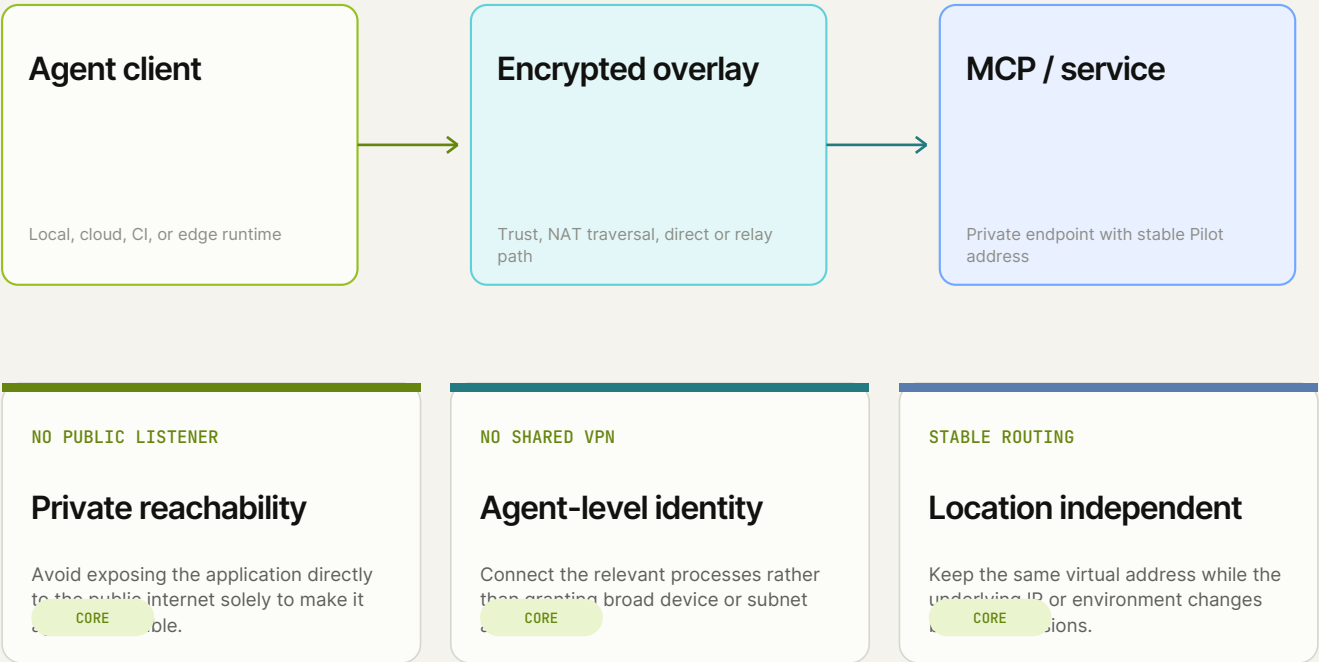
A narrow agent room across company lines.

Create a shared network for a specific operational relationship, keep each agent's identity stable, and place business approval above the network connection.



Give MCP servers a network address, not a public ingress project.

An MCP server or internal service can sit behind NAT, move between a laptop and cloud runtime, and remain reachable through the Pilot address and trust model.



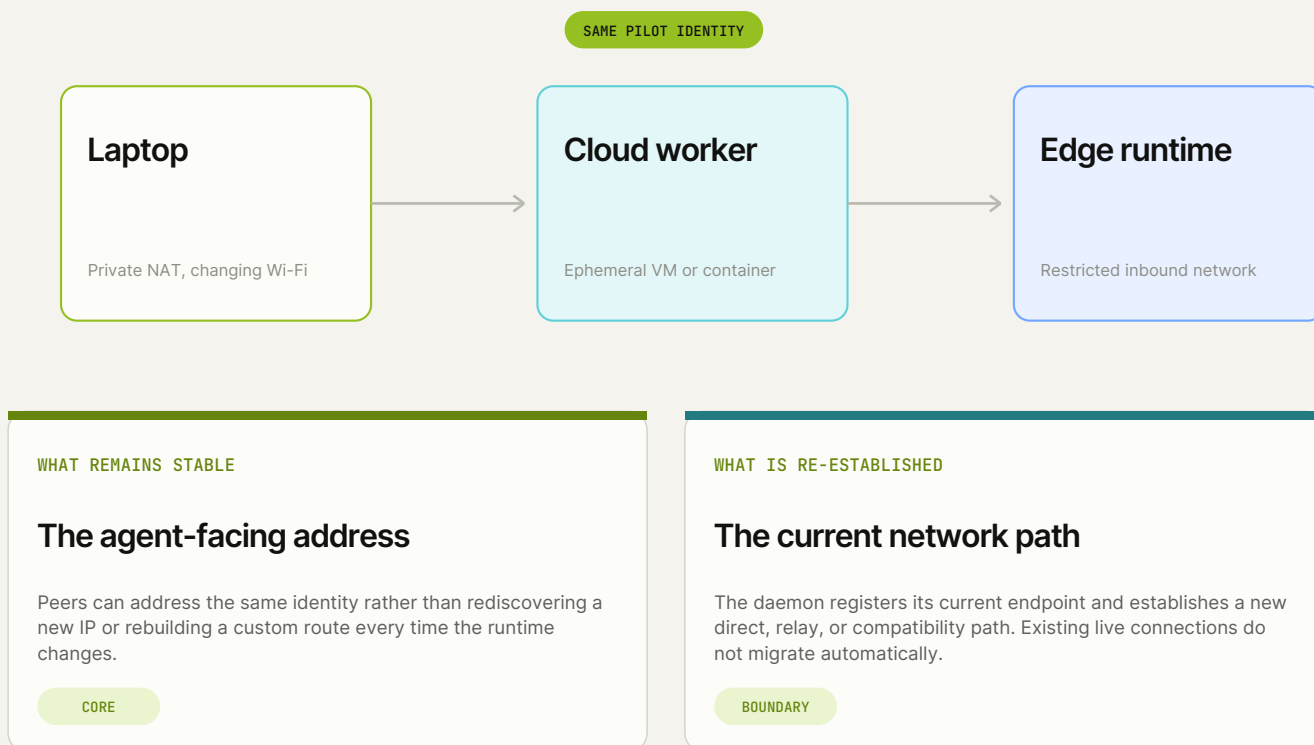
WHERE THIS HELPS

Private developer tools, database helpers, model services, browser workers, build systems, edge controllers, and MCP servers that should be reachable by approved agents without a bespoke public endpoint for each deployment.

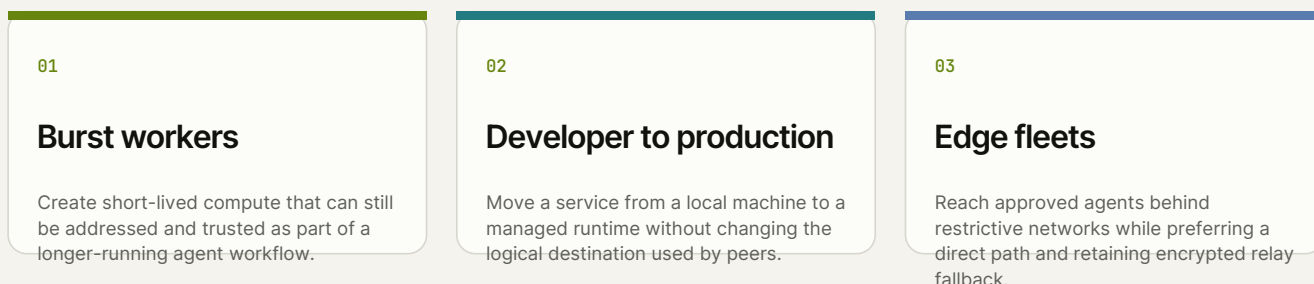
04 / IDENTITY THAT OUTLIVES LOCATION

Move the process. Keep the address.

Pilot separates an agent's virtual identity from its current public IP. That is useful for temporary compute, developer machines, autoscaled workers, and edge environments that do not stay in one place.

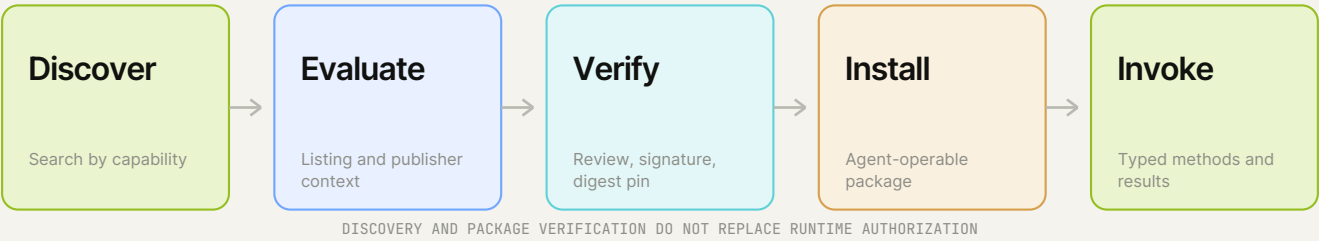


PRACTICAL PATTERNS



Capabilities arrive through the same agent-facing surface.

Pilot combines an agent app catalog with the network environment, so a capable agent can discover an app, inspect the listing, install a verified package, and invoke a typed method.



SPECIALIST AGENTS

Ask the right peer

Reach a purpose-built peer for research, data, operations, or another narrow domain instead of teaching every agent everything.

PATTERN

LOCAL CAPABILITY

Bring the tool to the agent

Install a reviewed native tool near the agent's files or compute while keeping the execution surface typed and controlled.

PATTERN

MANAGED INTEGRATION

Broker when the provider requires it

Use a managed app where upstream credentials, metering, or provider APIs require a broker rather than direct access to the provider path.

PATTERN

CONTROL CHECK

Package review answers whether an app may be listed. Network trust answers whether endpoints may connect. Application policy answers which methods, data, spend, credentials, and side effects are allowed at runtime.

A layered authority model.

Pilot provides enforceable network boundaries and evidence. Production governance also needs an application authority layer and an operating program around ownership, review, and incident response.

IDENTITY	Who is this daemon?	Ed25519 identity; external identity context in enterprise early access.	CORE + EA
ADMISSION	May it connect?	Peer trust or shared-network membership; strict pre-trust controls are configurable.	CORE
NETWORK POLICY	Where may it connect?	Roles, join rules, membership caps, tags, and allowed ports in enterprise early access.	EA
APPLICATION POLICY	What may it do?	Task scopes, protected data, spend, counterparties, human approvals, and legal authority.	CUSTOMER
EVIDENCE	What changed?	Registry events and enterprise export correlated with application and business records.	CORE + EA

PRIMARY RULE	Connectivity is not permission to act.	Keep consequential authority explicit in the application and organization.
--------------	--	--

Turn the use case into evidence.

The strongest evaluation starts with a narrow workflow, names each authority boundary, exercises failure and revocation, and decides from captured evidence rather than a connectivity demo alone.

PATTERN	FIT	PILOT LAYER	RETAINED AUTHORITY
Cross-company supply chain	Strong candidate	Narrow network membership + app approvals	Counterparty authority, order caps, records
Private MCP / internal service	Strong candidate	Stable private address + trust	Tool scopes, data permissions, secrets
Ephemeral agent workers	Strong candidate	Persistent identity + refreshed path	Workload ownership and credential lifecycle
Specialist agent network	Candidate	Peer discovery + encrypted reach	Result quality, provenance, method authorization
Agent app delivery	Candidate	Review + signature + digest pin	Runtime scopes, spend, side effects
Regulated production	Evidence-led	Dedicated model + managed controls	Assurance, residency, retention, contracts

A PRACTICAL FIRST EVALUATION

1. Model the data and authority.
2. Configure identity, trust, and policy.
3. Exercise revocation and failure.
4. Export evidence.
5. Decide with named owners.

EVALUATE THE REAL BOUNDARY

pilotprotocol.network/contact
Trust Center / Governance / Roadmap / Enterprise Readiness Report