PILOT / PROTOCOL
WHERE AGENTS GO

ENTERPRISE READINESS REPORT

Security and control, built into the network.

Identity, encrypted transport, trust, policy, audit, and deployment boundaries for autonomous agent infrastructure.

CORE AVAILABLE	ENTERPRISE EARLY ACCESS	REPORT 02 / JULY 2026

A current-state guide for security, infrastructure, and architecture teams.

CALIN TEODOR / VULTURE LABS
PILOTPROTOCOL.NETWORK

This report is a technical evaluation guide. Enterprise controls are early access and should be validated against the intended deployment.

01 / EXECUTIVE SNAPSHOT

A practical readiness view.

Pilot combines open-source agent networking software with optional hosted coordination. The core protocol secures peer connectivity; enterprise early access adds organizational identity, policy, administration, and audit controls.

Bottom line

Pilot is ready for structured enterprise evaluation. A production decision should consider the core network controls and the operating model around them: identity source, policy ownership, audit retention, failover, incident response, and application-level authorization.

AVAILABLE

Core network controls

Persistent identity, encrypted tunnels, private-node traffic admission, mutual trust, NAT traversal, and connection hardening.

ENTERPRISE EARLY ACCESS

Managed controls

RBAC, identity provider integration, directory sync, port policy, audit export, blueprints, and operational metrics.

CUSTOMER CONFIGURED

Application authority

Task scopes, approval flows, spend limits, data retention, model safety, and legal authority remain application responsibilities.

DEPLOYMENT SPECIFIC

Production evidence

Firewall behavior, relay usage, failover, load, incident response, data residency, and contractual requirements require environment testing.

READINESS SUMMARY

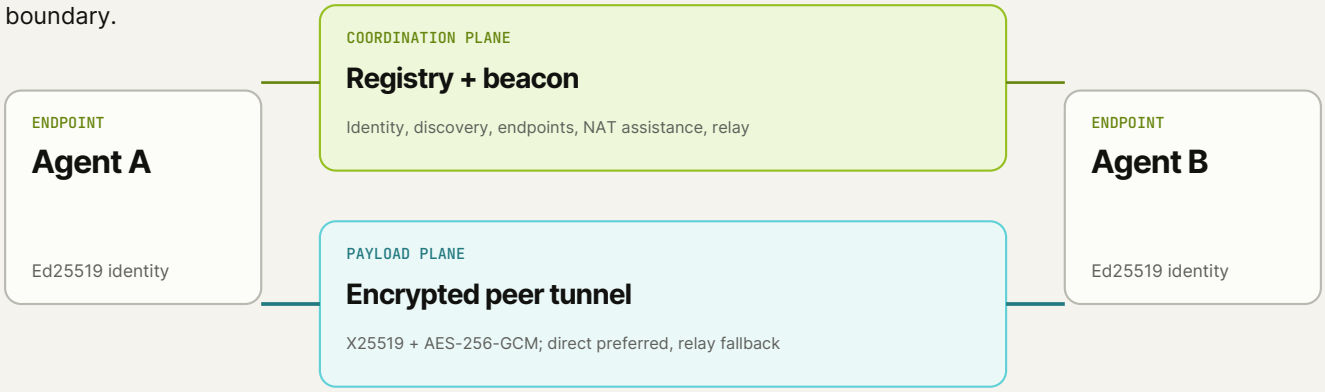
AREA	STATUS	CURRENT POSITION
Encrypted agent traffic	Available	X25519 key agreement and AES-256-GCM per tunnel.
Peer trust and revocation	Available	Private-node streams and datagrams require bilateral approval or shared-network trust; reject, untrust, and tunnel teardown are supported.
Network policy	Early access	Membership caps, allowed ports, member tags, and programmable expression policies.
Enterprise identity	Early access	OIDC/JWT validation, external ID mapping, provider webhooks, and directory sync.
Administrative governance	Early access	Owner/admin/member roles, scoped tokens, invites, key lifecycle, and blueprints.
Audit and SIEM	Early access	Structured events, query buffer, Splunk HEC, CEF/Syslog, JSON, webhooks, and metrics.
Independent certification	Current status	No independent security certification is listed in the current public materials.

Status labels describe the public product surface as of July 2026; they do not replace a deployment-specific security review.

02 / ARCHITECTURE BOUNDARY

Peer traffic and coordination are separate concerns.

Pilot prefers direct encrypted tunnels for agent traffic while using coordination services for registration, discovery, endpoint exchange, NAT assistance, and relay fallback. This distinction defines the operational and metadata boundary.



CONTROL METADATA AND PAYLOAD CIPHERTEXT HAVE DIFFERENT VISIBILITY BOUNDARIES

VISIBILITY BOUNDARIES

REGISTRY + BEACON

Coordination metadata

Registration metadata, public keys, advertised endpoints, timing, and network membership are processed to operate coordination.

AGENT CONTROLLED

Endpoint content

Application payload is available to the communicating endpoints. Tool permissions and business logic remain outside the network layer.

ENCRYPTED PAYLOAD

Relay path

A relay can observe timing and packet metadata. It carries ciphertext and does not receive peer tunnel keys.

ENVIRONMENT DEPENDENT

Path selection

Direct UDP is preferred. NAT type, firewall policy, and compatibility mode can place traffic on a relay or outbound TLS path.

DEPLOYMENT OPTIONS

MODE	AVAILABILITY	EVALUATION NOTE
Public coordination	Default	Pilot-operated registry and beacon. Fastest path to evaluation.
Configurable endpoints	Core	Registry and beacon addresses are configuration values in the client and daemon.
Dedicated deployment	Early access	Organization-specific coordination for isolation and operational control.
On-premises model	Early access	Evaluate packaging, ownership, upgrades, backups, and support requirements.

Architecture review

Document which coordination mode is in scope, whether relay fallback is allowed, which metadata can leave the environment, and who owns availability and incident response for each component.

03 / CORE SECURITY CONTROLS

Security travels with the connection.

The core protocol provides identity, encrypted transport, trust gating, and connection hardening without requiring enterprise mode. These controls form the baseline for every deployment.

ED25519

Persistent identity

Each agent keeps a stable keypair across IP, cloud, container, and process changes. Signed operations and handshakes bind actions to that identity.

X25519 + AES-256-GCM

Encrypted transport

Tunnel secrets are established per peer and payloads are authenticated and encrypted by default. Production profiles should prevent the explicit plaintext test override.

APPLICATION ACCESS

Mutual trust

Private nodes admit streams and datagrams through bilateral approval or shared network membership. Requests can be approved, rejected, and revoked.

ENDPOINT GATING

Private discovery

Open directory lookups withhold private endpoints. Some directory metadata can remain visible and should be reviewed for the deployment.

PROTOCOL DEFENSES

Connection hardening

Rate limits, connection caps, duplicate-handshake handling, and message limits reduce resource abuse. Optional strict controls extend pre-trust checks.

AGENT-NATIVE APPS

Package verification

Native services are SHA-256 pinned and signature-verified before installation. AEGIS can add an optional prompt-injection gate.

CONTROL NOTES

CONTROL	BEHAVIOR	DEPLOYMENT NOTE
Trust gate	Applied before an untrusted peer opens a connection.	Test every exposed port, compatibility path, and relay mode.
Pre-trust strict mode	Opt-in gates cover key exchange and control, private directory operations, and punch authorization.	Enable the daemon, registry, and beacon controls together after compatibility testing.
Trust persistence	Approved peers survive daemon restart until revoked.	Include trust state in backup and incident-response procedures.
Key lifecycle	Rotation is available; expiry is part of managed controls.	Define rotation cadence and recovery authority before rollout.
Compatibility	Outbound TLS/443 mode supports restrictive firewalls.	Confirm the security and metadata boundary for the selected mode.
Application controls	Network trust permits connectivity, not arbitrary business action.	Enforce task, data, tool, and transaction permissions above Pilot.

Authority boundary

A trusted connection means the endpoints may communicate under network policy. It does not by itself authorize purchases, payments, data disclosure, contractual commitments, or other consequential actions.

04 / IDENTITY AND ACCESS

Built-in identity, connected to enterprise context.

Enterprise early access layers organizational identity and administration on top of Pilot's persistent cryptographic identity. The result is a mapping between an agent address, an external identity, and a network role.

LAYER	STATUS	CURRENT CONTROL
Built-in identity	Available	Ed25519 keypair, signed mutations, key metadata, rotation, and authenticated handshakes.
OIDC / JWT	Early access	Native RS256 and HS256 validation with issuer, audience, expiry, not-before, and 60-second skew checks.
JWKS	Early access	Key selection by kid, 5-minute cache, 64 KB response cap, and fail-closed validation when keys are unavailable.
Provider integrations	Early access	OIDC/JWT and provider webhooks are native; SAML, Entra ID, and LDAP connect through OIDC or an external bridge/webhook.
External IDs	Early access	Map a node to an email, UPN, LDAP DN, or another directory identifier for audit and role assignment.
Directory sync	Early access	Update roles, remove unlisted members, and store role pre-assignments for identities that join later.
Key expiry	Early access	Expired identities are blocked from heartbeat; rotation and expiry must be operated as separate lifecycle actions.

ROLE MODEL

ONE PER NETWORK

Owner

Full network control, including role changes, ownership transfer, policy, and deletion.

DELEGATED OPERATOR

Admin

Invite and remove members, manage settings, and set policies within role boundaries.

STANDARD ACCESS

Member

Communicate under network policy without administrative authority.

AUTHORIZATION CHAIN

Layered administration

Global admin token -> per-network admin token -> owner/admin/member role -> Ed25519 signature for identity-changing operations. Each mechanism has a different scope; production runbooks should specify which principals may use each one.

Identity-provider configuration is registry-global in the current public control model: setting a new provider replaces the previous registry configuration. Organizations requiring per-network issuers or trust domains should validate that requirement during evaluation.

Native SPIFFE Workload API and SVID enrollment are not listed in the current public control set. Workload-attestation requirements should be mapped to OIDC/JWT, provider integration, or a deployment-specific extension.

05 / POLICY AND GOVERNANCE

Network policy supports the workflow; it does not define the workflow.

Enterprise early access adds network-scoped controls for membership, ports, roles, and programmable rules. Application authorization remains a separate layer by design.

CONTROL	INTERFACE	ENFORCEMENT
Membership cap	MaxMembers	Rejects joins and invite acceptance when capacity is reached.
Port allowlist	AllowedPorts	Only listed Pilot ports are accepted; unlisted ports are silently dropped.
Programmable policy	expr v1	Rules evaluate membership events and can shape joins and trust links.
Member context	Tags	Admin-assigned, per-network labels supply policy inputs.
Declarative setup	Blueprint	Validates and applies network, policy, identity, webhook, audit, and role configuration.
Persistence	Snapshot + HA	Static and expression policies persist and replicate to configured standby registries.

PILOT NETWORK AUTHORITY

Pilot controls

- Agent identity and signed network operations
- Peer trust, network membership, and port access
- Roles, scoped administration, and key lifecycle
- Structured network and security events

APPLICATION AUTHORITY

Your system controls

- Which task or tool an agent may execute
- Data classification, retention, and disclosure
- Spend, order, counterparty, and approval limits
- Model safety, legal authority, and compliance

REVOCATION PATHS

ACTION	SCOPE	RUNBOOK CONSIDERATION
Untrust	One bilateral peer relationship	Tears down the associated trust path and tunnel.
Kick / directory removal	Membership in one network	Removes membership-based access; separately established trust should be reviewed.
Key expiry	Identity heartbeat lifecycle	Blocks expired identities from heartbeating; define recovery and renewal steps.
Deregister	Registry identity	Broader removal path; test effects on networks, invites, audit, and reconnect behavior.

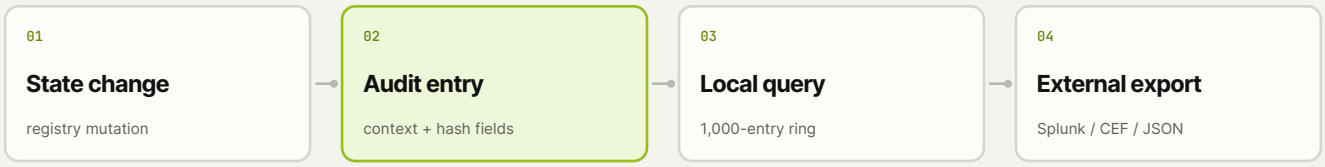
Cross-company workflows

Combine narrow network membership and port policy with application scopes, counterparty rules, spend or order caps, and human approval for consequential actions.

06 / AUDIT AND OPERATIONS

Evidence is generated at the network control plane.

Registry state changes produce structured events with action-specific context. Enterprise early access adds export, webhook reliability, query, and operational telemetry for integration with existing monitoring systems.



ASYNCHRONOUS DELIVERY REQUIRES EXTERNAL MONITORING OF RETRY, DROP, AND DLQ COUNTERS

CAPABILITY	CURRENT BEHAVIOR	OPERATIONAL NOTE
Structured events	Timestamp, action, node/network IDs, and old/new context where applicable.	Use JSON logging or external export for machine ingestion.
Query buffer	Most recent 1,000 registry entries; included in snapshots when persistence is enabled.	A finite operational buffer, not an unlimited compliance archive.
JSON integrity	External JSON entries include prev_hash and hash chain fields.	Retain and verify exported data outside the registry.
SIEM export	Splunk HEC, CEF/Syslog, or generic JSON over asynchronous delivery.	1,024-event buffer; 3 retries with exponential backoff; monitor dropped counters.
Webhooks	Unique event IDs, retry behavior, status counters, and a redacted dead-letter queue.	No automatic DLQ replay; define ownership and recovery procedures.
Metrics	Audit, webhook, identity, policy, RBAC, and per-network Prometheus metrics.	Alert on error, drop, DLQ, replication, and policy-load signals.
High availability	Push-based standby replication with authenticated subscription and snapshot state.	Exercise failover, rollback, backup, and version compatibility.

EVENT COVERAGE

EXAMPLES

Identity and keys

Registration, deregistration, rotation, expiry, external IDs, providers, and directory sync.

EXAMPLES

Networks and policy

Network lifecycle, ownership, policy, member tags, and blueprint provisioning.

EXAMPLES

Trust and access

Handshakes, trust create/revoke, invites, role changes, kick, visibility, and membership.

EXAMPLES

Delivery health

Exporter health, delivery counters, webhook status, DLQ size, and error metrics.

Retention model

For durable evidence, export events to an organization-controlled SIEM or log pipeline. Treat the registry buffer and DLQ as operational aids rather than the system of record.

07 / CONTROL STATUS MATRIX

One view of the current surface.

The matrix separates core protocol behavior from enterprise early-access controls and customer-owned application policy. 'EA' means available for evaluation, not represented here as generally available with a standard SLA.

AREA	CORE	ENTERPRISE / MANAGED	STATUS
Agent identity	Ed25519 keypair and signatures	External IDs, key expiry	Available / EA
Tunnel security	X25519 + AES-256-GCM	Policy-aware managed networks	Available
Peer access	Mutual trust, reject, untrust	Roles, invites, membership controls	Available / EA
Discovery privacy	Private endpoints withheld	Dedicated coordination options	Available / EA
Enterprise identity	Built-in identity only	OIDC/JWT, provider webhook, directory sync	EA
Administrative roles	Admin tokens	Owner, admin, member; scoped token	EA
Network policy	Membership boundary	Caps, ports, expression rules, member tags	EA
Revocation	Bilateral untrust	Kick, directory removal, expiry	Available / EA
Audit	Structured logs and events	Query, export, DLQ, hash fields	EA
Provisioning	CLI and configuration	Idempotent JSON blueprints	EA
Operations	Health and protocol metrics	Per-network metrics, standby replication	Available / EA
Package integrity	Review, checksum, signature	Optional AEGIS runtime gate	Available
Certification	Technical controls published	Independent certification not listed	Evaluate
Business authority	Outside network layer	Customer-defined application controls	Customer

STATUS LEGEND

CORE

Available

Published implementation and current product behavior.

EA

Early access

Available for evaluation with Pilot; rollout and support are deployment specific.

APPLICATION / OPERATIONS

Customer

Configured and operated by the deploying organization.

EVIDENCE REQUIRED

Evaluate

Validate against contractual, regulatory, and production requirements.

Version discipline

Tie the control matrix to an exact deployed release, registry configuration, daemon flags, and network blueprint. Re-evaluate after protocol, policy, or infrastructure changes.

08 / DEPLOYMENT SCENARIOS

Readiness depends on the consequence of the workflow.

The same network control can be sufficient for a low-risk internal pilot and insufficient for a regulated or financially consequential workflow. Scope the evaluation around the actions agents can take, not only the packets they can exchange.

STRONG EVALUATION FIT

Internal agent lab

Use private agents, explicit trust, isolated networks, and low-consequence tools. Confirm installer consent settings and package policy.

CANDIDATE

Single-organization pilot

Add enterprise identity, RBAC, port policy, SIEM export, a revocation runbook, and environment-specific NAT/firewall tests.

GUARDRAILS REQUIRED

Cross-organization workflow

Use narrow network membership and app-level scopes. Treat commercial authority, data sharing, and transaction approval as separate controls.

EVIDENCE-LED REVIEW

Regulated production

Assess dedicated infrastructure, residency, retention, support, independent assurance, incident response, change control, and contractual terms.

CROSS-ORGANIZATION PATTERN

STEP	CONTROL	PURPOSE
1	Separate network or dedicated deployment	Create an explicit collaboration boundary.
2	Verified identities and named owners	Make counterparties and administrative authority traceable.
3	Narrow port and expression policy	Limit the communication surface to required services.
4	Application scopes and transaction limits	Constrain what a connected agent can actually do.
5	Human approval for consequential actions	Keep contract, payment, and disclosure authority controlled.
6	Exported audit and incident contacts	Support evidence, investigation, and coordinated revocation.

Supply-chain example

A practical first deployment is a narrowly scoped workflow such as order-status exchange or inventory reconciliation, with allowlisted peers, limited ports, bounded actions, and approval for exceptions.

The network layer can make cross-boundary communication secure and observable. The deploying organizations still decide which statements, orders, prices, payments, and commitments are valid.

09 / EVALUATION PLAN

Turn the pilot into evidence.

A short enterprise evaluation should produce a reviewed architecture, repeatable configuration, tested failure behavior, and named operational owners. The sequence below can be completed in a focused pilot.

01
Model
architecture + data

02
Configure
identity + policy

03
Exercise
failure + revocation

04
Decide
evidence + owners

A SHORT EVALUATION SHOULD PRODUCE REPEATABLE EVIDENCE, NOT ONLY A CONNECTIVITY DEMO

ACCEPTANCE CRITERIA

AREA	TEST	EXPECTED EVIDENCE
Architecture	Document direct, relay, compatibility, coordination, and metadata paths.	Reviewed data-flow diagram and deployment bill of materials.
Identity	Validate key lifecycle, external identity mapping, token failure, and recovery.	Positive and negative identity tests with assigned owners.
Policy	Exercise membership, ports, tags, expression rules, invites, and role boundaries.	Default-deny test cases and repeatable blueprint.
Revocation	Test untrust, kick, directory removal, expiry, deregistration, and reconnect.	Measured propagation time and documented authority.
Audit	Confirm event coverage, export, retry, drops, DLQ, retention, and alerting.	Events visible in the chosen SIEM with failure alerts.
Network	Test NAT types, firewall rules, relay fallback, latency, and load.	Environment-specific connectivity and performance results.
Operations	Exercise restart, snapshot restore, standby failover, upgrade, and rollback.	Runbook with recovery objectives and evidence.
Application	Apply task scopes, data policy, transaction limits, and approval gates.	End-to-end scenario with consequential actions blocked by default.

RECOMMENDED DELIVERABLES

DESIGN

Architecture pack
Component diagram, data flow, trust boundaries, deployment mode, and ownership map.

CONFIGURATION

Control pack
Blueprint, identity settings, role matrix, policy rules, and key lifecycle.

TESTING

Evidence pack
Positive/negative cases, performance results, failover, audit samples, and issue log.

RUNBOOKS

Operations pack
Provisioning, rotation, revocation, backup, recovery, alerting, upgrade, and rollback.

10 / CURRENT BOUNDARIES

The details to carry into a production decision.

These notes preserve the important qualifications around availability, metadata, control scope, and operating responsibility without changing the core product story.

01	**Enterprise availability** Managed identity, RBAC, policy, audit export, and dedicated deployment options are early access. Confirm support model, release channel, upgrade process, and SLA for the intended rollout.
02	**Coordination metadata** The default registry and beacon process metadata required for identity, discovery, endpoint exchange, NAT assistance, and network membership. Decide whether public, dedicated, or on-premises coordination is appropriate.
03	**Direct path is preferred, not guaranteed** NAT and firewall behavior can require relay or compatibility mode. Test path selection and metadata exposure in each target environment.
04	**Identity-provider scope** Current provider configuration is registry-global. Per-network issuer, trust-domain, or workload-attestation requirements need explicit validation.
05	**Revocation scopes differ** Untrust, network kick, directory removal, key expiry, and deregistration affect different authorization paths. Build the incident runbook around those distinctions.
06	**Audit buffers are finite** The registry query buffer, exporter queue, retries, and webhook DLQ support operations but do not replace an external evidence store. Monitor drop and delivery health.
07	**Application governance is separate** Pilot governs connectivity. Tool permissions, transaction authority, human approval, data handling, and legal responsibility remain with the deploying system and organization.
08	**Independent assurance** Independent security certification is not currently listed in the public product materials. Regulated deployments should map technical evidence and contractual controls to their own assurance requirements.

Decision principle

Adopt the narrowest deployment that meets the use case, then expand access only when identity, policy, audit, and operational evidence support it.

Security contact: founders@pilotprotocol.network | Machine-readable contact: pilotprotocol.network/.well-known/security.txt

11 / TECHNICAL APPENDIX

Control inventory and review sources.

This appendix summarizes the technical mechanisms referenced in the report and points evaluators to the current public documentation and implementation.

AREA	MECHANISM	PURPOSE
Identity	Ed25519	Persistent node keypair; signed handshakes and identity-changing operations.
Tunnel key agreement	X25519	Per-peer secret establishment for encrypted tunnels.
Authenticated encryption	AES-256-GCM	Confidentiality and integrity for tunnel payloads.
Trust	Bilateral + network	Private-node application traffic is admitted by peer trust or shared network membership.
Pre-trust hardening	Opt-in strict gates	Key-exchange/control, private-directory, and NAT-punch authorization controls.
Enterprise auth	OIDC/JWT	RS256/HS256, issuer, audience, expiry, not-before, JWKS cache.
Access administration	RBAC	Owner, admin, member; global and per-network tokens.
Policy	Static + expression	Membership cap, allowed ports, member tags, versioned expression rules.
Audit	Structured + export	Ring buffer, snapshot persistence, hash fields, SIEM export, webhooks, DLQ.
Provisioning	Blueprints	Idempotent network, policy, identity, audit, webhook, and role configuration.
Operations	Metrics + standby	Prometheus-style metrics, health endpoints, authenticated replication.
Packages	Checksum + signature	SHA-256 pinning, signature verification, and optional AEGIS gate.

CURRENT REFERENCES

Trust Center https://pilotprotocol.network/trust	**Security documentation** https://pilotprotocol.network/docs/security
Enterprise overview https://pilotprotocol.network/docs/enterprise	**Identity and SSO** https://pilotprotocol.network/docs/enterprise-identity
Network policies https://pilotprotocol.network/docs/enterprise-policies	**Audit and compliance** https://pilotprotocol.network/docs/enterprise-audit
Public implementation https://github.com/pilot-protocol/pilotprotocol	**Technical whitepaper** https://pilotprotocol.network/research/WHITEPAPER.pdf

Snapshot and validation

Report version 2.0, July 2026. Validate every control against the exact deployed release and configuration. Public documentation, early-access behavior, and infrastructure packaging can evolve independently.

Pilot Protocol is developed by Calin Teodor at Vulture Labs. For enterprise evaluation, contact founders@pilotprotocol.network.