



BLACK SWAN NET

Direct secure communications

Synchronized peer sessions. Endpoint-bound identity. Maintained assurance.

Secure communications without a provider in the middle.

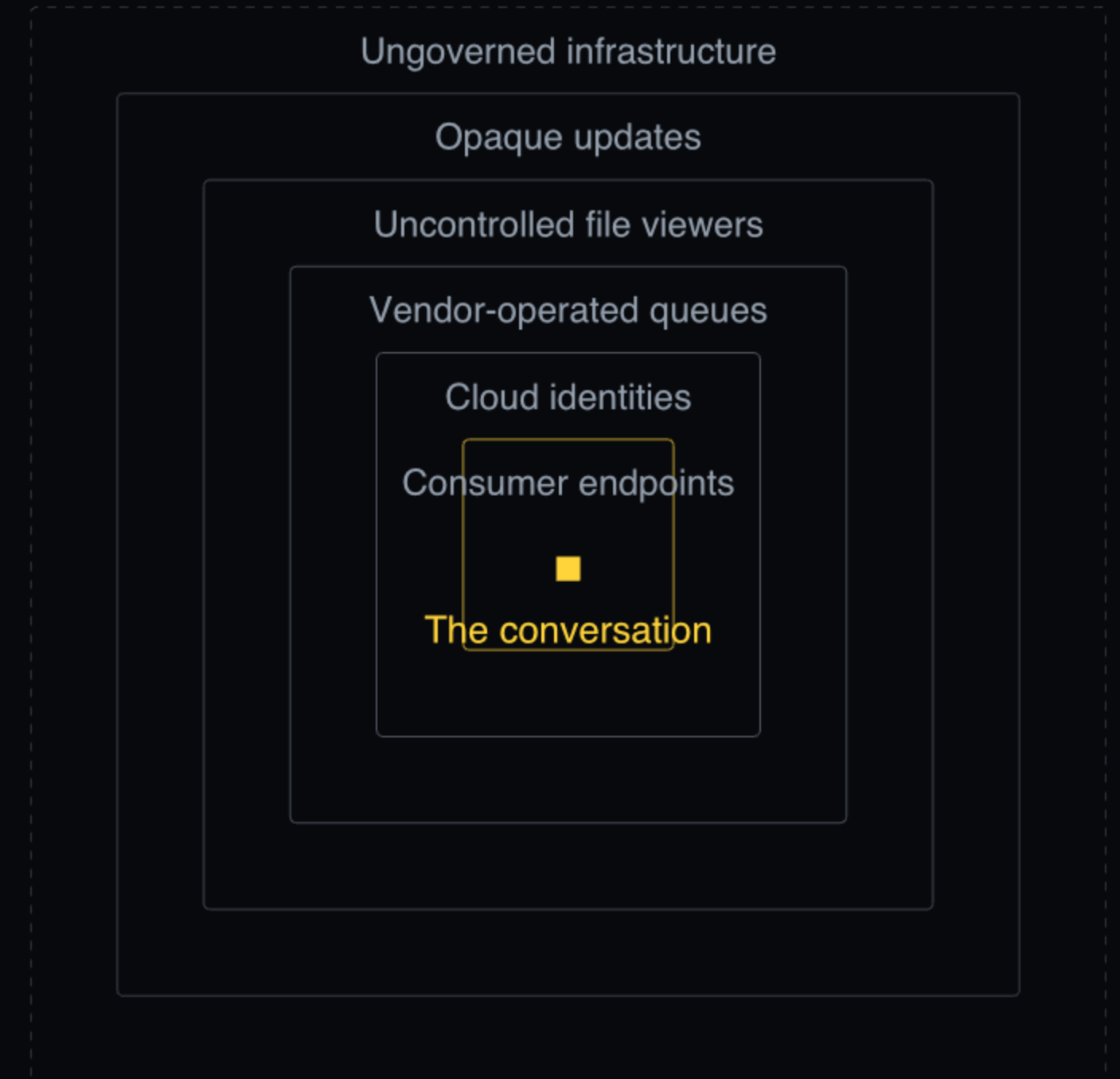
ACTIVE PRODUCT DEVELOPMENT • PATENT PENDING

THE PROBLEM

Encryption is no longer the whole problem

High-value conversations still depend on consumer endpoints, cloud identities, vendor queues, uncontrolled viewers, opaque updates, and infrastructure the customer does not govern.

The content may be encrypted.
The trust model is still outsourced.



One controlled core. Four commercial products.

- | | | |
|----|-----------------------------|---|
| 01 | Black Swan Direct | Stock Pixel track with a minimal full-Linux userspace and synchronized direct sessions. |
| 02 | Sovereign + Gateway | RED/GREEN isolation for hostile networks; Gateway extends the policy boundary. |
| 03 | Black Swan Assurance | Provisioning, releases, evidence, depot recovery, capture response, logistics, and support. |

Standardized core. Customer variation through policy—not source forks.

Trust starts in the room

ENDPOINT A
K7F2 · 9QX1

basalt · meridian · flare

Both operators compare the same phrase and device labels. The human check is deliberate.

ENDPOINT B
K7F2 · 9QX1

- 1

Pair devices in a controlled room.
- 2

Exchange endpoint-bound identities locally.
- 3

Compare the same phrase and device labels.
- 4

Pin the relationship. Identity changes require explicit re-pairing.

Phone numbers, SIMs, email accounts, vendor accounts, and radio association never establish cryptographic trust.

Full Linux narrows the attack surface



DEDICATED
APPLIANCE

OUTSIDE THE BOUNDARY

Browser

Email

App store

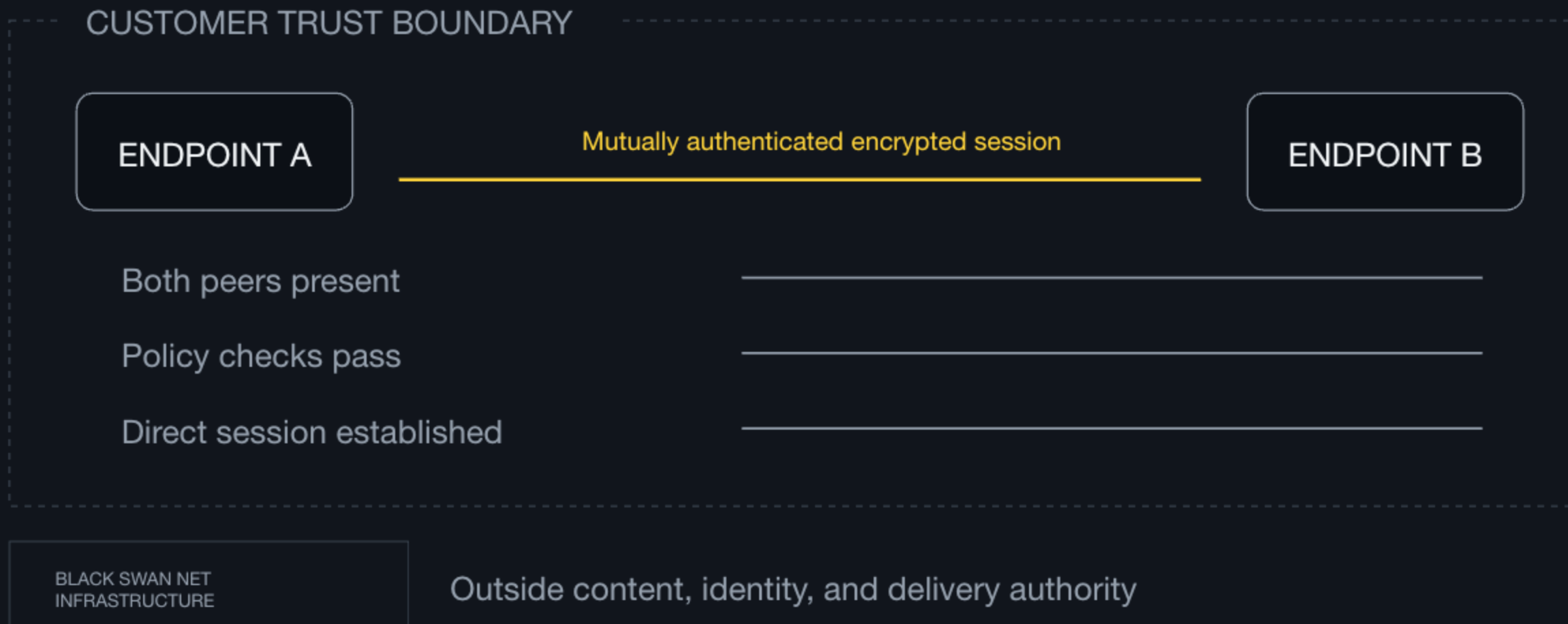
Android runtime

- Unmodified Pixel 10a reference hardware
- Minimal, immutable, controlled full-Linux userspace
- Verified boot and rollback-protection direction
- No ordinary browser, email, app store, consumer backup, or Android runtime
- Policy-controlled radios, sensors, export, and administrative actions
- Signed releases, controlled provisioning, revocation, and depot recovery

The selected production endpoint is full Linux—not Android or GrapheneOS.

Implementation evidence, device validation, and independent escape testing remain required.

Direct means direct



The architecture excludes

No message server, mailbox, or queue

No cloud store or asynchronous path

No vendor directory or discovery

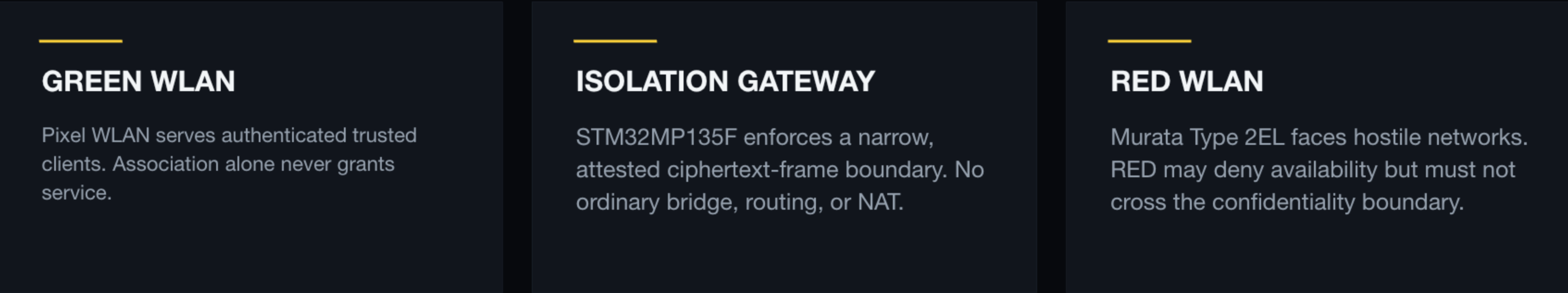
No relay, push, or vendor key custody

No administrative decryption authority

If the peer is absent, no message is transmitted or deposited with Black Swan infrastructure.

This boundary reduces selected dependencies; it does not eliminate metadata or denial-of-service risk.

Separate trusted clients from hostile networks



BOUNDARY RULES

Unknown GREEN clients receive no useful service	External USB is eliminated in the fielded design	RED and GREEN are not bridged, routed, or NATed	Only narrow attested ciphertext frames cross	RED compromise may deny availability—not confidentiality
---	--	---	--	--

Radio association is connectivity—not identity, trust, or session authority.

HONEST DELIVERY STATE

If the peer is absent, nothing is delivered



NO ASYNCHRONOUS MODE

No operational Black Swan mailbox, queue, store-and-forward service, or relay accepts content.

AVAILABILITY IS EXPLICIT

Blocking, jamming, and peer unavailability can prevent communication. Black Swan Net does not guarantee delivery.

Operators see the true state: local, connected, decrypted, or read.

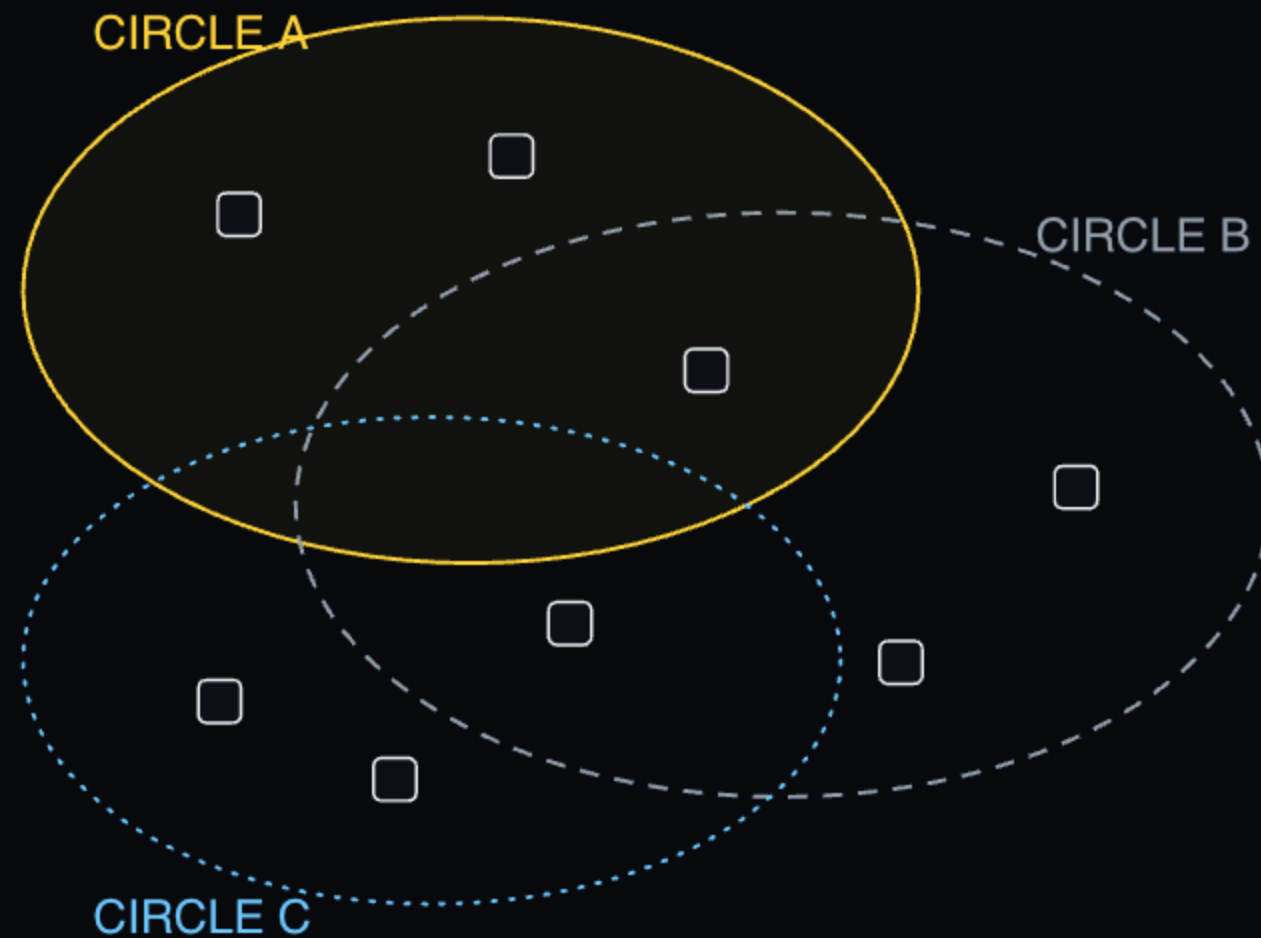
Attachments use a controlled security path

- | | | | | | |
|----|---|----|--|----|--|
| 01 | Encrypt each object and bind it to a signed manifest. | 02 | Inspect actual content rather than trusting the filename. | 03 | Strip, preserve, or separately protect metadata according to policy. |
| 04 | Block active content, scripts, macros, embedded executables, and unsupported formats. | 05 | Decode, reconstruct, or render approved content in a constrained viewer. | 06 | Require explicit policy authorization for export. |

Encryption protects delivery. Controlled rendering helps protect the endpoint after arrival.

Release requires validation, sandboxing, and fuzz testing.

Replace the endpoint. Preserve the fleet.



Each authorized endpoint has its own identity, policy, and membership.

Opening a fielded device triggers permanent identity revocation.

Affected membership and key epochs advance after authenticated convergence.

Replacement creates a new identity—never a restored clone.

Hostile custody triggers quarantine and destruction review.

Compromise response contains the affected identity while preserving unaffected peers and governed fleet continuity.

Security evidence travels with the capability

- | | | | |
|----|--|----|--|
| 01 | System architecture and trust boundary | 06 | Independent audit, penetration, and escape-test results |
| 02 | Threat model, abuse cases, and documented non-goals | 07 | RED/GREEN isolation and boundary-test evidence |
| 03 | Identity, pairing, protocol specifications, and test vectors | 08 | Supply-chain, provisioning, and secure-logistics records |
| 04 | Software bill of materials and dependency records | 09 | Depot recovery, revocation, custody, and incident procedures |
| 05 | Signed build provenance and reproducibility evidence | 10 | Residual-risk, remediation, and release-status record |

Assurance is a maintained service—not a one-time slogan.

Evidence completeness is stated by release. Gaps and assumptions remain visible.

Assurance profiles remain deliberately separate

Commercial privacy

AUDIENCE

Boards, family offices, legal and M&A teams, executive protection, crisis teams

ARCHITECTURE

Direct-only full-Linux endpoints with customer-defined policy

ASSURANCE DIRECTION

Independent assessment, hardware binding, secure development, lifecycle evidence, and Assurance options

Regulated / CUI

AUDIENCE

Federal contractors, critical infrastructure, and regulated enterprises

ARCHITECTURE

Direct-only endpoints with customer-managed policy, administration, and records controls

ASSURANCE DIRECTION

Applicable control mapping, validated components where required, and support for authorization of an exact configuration

Classified / NSS

SPONSOR-DEPENDENT

AUDIENCE

Sponsor-defined national-security missions

ARCHITECTURE

Sponsor-approved architecture, components, operating environment, and mission boundary

ASSURANCE DIRECTION

Sponsor-led evaluation, component validation, system assessment, and exact customer authorization

Component validation ≠ product evaluation ≠ system assessment ≠ customer authorization.

Black Swan Net does not independently authorize classified use.

Choose the engagement path that matches the decision

01

Private demonstration

Review the direct-session workflow, endpoint controls, failure states, and current development evidence.

02

Enterprise pilot

Define a 6–25 endpoint fleet, mission boundary, operating policy, custody, and measurable success criteria.

03

Paid design study

Translate the mission into architecture, operating procedures, test cases, costs, and an evidence plan.

04

Government briefing

Scope an unclassified discussion, controlled evaluation, CUI pilot, integrator path, or sponsor-defined program.

05

Integration partnership

Align interfaces, customer policy, logistics, evaluation responsibilities, and support boundaries.

06

Deployment decision

Proceed only when the exact configuration, evidence, CONOPS, authorization path, and customer approvals align.

Each engagement produces evidence for a decision—not just a demonstration.

NEXT STEP

Bring the mission, threat model, and constraints

Together, we will define:

- What information must be protected
- Which trust dependencies should be removed or isolated
- How identity, custody, sessions, and updates should work
- What the evaluation must prove
- Which assurance profile is appropriate

Black Swan Net — direct secure communications with a controlled trust surface.



Request an unclassified briefing, demonstration, pilot, or integration discussion

Gene Avakyan

Founder & Project Lead

contact@blackswannet.com

<https://blackswannet.com>