SkyDefended InfraApp v1.3

Architecture Distribuited Zero Trust and Model Multi-Plane

May 21, 2026 | Technical Architecture Document | Ismael Cruz Casasola

NEXOCYBER NETWORKS
NCN
NETWORKING, SEGURITY AND SYSTEMS

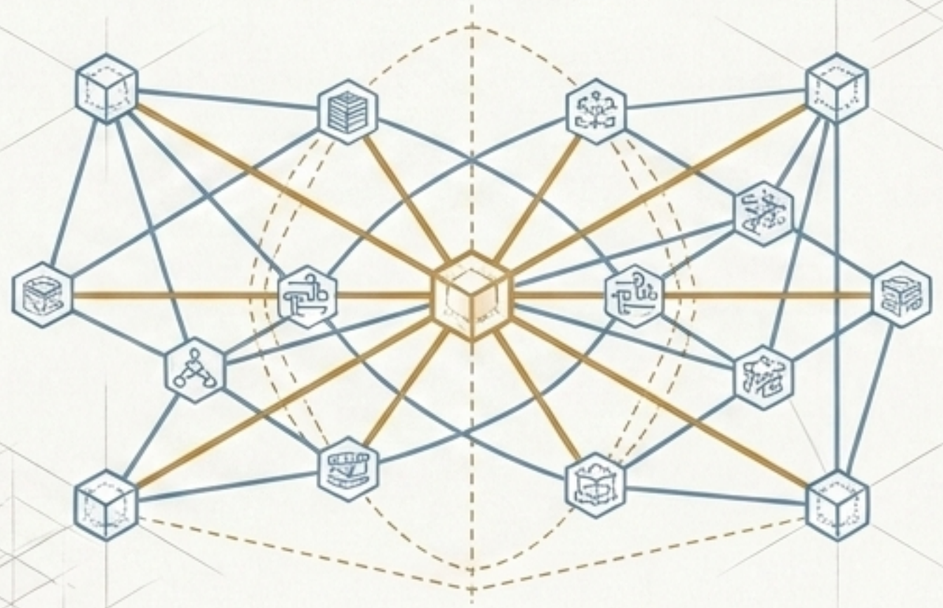
NEGATIVE SPACE

Data Centralization

SkyDefended InfraApp does NOT centralize the data or the functional logic of the applications. It does not absorb the operational domain of the software.

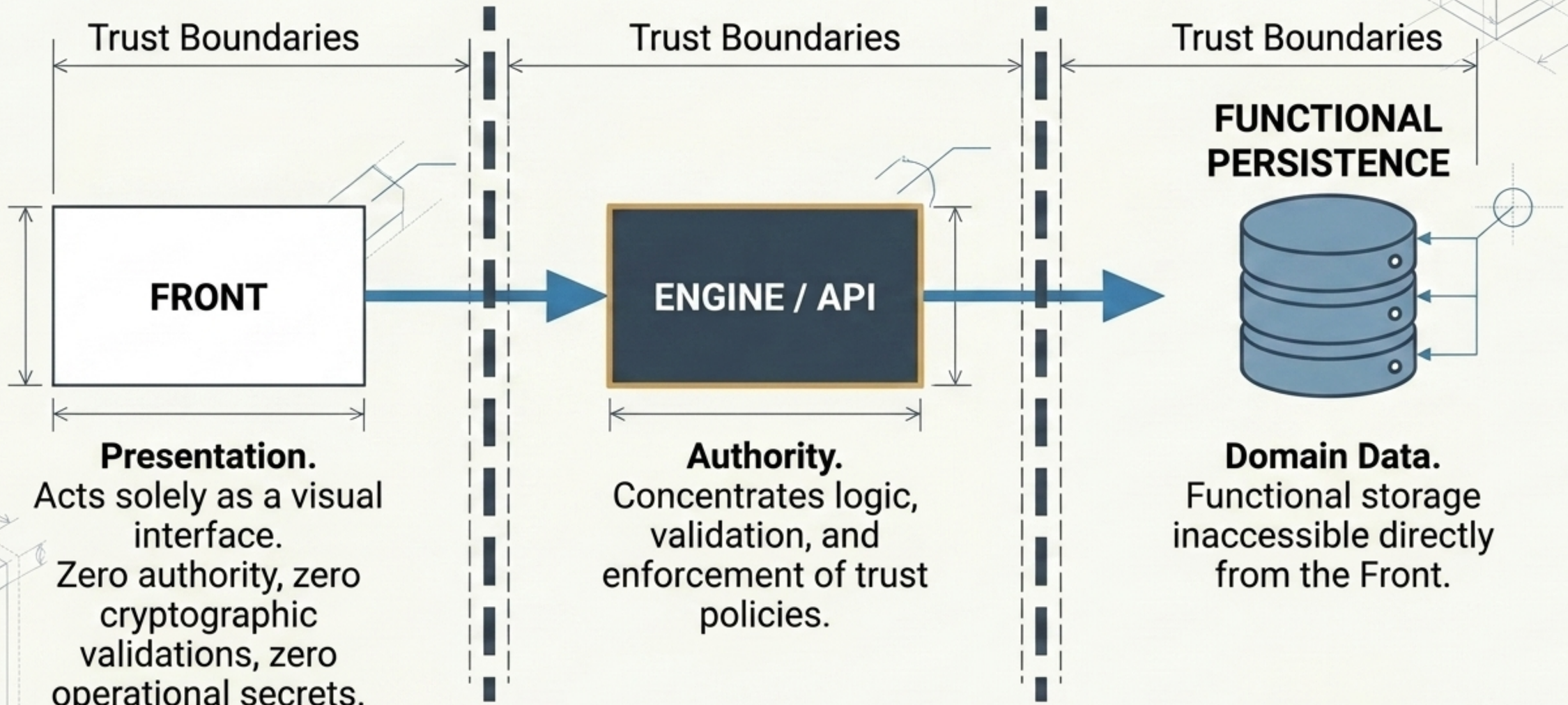
THE CORE AXIOM

Decentralized execution with centralized policy



Centralizes conditions. Exclusively governs the rules under which software can exist, operate, and interact within a distributed Zero Trust trust model.

The Core Architectural Principle

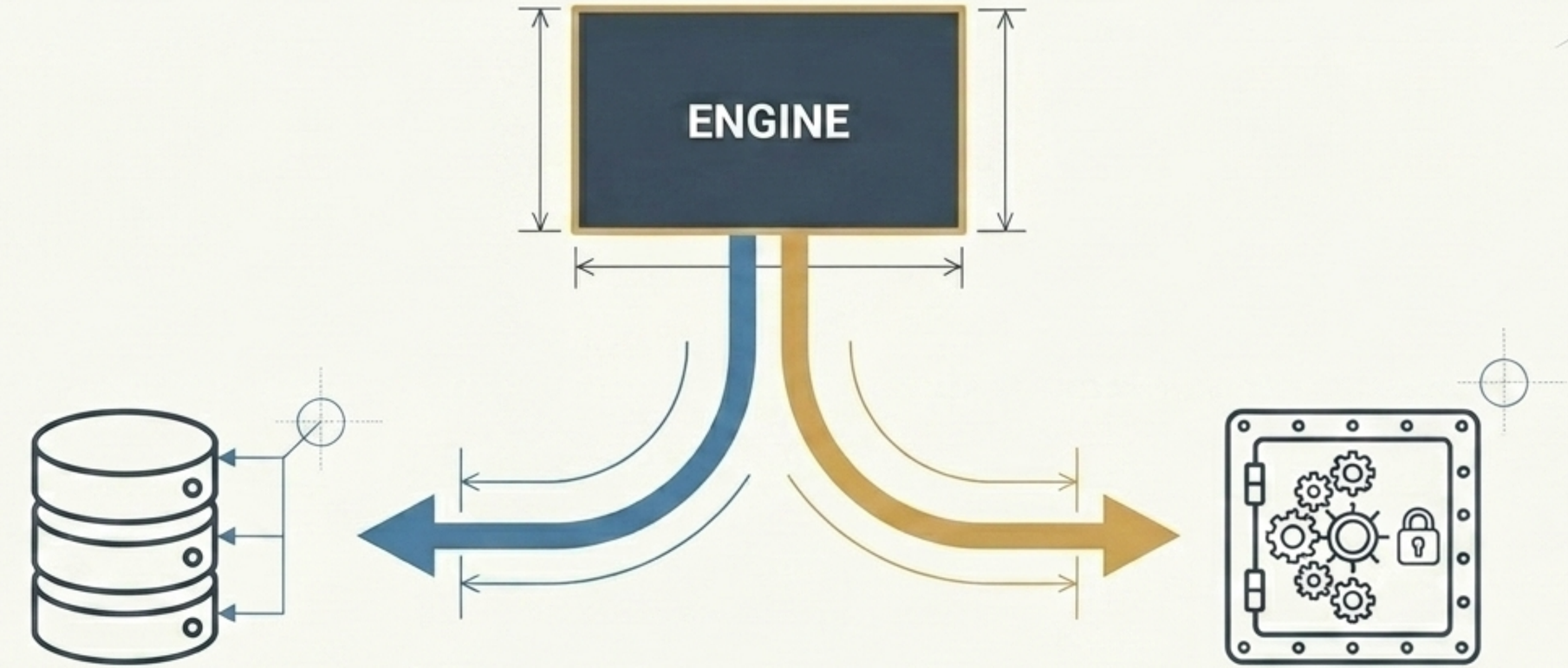


Presentation.
Acts solely as a visual interface.
Zero authority, zero cryptographic validations, zero operational secrets.

Authority.
Concentrates logic, validation, and enforcement of trust policies.

Domain Data.
Functional storage inaccessible directly from the Front.

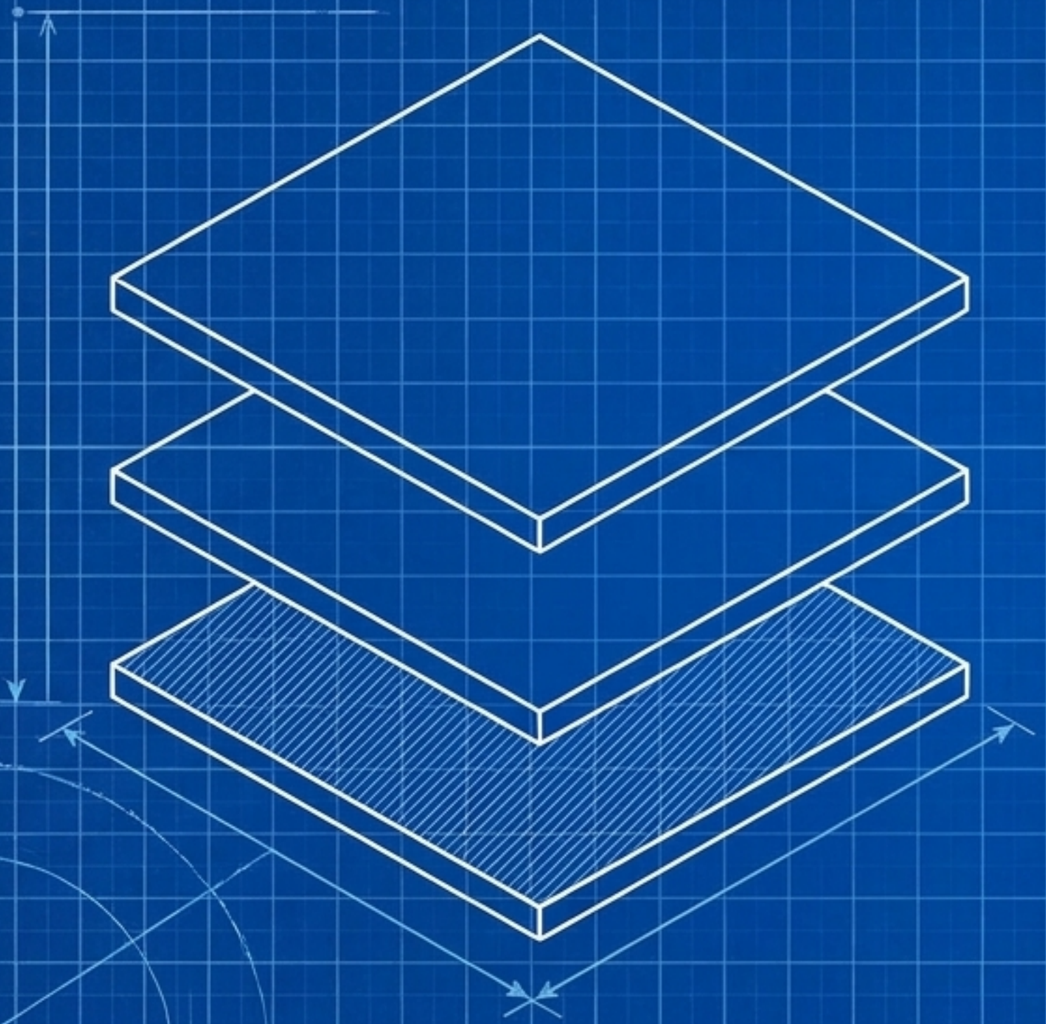
Separation of the Persistence Model



Functional Persistence
Stores operational data, state, and configuration. (Functional Domain).

Decoupled Cryptographic Persistence
Custody of identities, cryptographic material, and secrets. Never stored in functional DBs or ephemeral runtime memory. (Trust Domain).

The Three-Plane Model



Control Plane

Control (FRONT → ENGINE → DB)
Establishes tenancy, defines Policy Bundles, and issues root cryptographic trust.

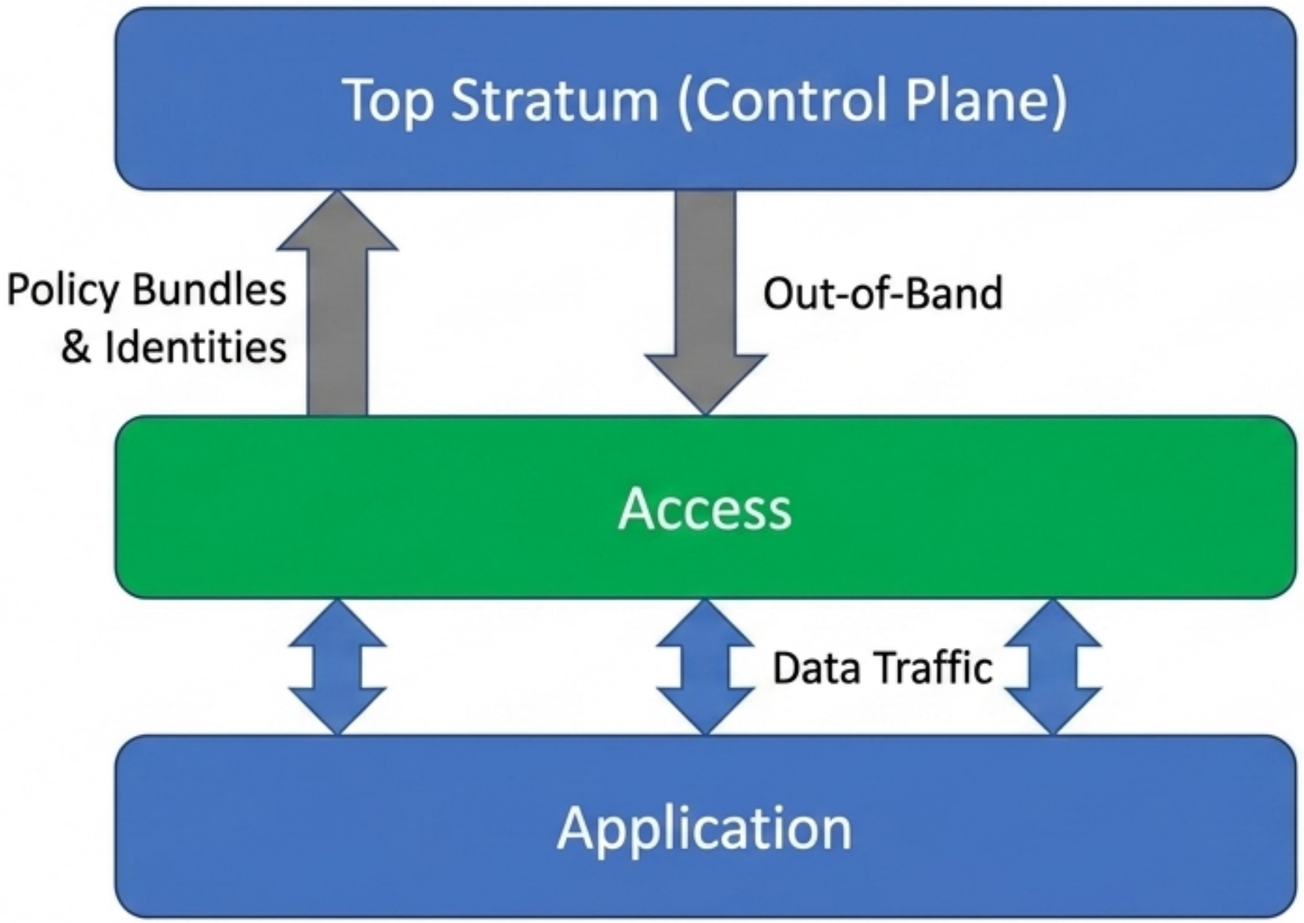
Access Plane

Access (FRONT → ENGINE → DB)
Single point of entry and unified tenant administration. Customer's operating environment.

Application Plane

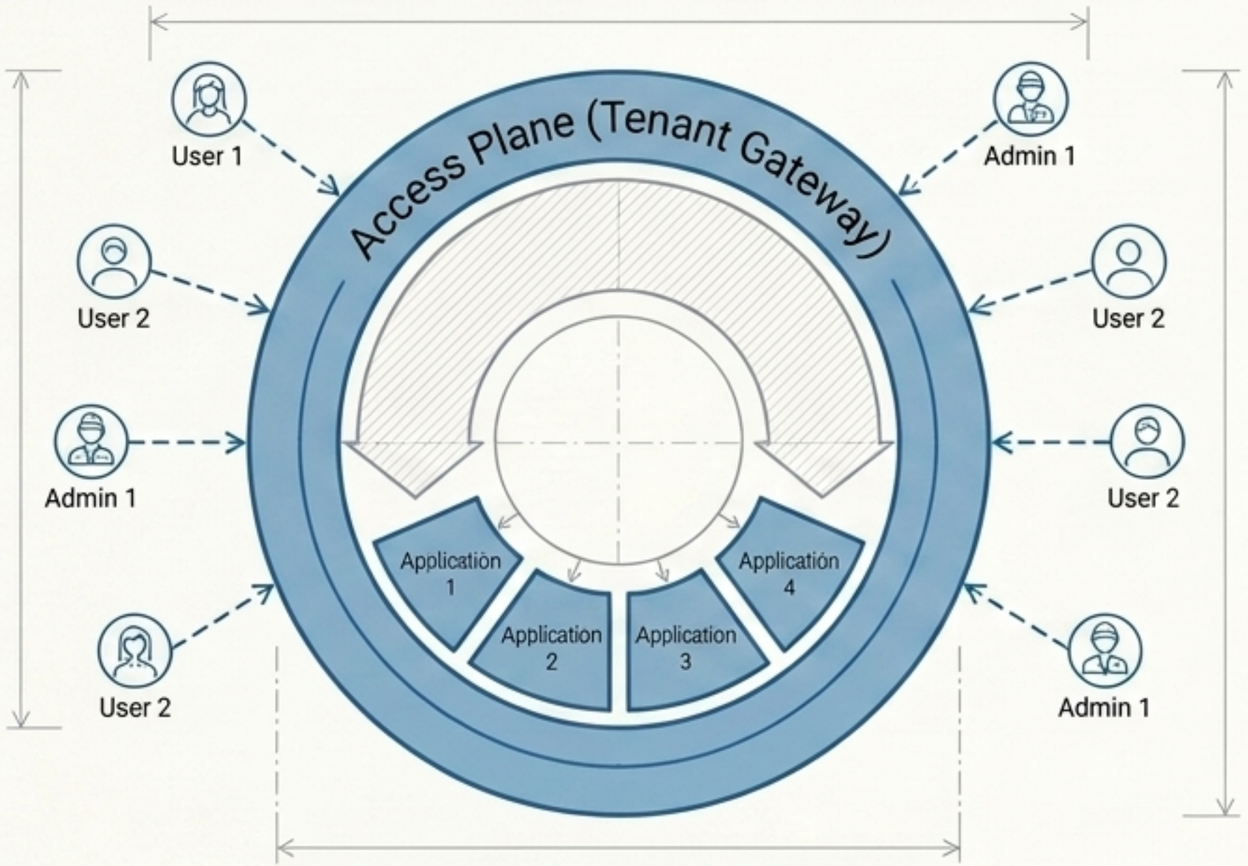
Application (FRONT → ENGINE → DB)
Functional execution, business logic, and independent data custody.

Control Plane: Root of Trust



What IT IS	What IT IS NOT
Root of Trust.	It is not a data plane.
Membership registers (Tenants, Licenses).	Outside the application data path.
Trust registers (Cryptographic identities, Policy Bundles).	Does not hold operational private keys of lower Engines.
Operated entirely by NCN.	Does not execute functional logic.

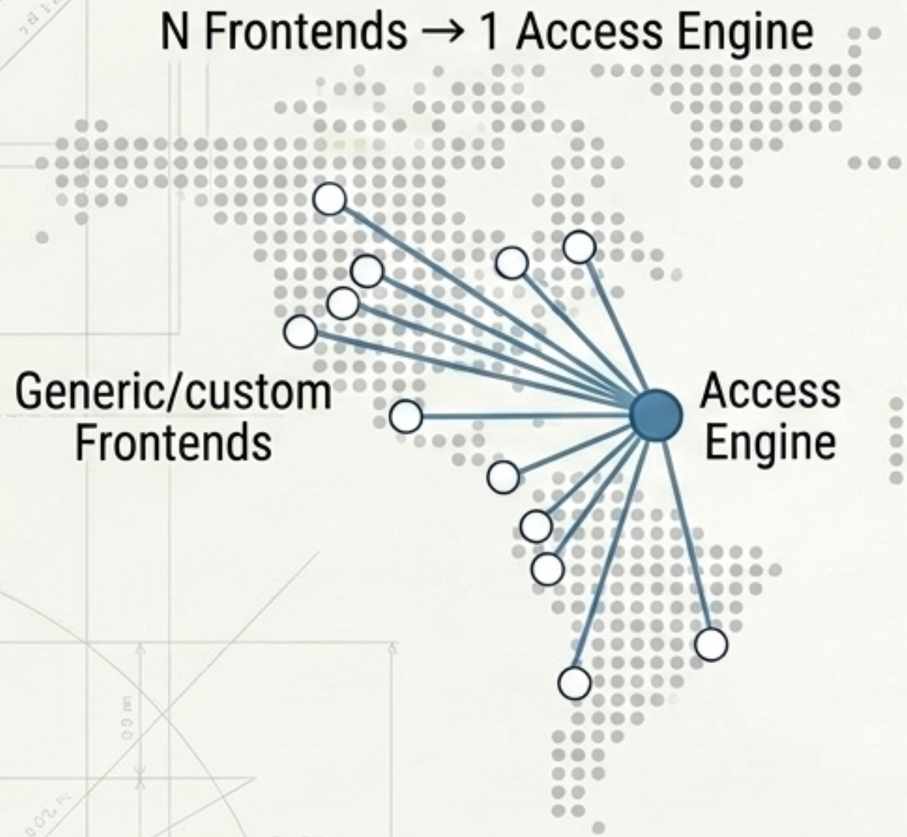
Access Plane: Tenant Gateway

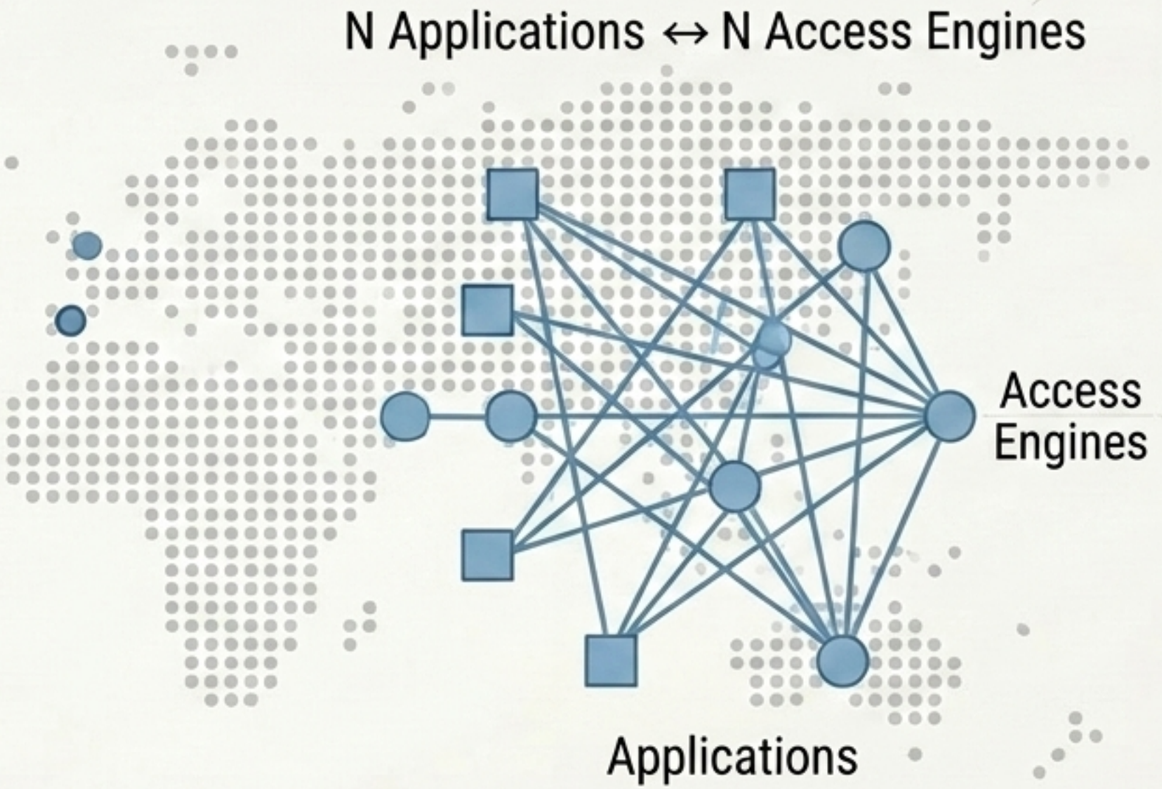


The unified administrative shell of the tenant. Instances identities, sessions, ingress policies, and operational context.

Structural Rule: Unifies the administrative experience and access control, but DOES NOT define business logic or govern internal product data.

Topological Independence and Distributed Relationships

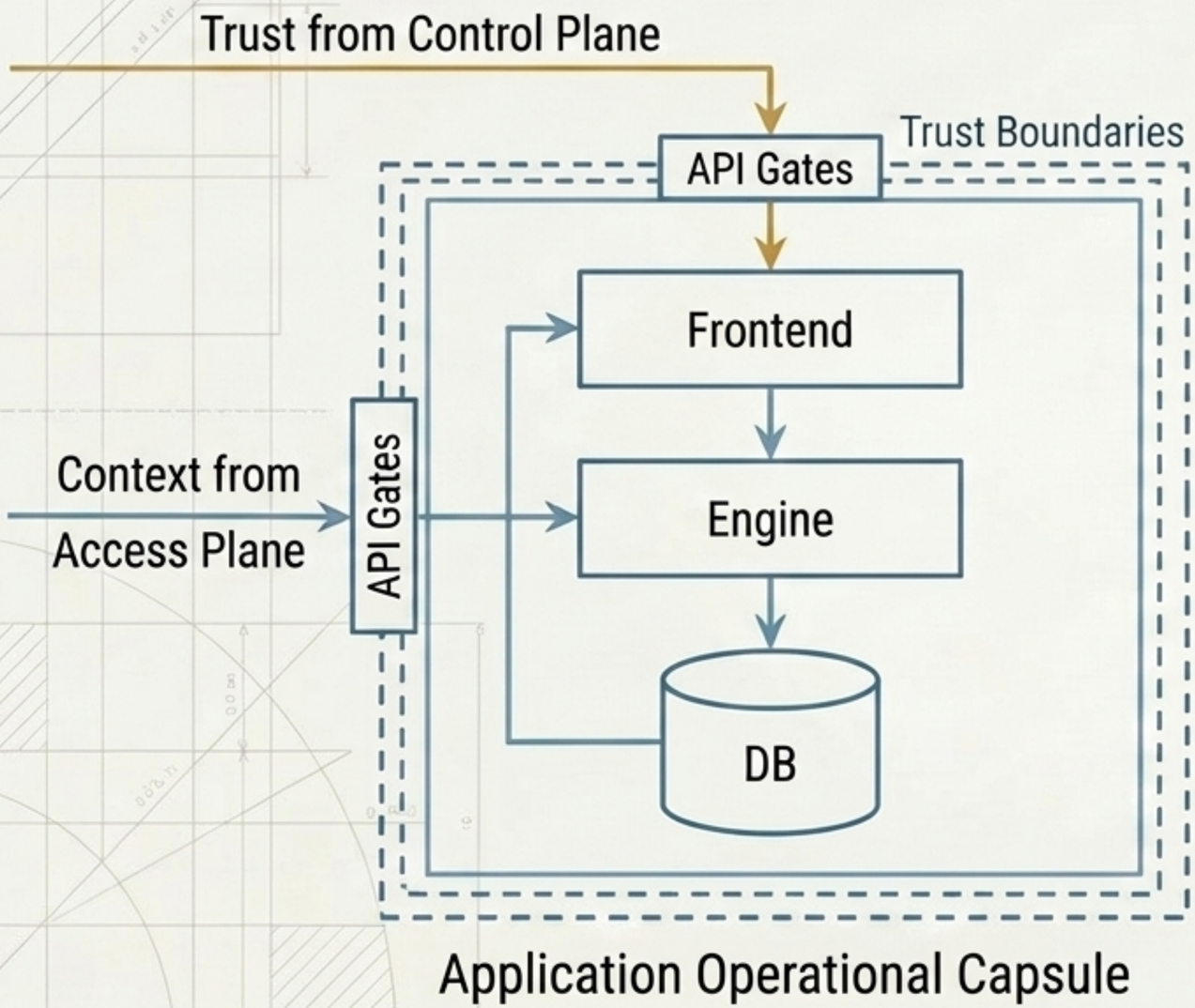




Topological Independence: Generic or custom-branded Frontends (N) point to the same authority (1 Engine).

Applications connect to the Access Plane without being tied to a specific physical or geographical instance.

Application Plane: The Operational Capsule

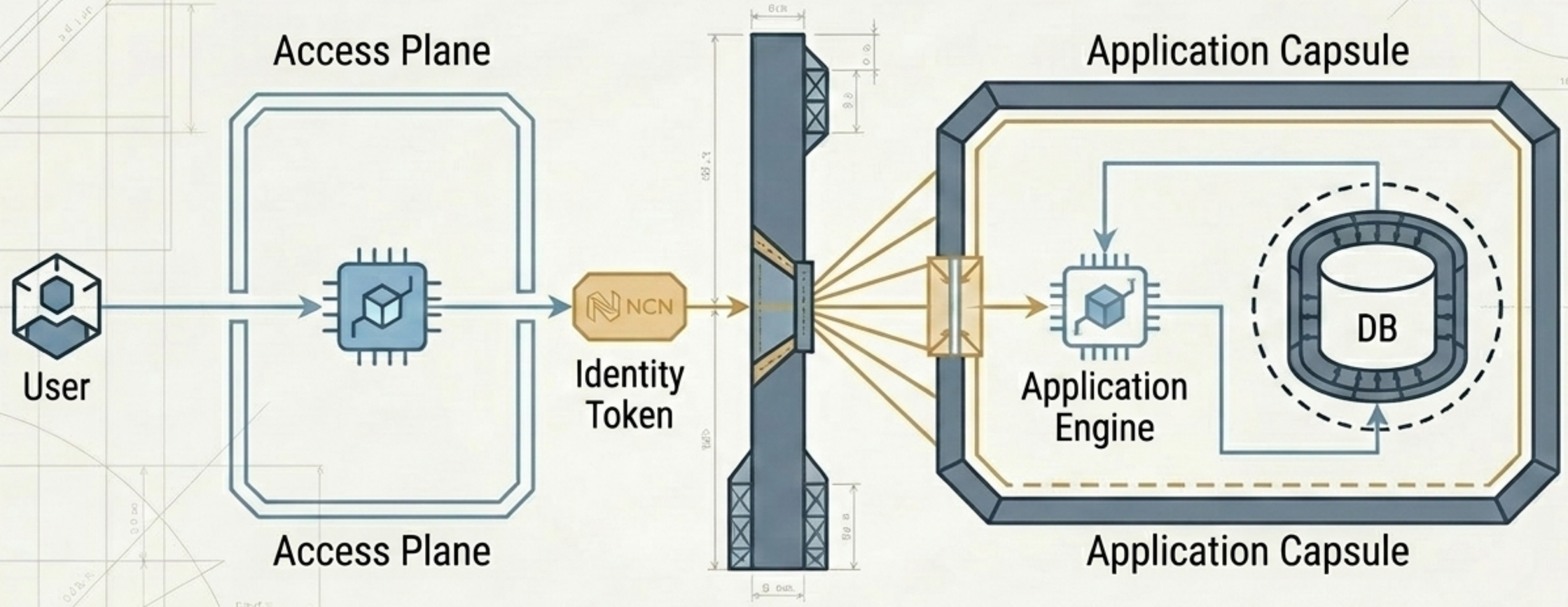


Total Functional Autonomy: The application maintains its own data model, logic, and internal rules.

Local Validation: Verifies trust using Policy Bundles without relying on synchronous calls to the Control Plane.

Additional Frontends: Ability to expose independent public portals outside the administrative shell.

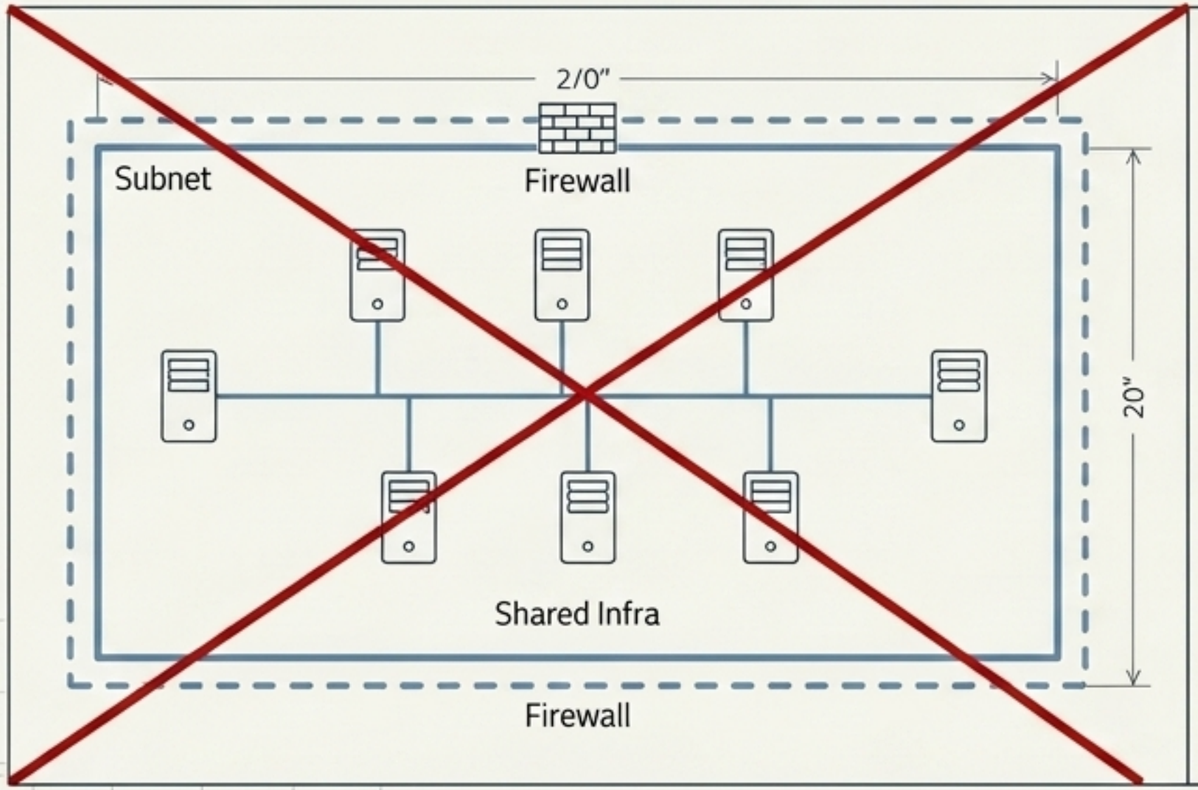
Integration without Absorption



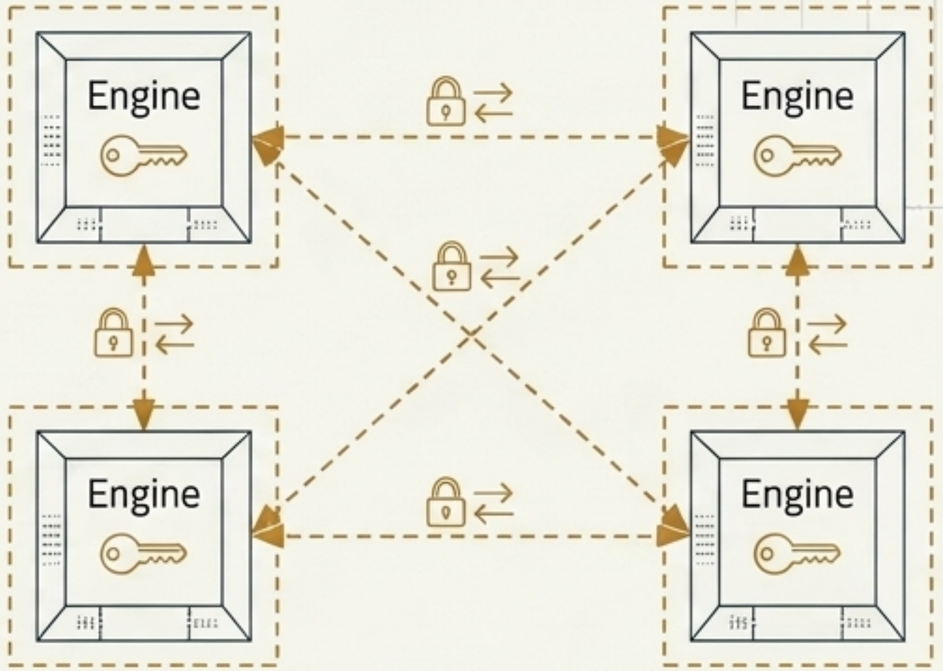
- The user interacts in the unified administrative environment of the tenant.
- The Access Plane transports identity and context.
- Persistence, internal processing, and data remain strictly encapsulated in the application domain.

Trust Mechanics: Distributed Trust Boundaries

Implicit Trust (Subnet/Proximity)



Distributed Cryptographic Trust

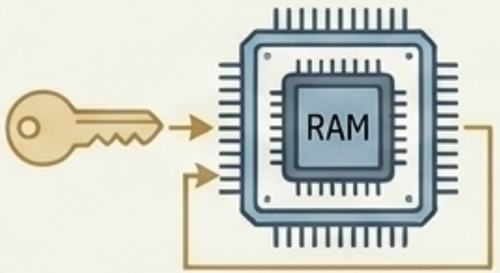


Distributed Trust Boundaries. Trust does not reside in shared infrastructure, topological proximity, or user sessions.

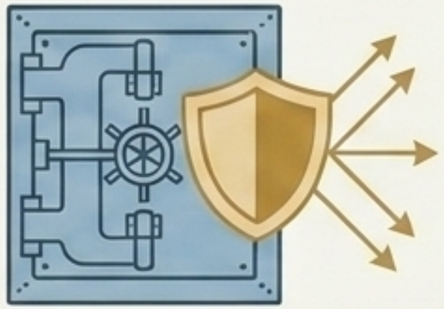
Identity Associated with Engines. Each Engine possesses a persistent cryptographic identity, validated locally via Zero Trust mechanisms.

Evolution of Cryptographic Custody

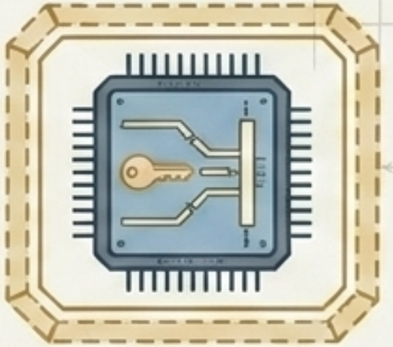
Level 1 (Vault KV)



Level 2 (Vault Transit)



Level 3 (HSM remote-sign)



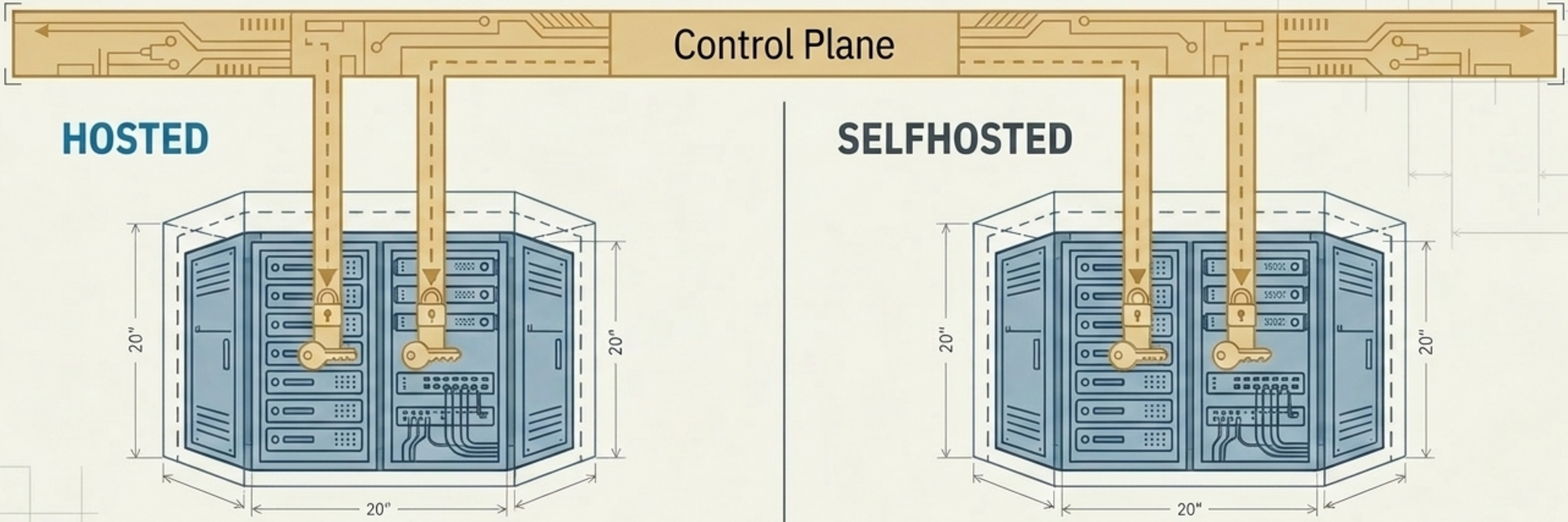
Decoupled persistence.
Temporary load in runtime memory.

Non-exportable custody.
The runtime requests operations without direct access to the key.

Hardware-backed custody.
The private key never leaves the dedicated module.

Structural Objective: Progressively decouple cryptographic operations from the ephemeral runtime.

Operating Models and Topological Resilience



Operated by NCN (Infrastructure, runtime, networking). Data autonomy maintained.

Operated by Client/Third Party (Physical sovereignty, regulatory compliance).

In both models, the Control Plane continues to distribute trust and the tenant maintains full integration without fracturing the security topology.

Multi-Tenant Isolation on Shared Infrastructure

Coexistence on shared infrastructure with cryptographic and operational isolation.

Logical separation guaranteed through distributed Policy Bundles

Independent cryptographic identities per context.

Zero implicit inter-tenant trust; all interaction requires explicit enablement in the Control Plane

Architectural Synthesis: SkyDefended InfraApp

Structural Axiom.

(FRONT → ENGINE → Persistence).
Unbreakable separation of
presentation and authority.

Three Planes.

(Control, Access, Application).
Separation of ownership,
administration, and execution.

Unified Governance.
Absolute Data Autonomy.

Zero Trust Identity.

Trust founded on decoupled
cryptographic persistence,
never on proximity or
network.

Integration without Absorption.

Applications integrate into the
tenant shell without sacrificing their
functional or topological sovereignty.