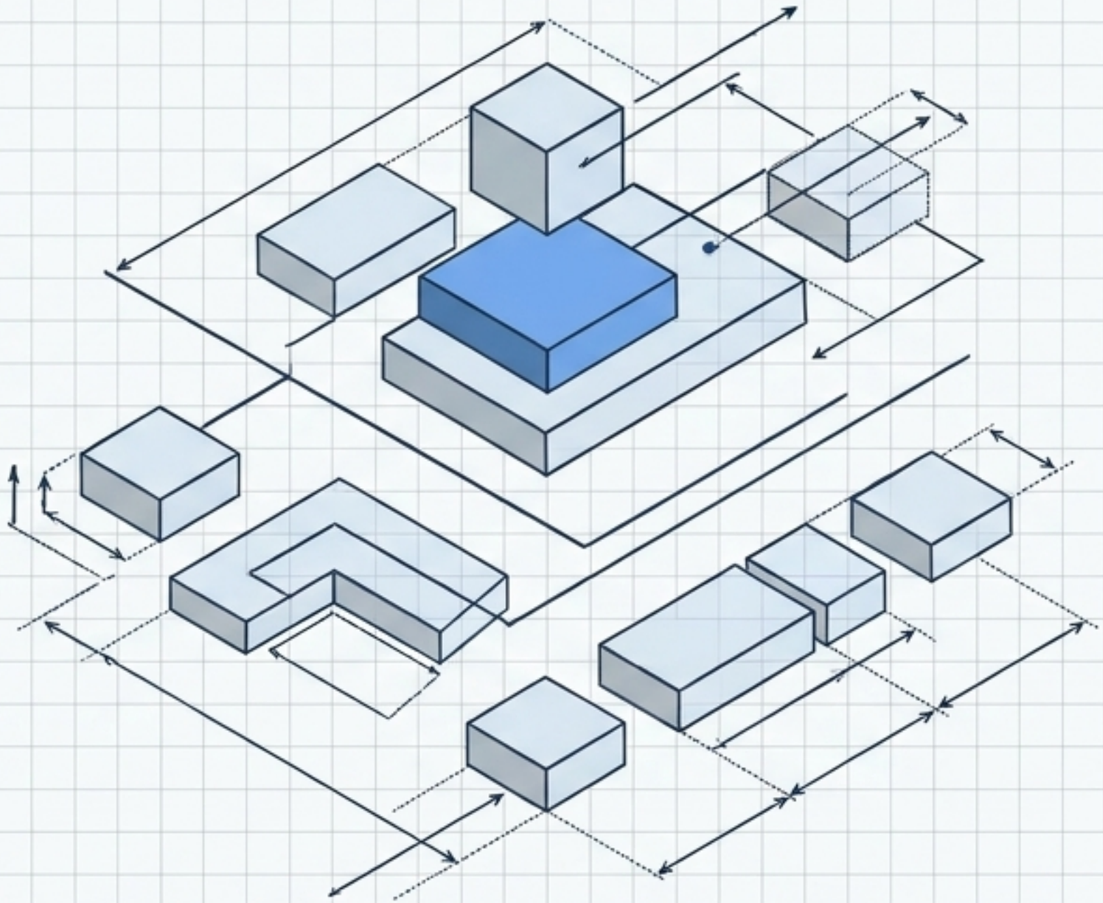
Distributed Authoritative Governance Model

Multi-Plane Zero Trust Architecture in SkyDefended InfraApp (v1.1)



Document: D06 - IAM + PIM + ABAC
Author: Ismael Cruz Casasola

NEXOCYBER NETWORKS

NotebookLM

The Paradigm of Authoritative Sovereignty

SkyDefended InfraApp implements a sovereign layer of distributed authoritative governance built on explicit cryptographic trust.

Identity-Centric

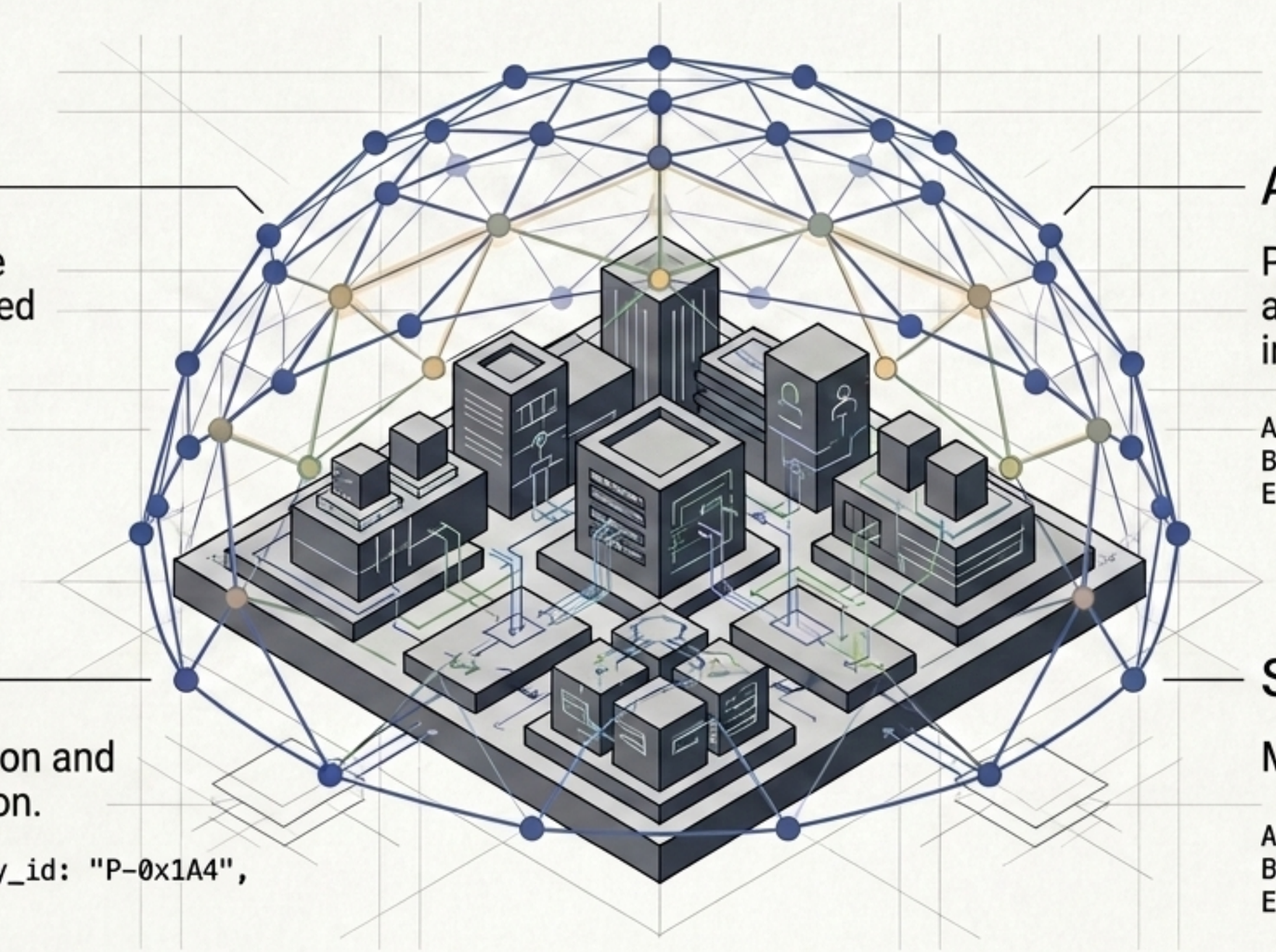
Authorization follows the cryptographically validated identity.

```
PKI_VALIDATED: true;
ASSERTION_BOUND: user_did
```

Application Autonomy

Provides the unified administrative layer without invading business logic.

```
ADMIN_LAYER: unified_control;
BUSINESS_LOGIC: untouched;
ENFORCEMENT: decentralized
```



Context-Aware

Distributed local validation and real-time ABAC evaluation.

```
LOCAL_POLICY_EVAL: {policy_id: "P-0x1A4",
timestamp: "T-NOW",
risk_level: "LOW"}
```

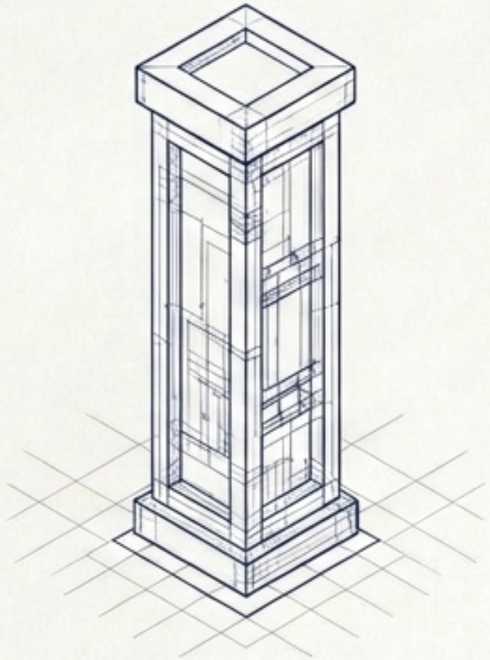
Sovereign Shield

Multi-tenant ecosystem

```
ADMIN_LAYER: unified_control;
BUSINESS_LOGIC: untuched;
ENFORCEMENT: decentralized
```

NotebookLM

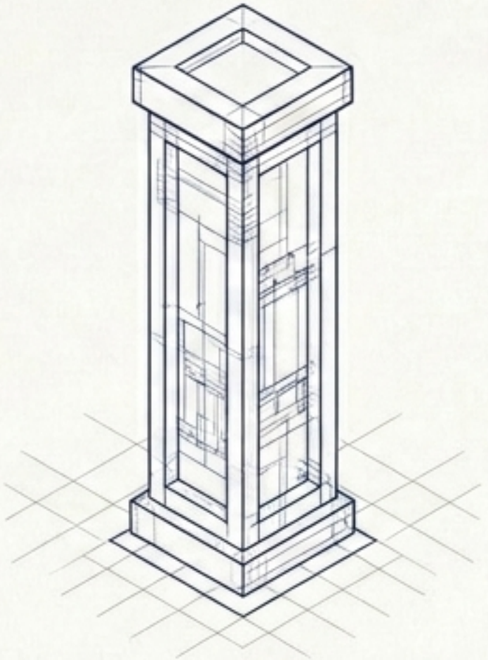
Decoupling Access: The Zero Trust Triad



Authentication (Identity)

Question: Who are you?

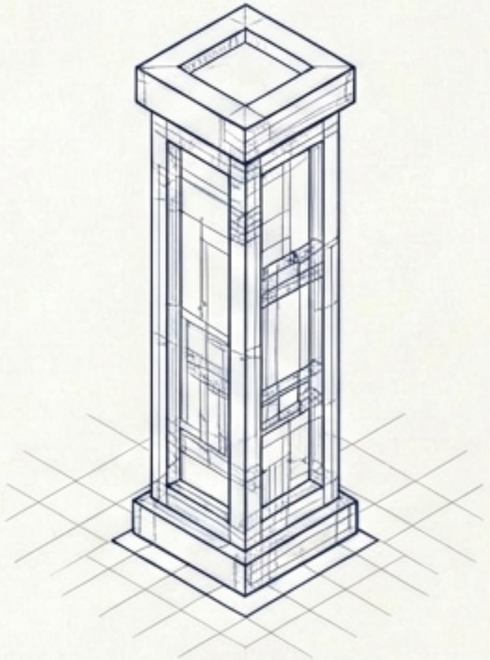
Mechanism: `Valid identity, credentials, OIDC.`



Cryptographic Trust (D02)

Question: Can we relate?

Mechanism: `RSA Signatures, JWKS, Trust Bundles, Engines.`



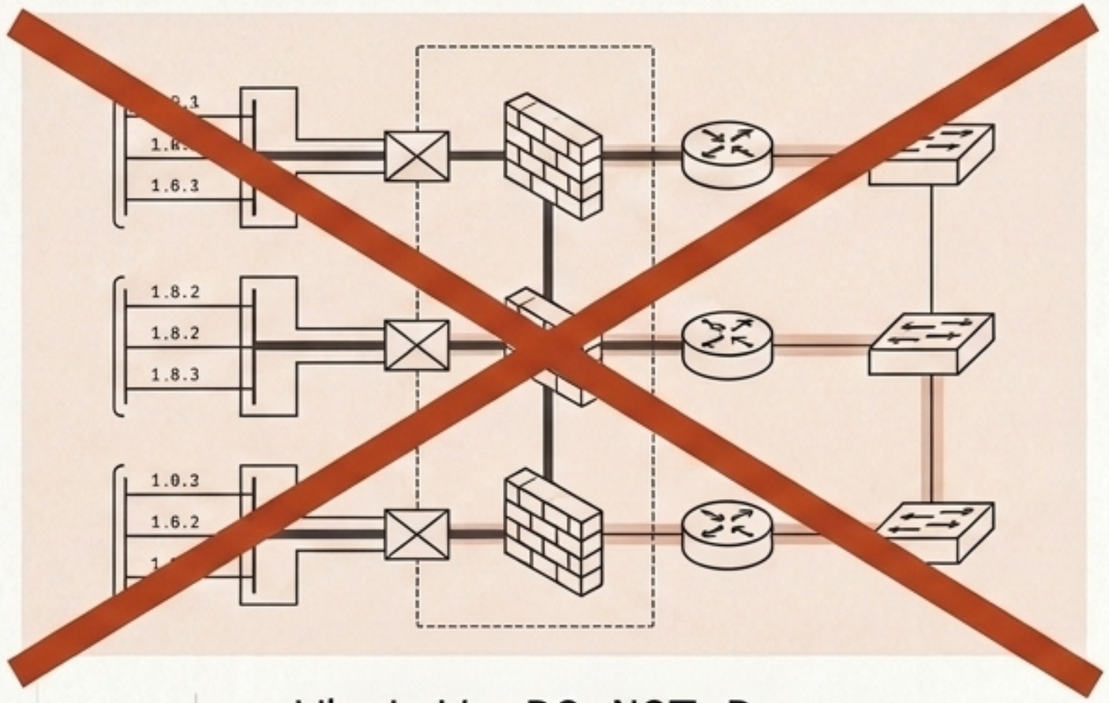
Authorization (D06)

Question: What can you do in this relationship?
Mechanism: `Explicit permissions, IAM, PIM, local validation.`

Cryptographic trust and authorization represent strictly distinct layers of the system.

NotebookLM

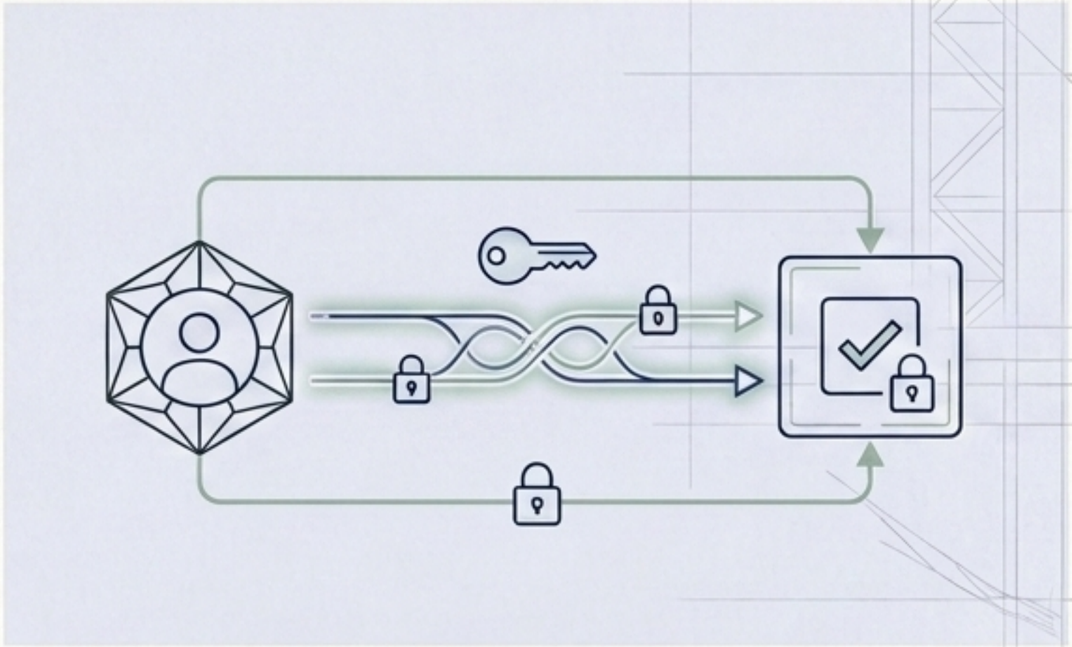
Zero Trust Principles: Decision Vectors



What We DO NOT Do

SkyDefended InfraApp does NOT base authorization on:

- Network or subnets.
- Cluster or shared infrastructure.
- Topological proximity.
- IP or physical location.



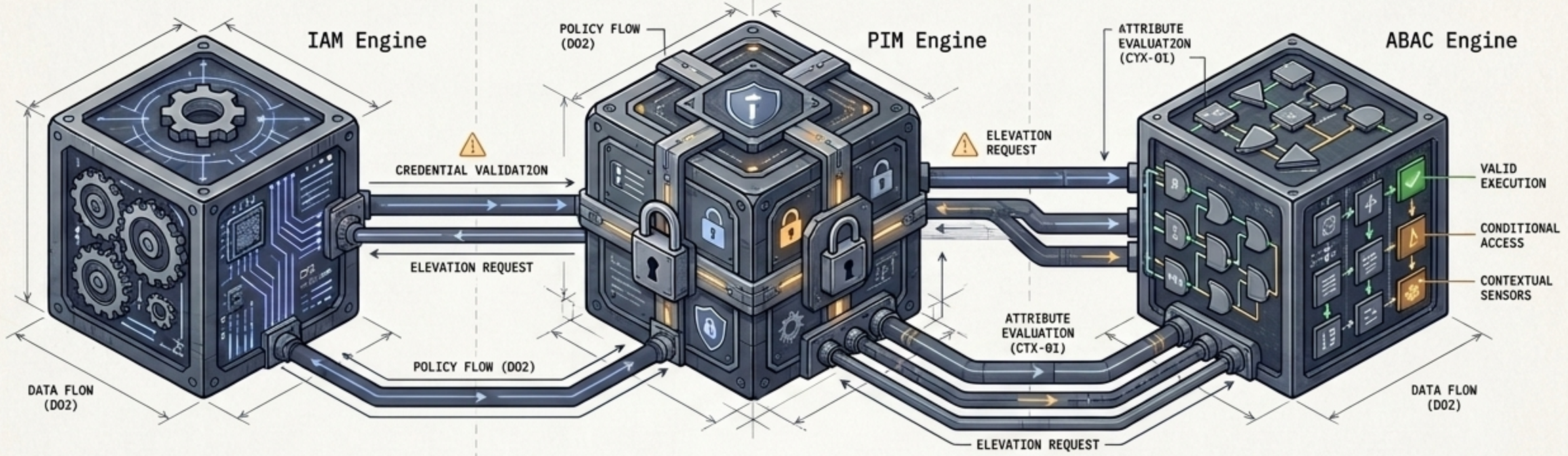
What We DO

Authorization always derives from:

- Explicit identity.
- Declared authorizative capacity.
- Context.
- Cryptographically authorized relationships.
- Local validation.

NotebookLM

Governance Engines: IAM, PIM and ABAC



IAM (Identity & Access Management)	PIM (Privileged Identity Management)	ABAC (Attribute-Based Access Control)
Nature: Persistent structural capacity.	**Nature:** Contextual temporary elevation.	**Nature:** Contextual restriction.
Purpose: Daily operation, automation, base roles.	**Purpose:** Critical operations, destructive changes, auditing.	**Purpose:** Define under what conditions an already authorized capacity operates.
Duration: Permanent.	**Duration:** Limited (with automatic expiration).	**Mechanism:** Rules on bindings and roles.

NotebookLM

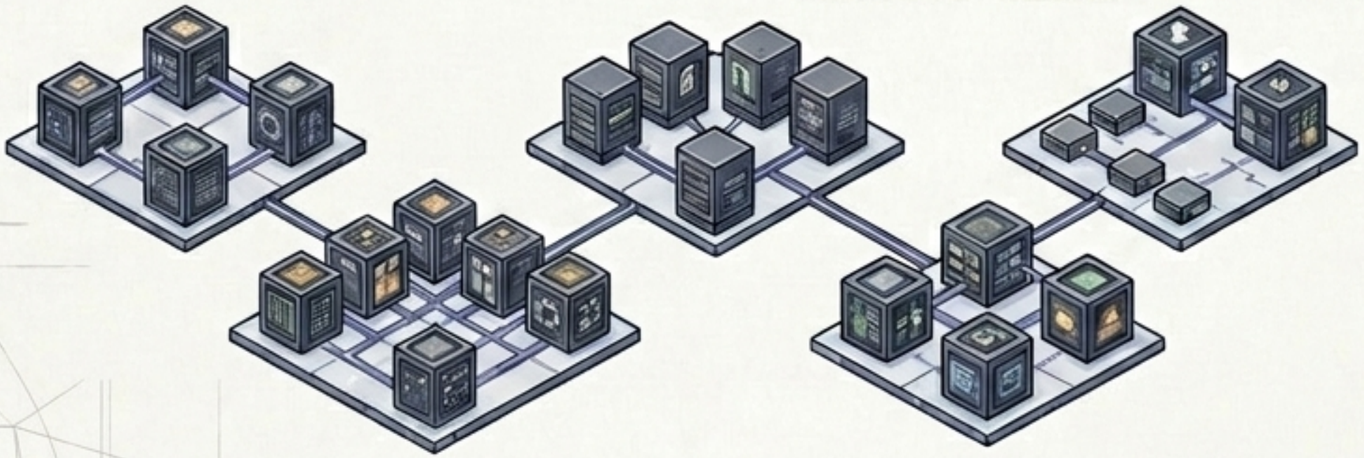
Isolation Topology: Control vs. Access

Control Plane

Key Characteristics
▪ **Governs:** Platform Root of Trust, operators, authoritative synchronization.
▪ **Excludes:** Tenants, functional business logic.
▪ **Model:** PIM-First (Temporary elevation priority).

TRUST BOUNDARY

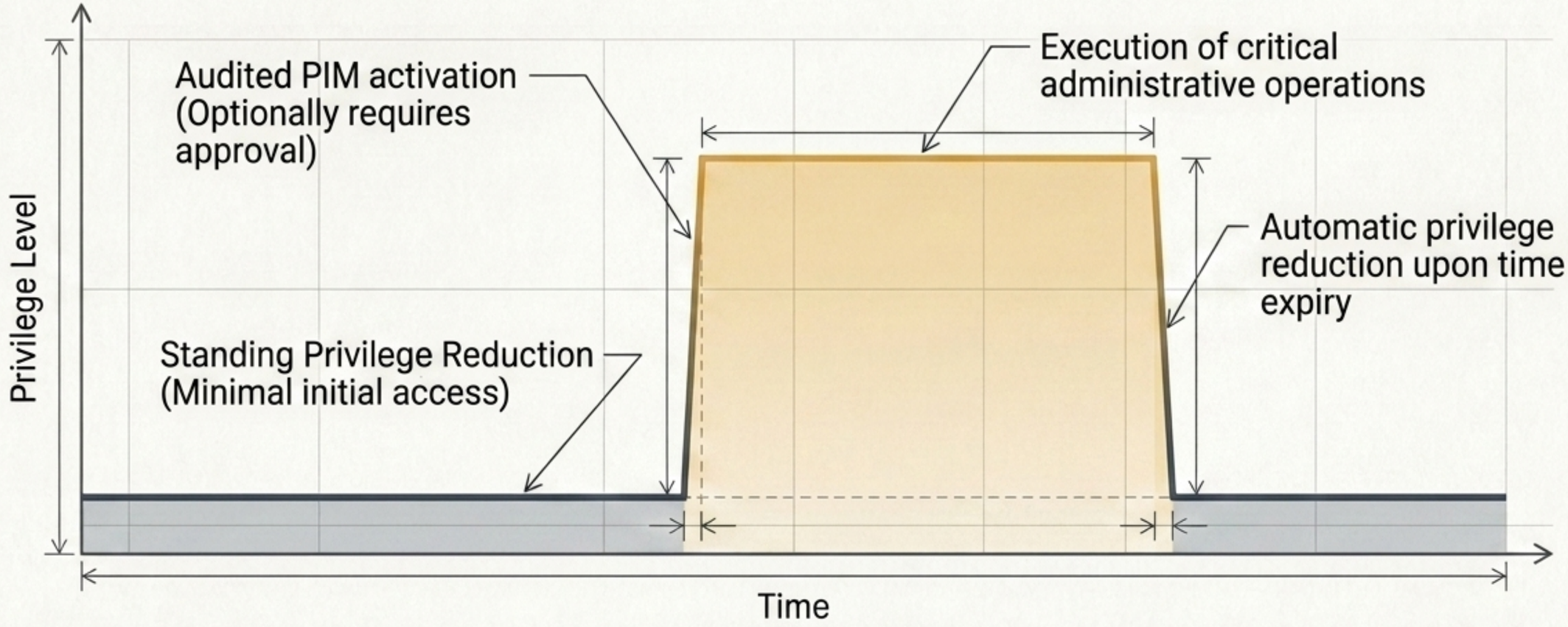
Access Plane



Key Characteristics
▪ **Governs:** Tenants, functional users, application administration.
▪ **Model:** Hybrid (Persistent operational IAM + PIM for sensitive ops.).

NotebookLM

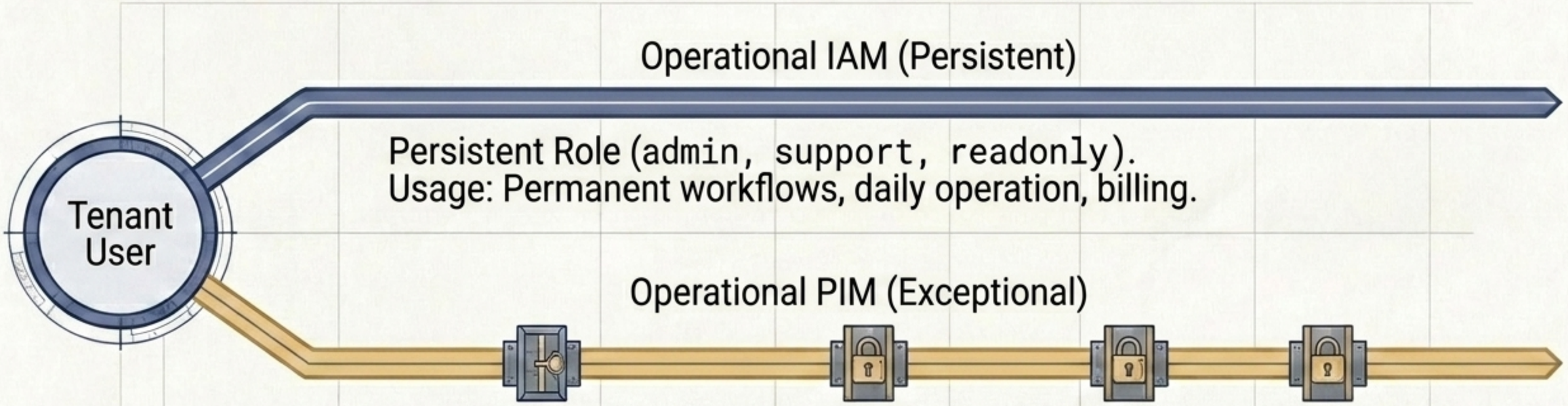
Control Plane: PIM-First Architecture



Permanent IAM roles are reserved for automation and machine identities. Human administrative operation occurs exclusively through temporary PIM elevation.

NotebookLM

Access Plane: Hybrid Operational Governance



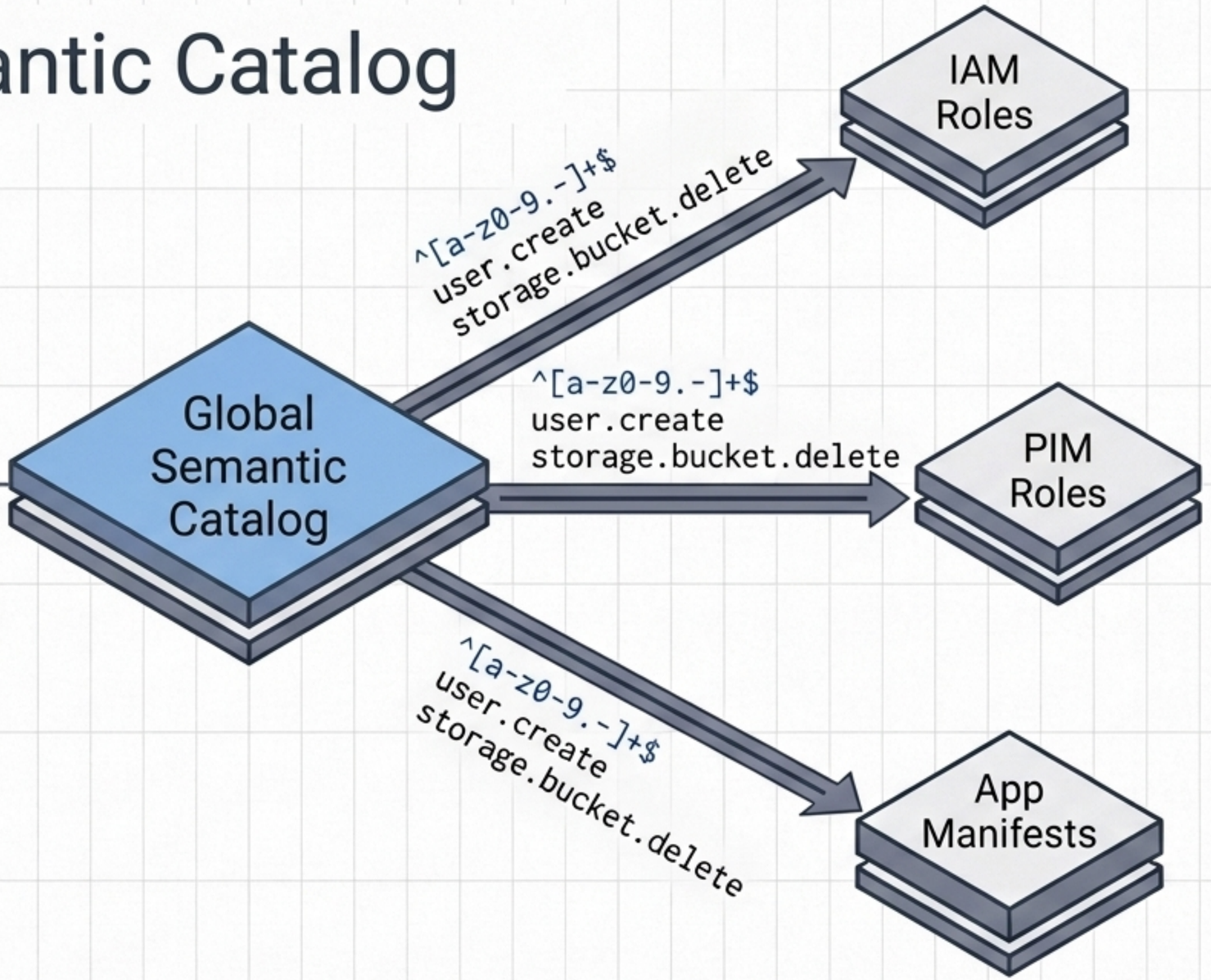
Users maintain one or several persistent IAM roles, with zero or several temporarily assignable PIM roles.

NotebookLM

The Global Semantic Catalog

- **Global Semantic Identity:** Permissions are identified by unique slugs (e.g., `user.create`, `storage.bucket.delete`).

- **Single Source of Truth:** Permissions exist only once. PIM and IAM Roles instantiate the same semantic permissions without duplicating them.

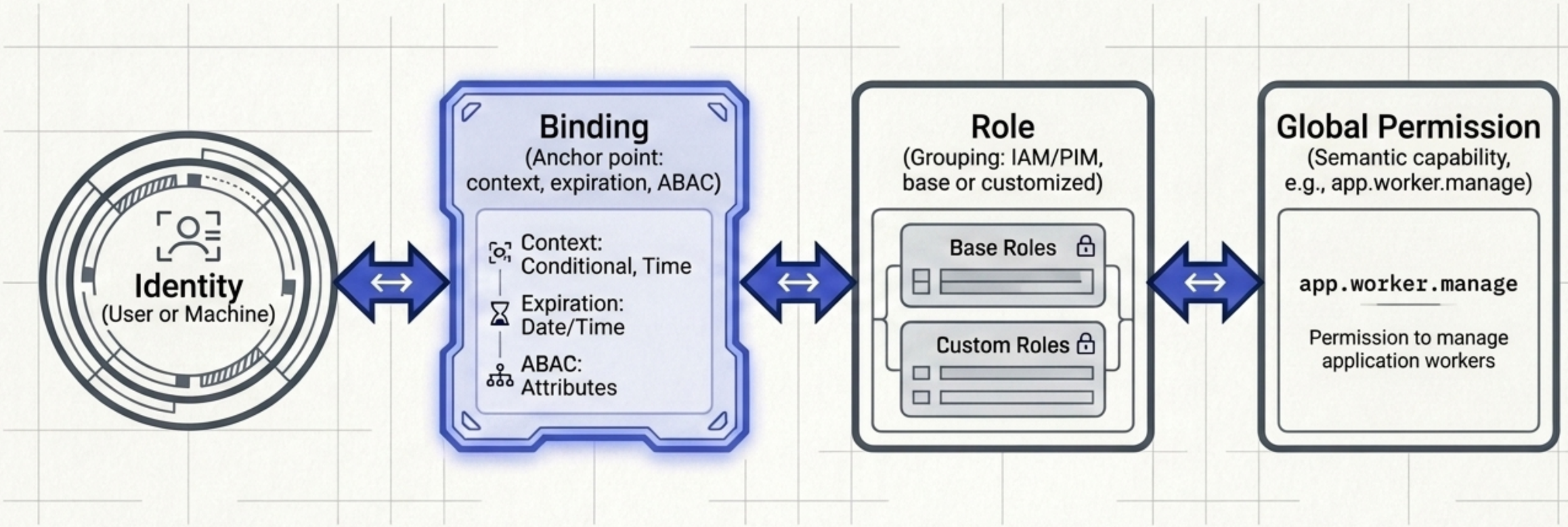


Exclusions

The catalog does NOT store state: it does not contain sessions, bindings, tenants, or active elevations. Only reusable definitions.

NotebookLM

Anatomy of Assignment: Authoritative Bindings

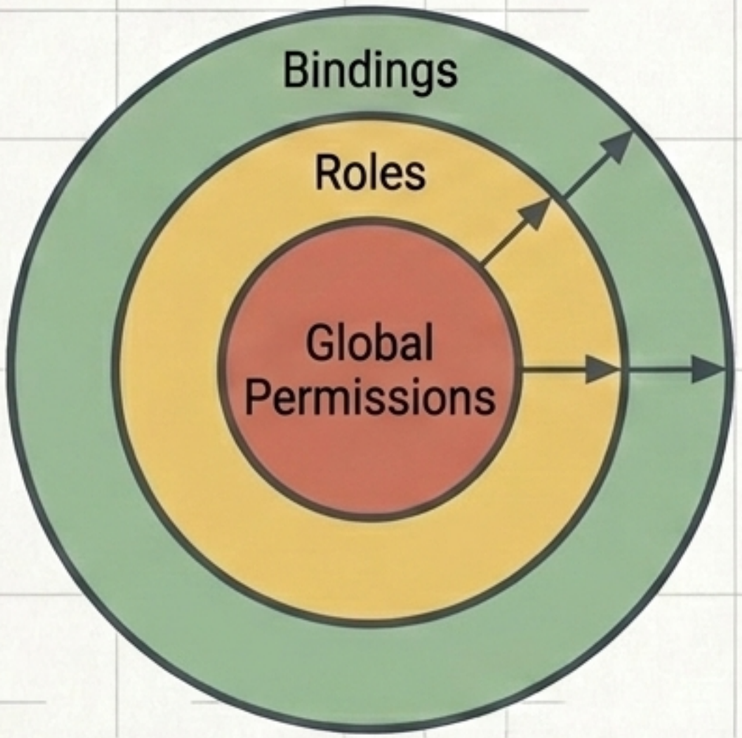


Insight

The binding is the effective assignment. It dynamically relates identities to groupings of semantic capabilities.

NotebookLM

“Blast Radius” Control: Contextual ABAC Strategy

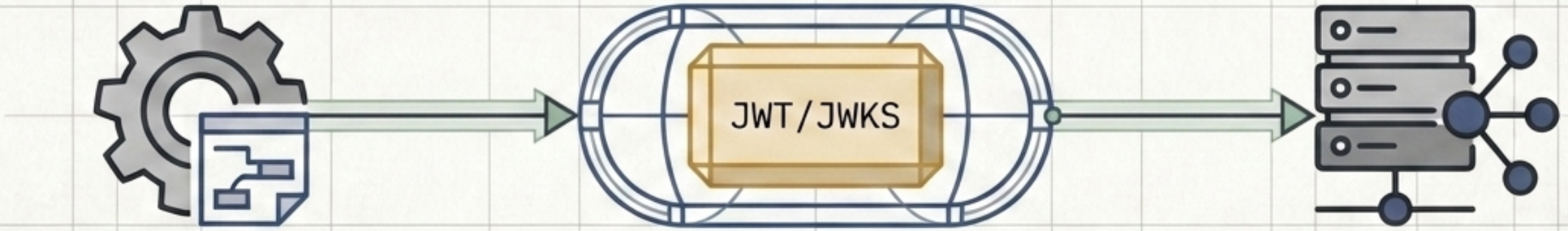


- **(Red) NEVER on Permissions (Access):** Applying ABAC to global permissions causes contextual pollution, blocking system operations by propagating restrictions to all roles that use that permission.
- **(Green) YES on Bindings and Roles:** The ABAC contextual restriction is applied in the outer layers of assignment.

In the Access Plane, permissions remain as pure authoritative semantics. Contextualization occurs locally in the Binding.

NotebookLM

Machine Identity and Service Principals Governance



Non-Human Subjects

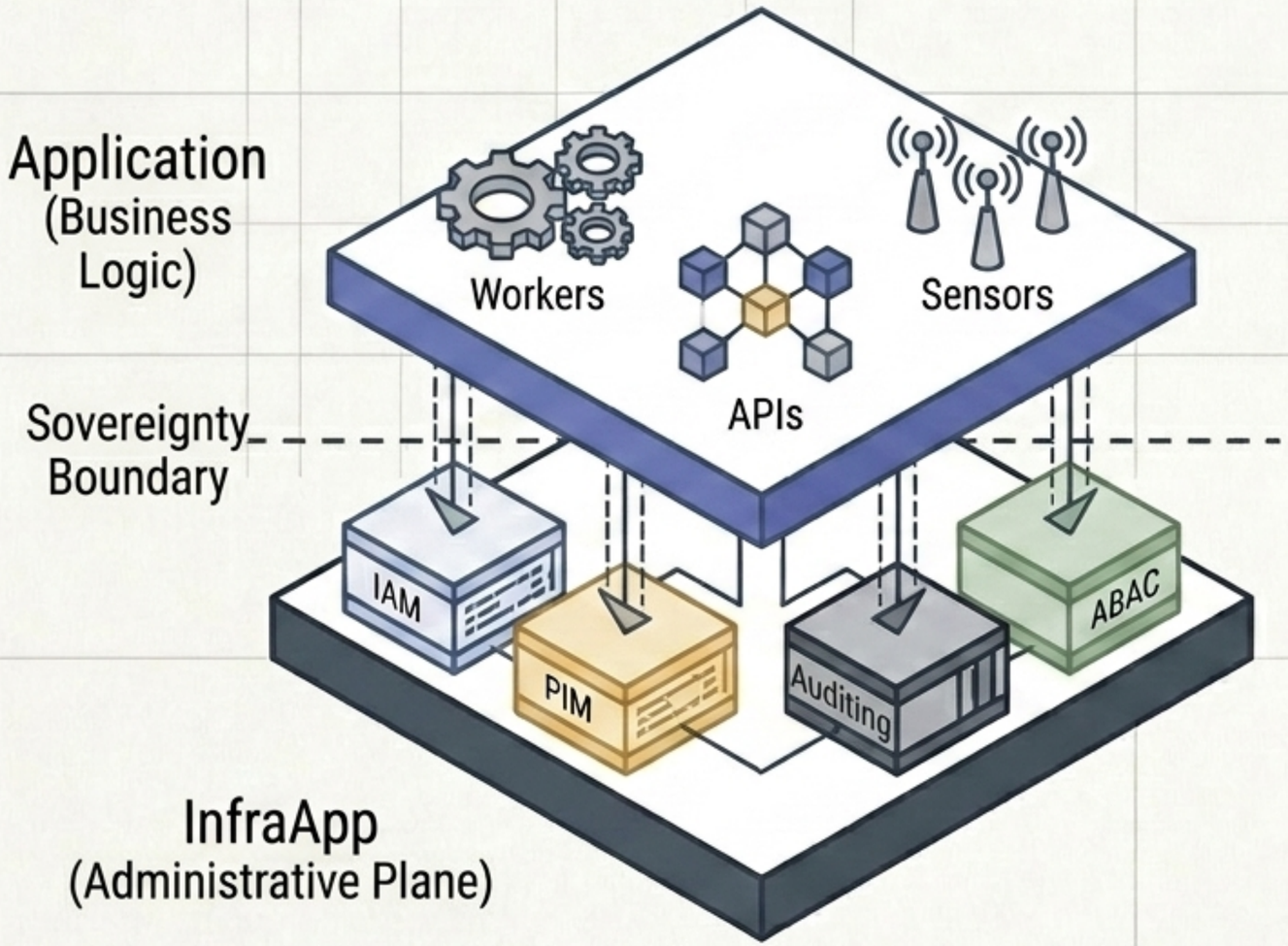
Workers, internal processes, pipelines, App <-> App integration.

Control Mechanism

- Machine identities operate mainly under persistent IAM roles.
- They are governed by the same global permissions, bindings, and ABAC restrictions as human identities.
- Inter-application communication requires cryptographically signed workloads (D02).

NotebookLM

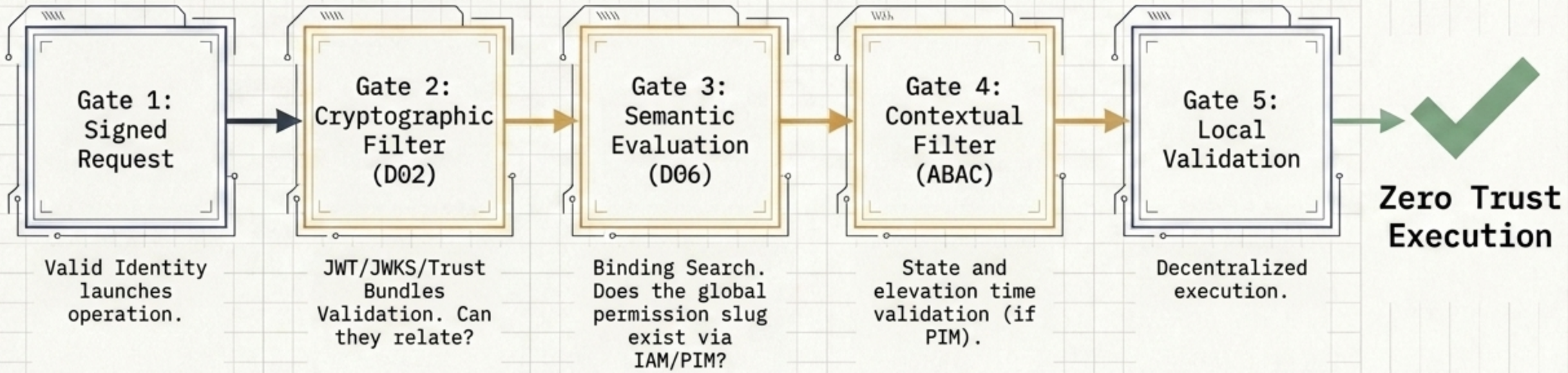
Application Integration: The Unified Administrative Plane



- **Functional Autonomy**: The app mainteins 100% control over its business logic, public APIs, and internal processes.
- **Delegated Administrative Layer:** The app synchronizes its permissions (manifests) with InfraApp, consuming the platform to govern administrative users, privilege elevation, and auditing.

NotebookLM

Distributed Authorization Flow (Synthesis)



NotebookLM

Architectural Conclusions

SkyDefended InfraApp implements a sovereign layer of distributed authorization governance built on explicit cryptographic trust.

Control

Maintains global semantic authority.

Access

Materializes the operational and contextual authorization.

Applications

Consume IAM/PIM/ABAC while retaining absolute functional autonomy.

Architecture complete. End of D06 specification.

NotebookLM