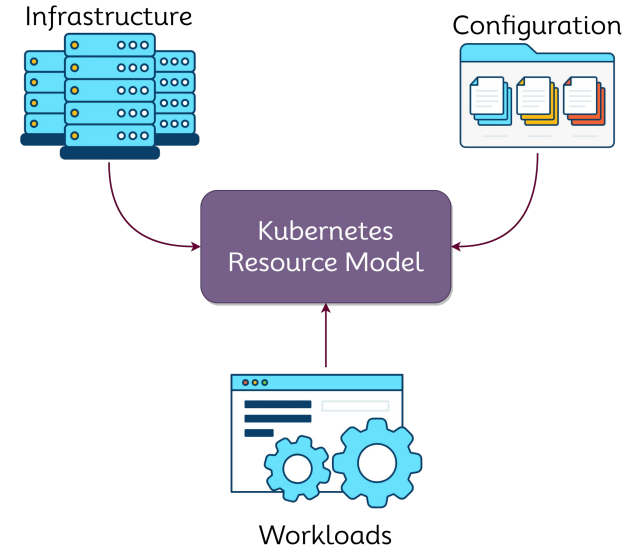


Nephio Security Automation

- Rahul Jadhav, CTO, [AccuKnox](#)

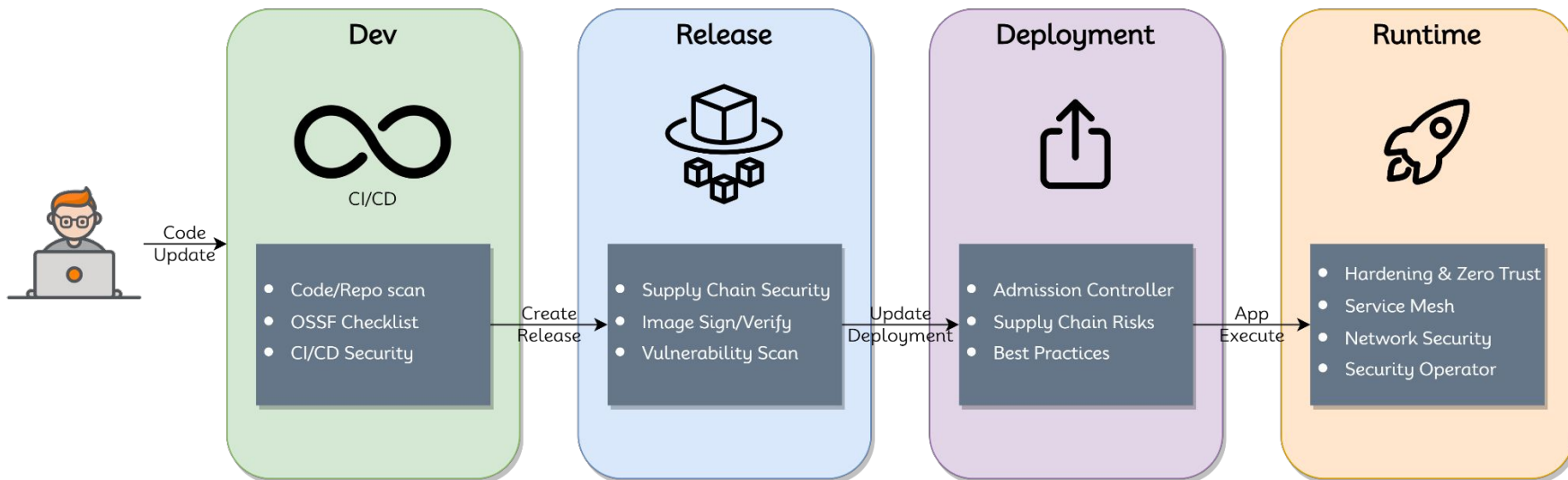


- Single, unified platform for automation
 - K8s & KRM
 - Infra, Workloads, & Configuration
- Declarative config with active reconciliation
 - Configuration as Data (CaD)
- Cooperative management
 - Humans + Machines

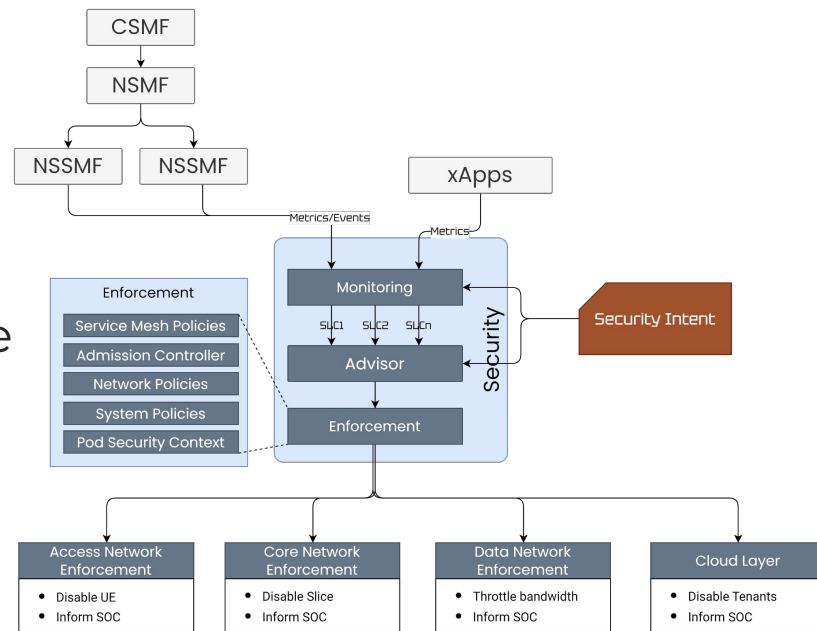


Differentiate: **Secure Telco Automation Framework**

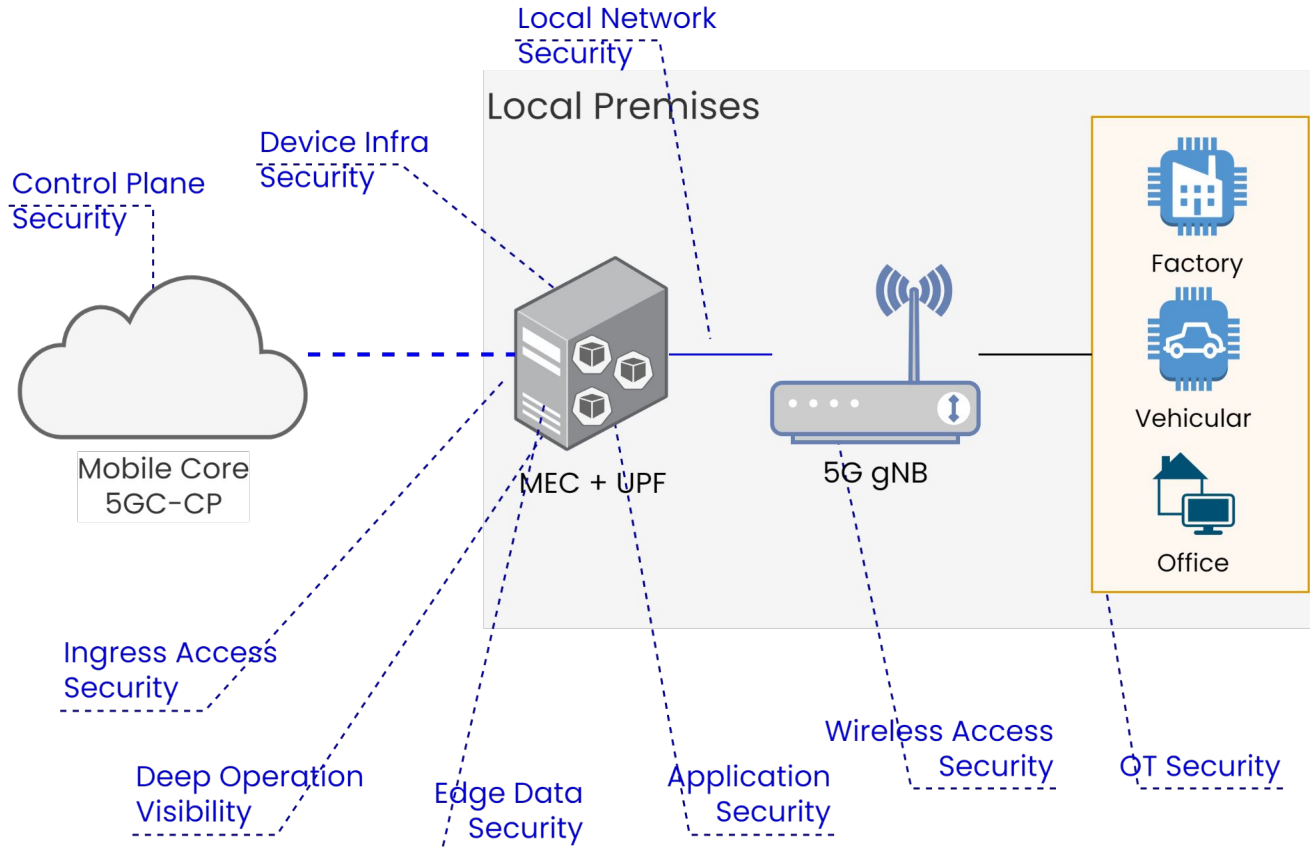
Holistic: Secure all stages
Focus on security intent than on tooling
Zero Trust Enablement
Frictionless Security



- Problem Statement
 - Handling security at scale
 - Tools/Engines heterogeneity
 - Adopt to dynamically changing deployments
- Solution Space
 - Security as intent
 - K8s Operator to manage tooling/policies
- K8s Storage, App deployments have achieved this
 - Doing it at multi-cluster is yet another problem

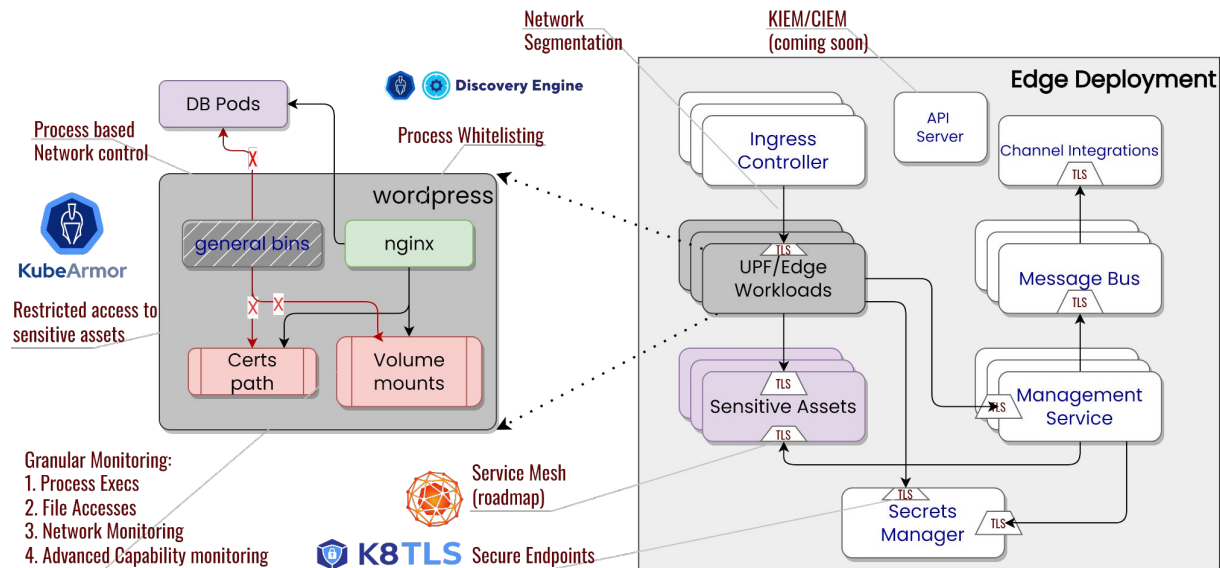
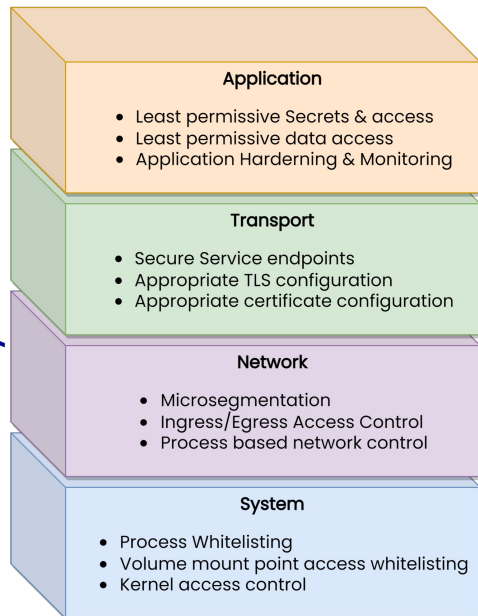


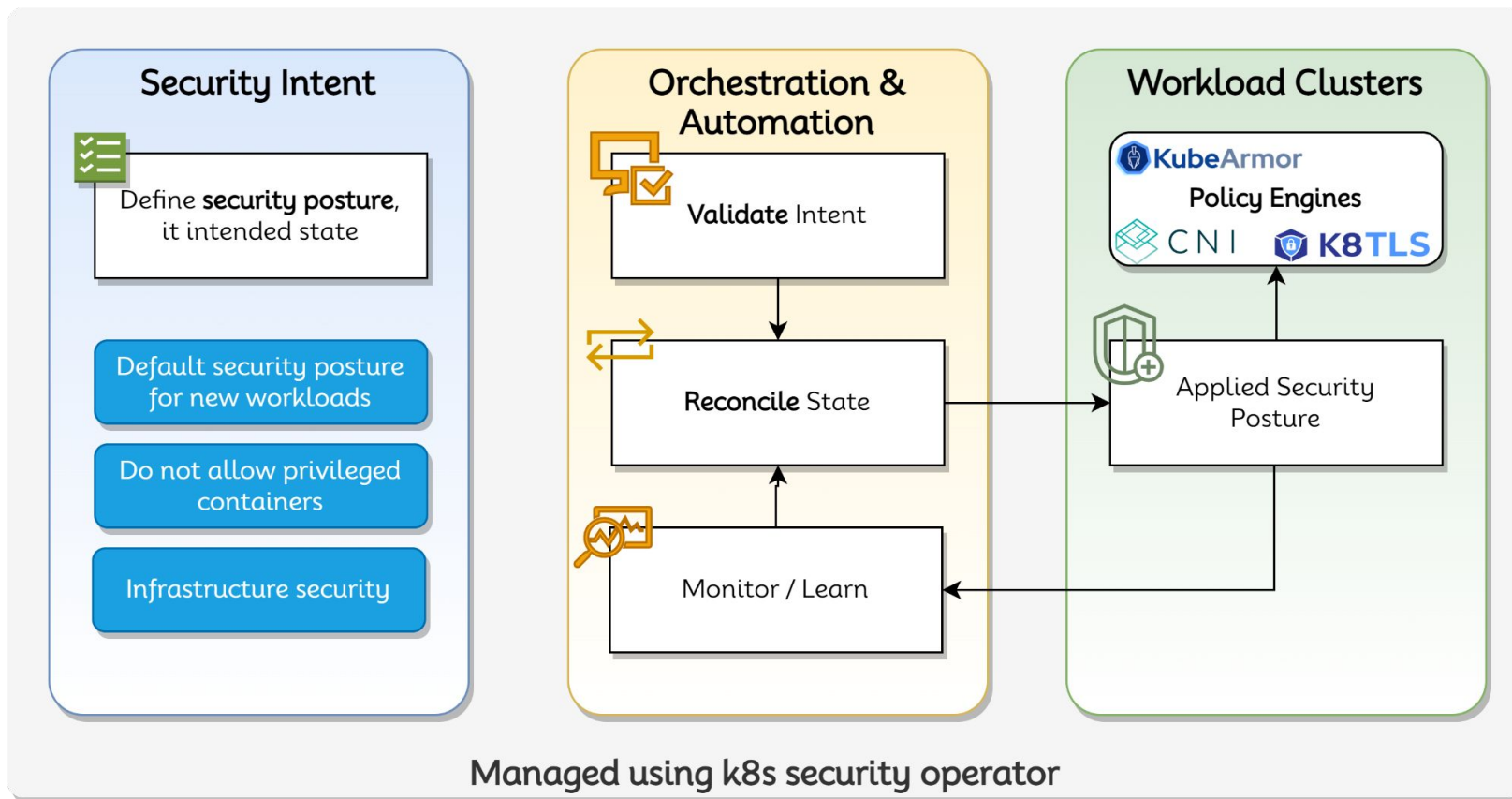
Use-case: Private 5G Security Implications



Zero Trust Enablement

Multi Layer Zero Trust





Our work in 5G open communities

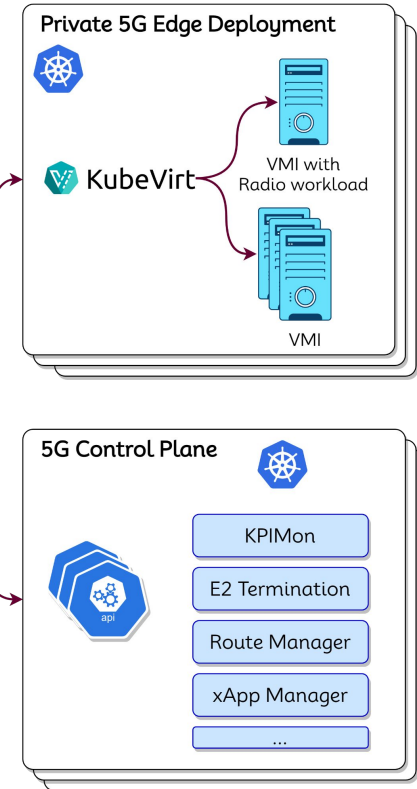
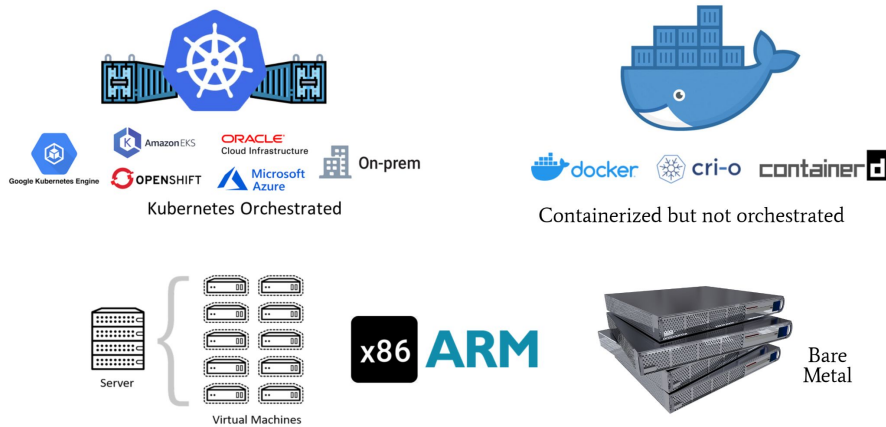
- [LF Nephio TSC member](#)
- [Intel Smart Edge Partner](#)
- [Linux Foundation - Open Horizon](#)
- [Policy Templates](#)
 - ENISA
 - MITRE FiGHT
- [CNCF KubeArmor Project Maintainer](#)
- [5GSec.com:](#)
 - AccuKnox, Stanford Research, Ohio University effort
- [NSF DoD Awards](#)
- RedHat Telco Partner
- [5G-SBP participant](#)
- 5G Open Innovation Labs
- [K8TLS](#) Service Endpoint scanner



- Lightweight sensor for edge deployments
 - **Reduced vcpu** (<50ms) and memory (<100MB) requirements
- Do not assume always on cloud connectivity
 - Policy engines/enforcement should **continue without connectivity**
 - **Sync up** the state when online
- Deployment Models
 - **Virtual Machine** & Containerized deployment support
 - **KubeVirt** support
- 5G Policy Templates
 - **ENISA** support
 - **MITRE FIGHT** support
- Native Integration with edge/5G platforms
 - LF Open Horizon integration as **kubearmor-security operator**
- Scan service endpoints
 - Based on **3GPP TS 33.501** spec
 - Added a new scanning engine **k8tls** (pronounced cattles)

Workload Deployment Models

- Virtual Machine, Bare Metal
- Containerized
- Orchestrated
- **Hybrid is the reality**



- Intent driven security automation with Nephio's core vision
 - Achieves security automation at scale
 - Primitives at play under the hood
 - Native K8s security operator
 - Configuration-as-Data
- Nephio Security SIG discussions in progress ...