Practical approaches to managing and securing cyber-physical systems

Sanjiv Doshi, Principal Engineer - Cisco

Nov 2018

Cisco's take on Cyber-Physical Systems

- Cyber-Physical Systems are fundamentally integration of three components
  - Physical World (OT)
  - Network (IT)
  - Compute (IT)
- Cisco play a big role in IT networking
  - Cyber-physical systems are an extension to IT networks
- We have an important role in compute as well
  - Maybe not at the deep edge, but certainly the next level

IT impact to Cyber-Physical Systems Networking

- Extend the reach of IP to OT
  - Maybe not to the last mile in all theaters but the visibility of CPS systems to IT will be through IP
  - Bucketized to three theaters
    - Extended Enterprise - Warehouse distribution centers
    - Remote and Mobile assets - Public safety fleets, Kiosks
    - Industry Plays - Factories, Utilities, Oil & Gas
- Normalize CPS ecosystem in all theaters across all domains
  - Connectivity
  - Security
  - Compute

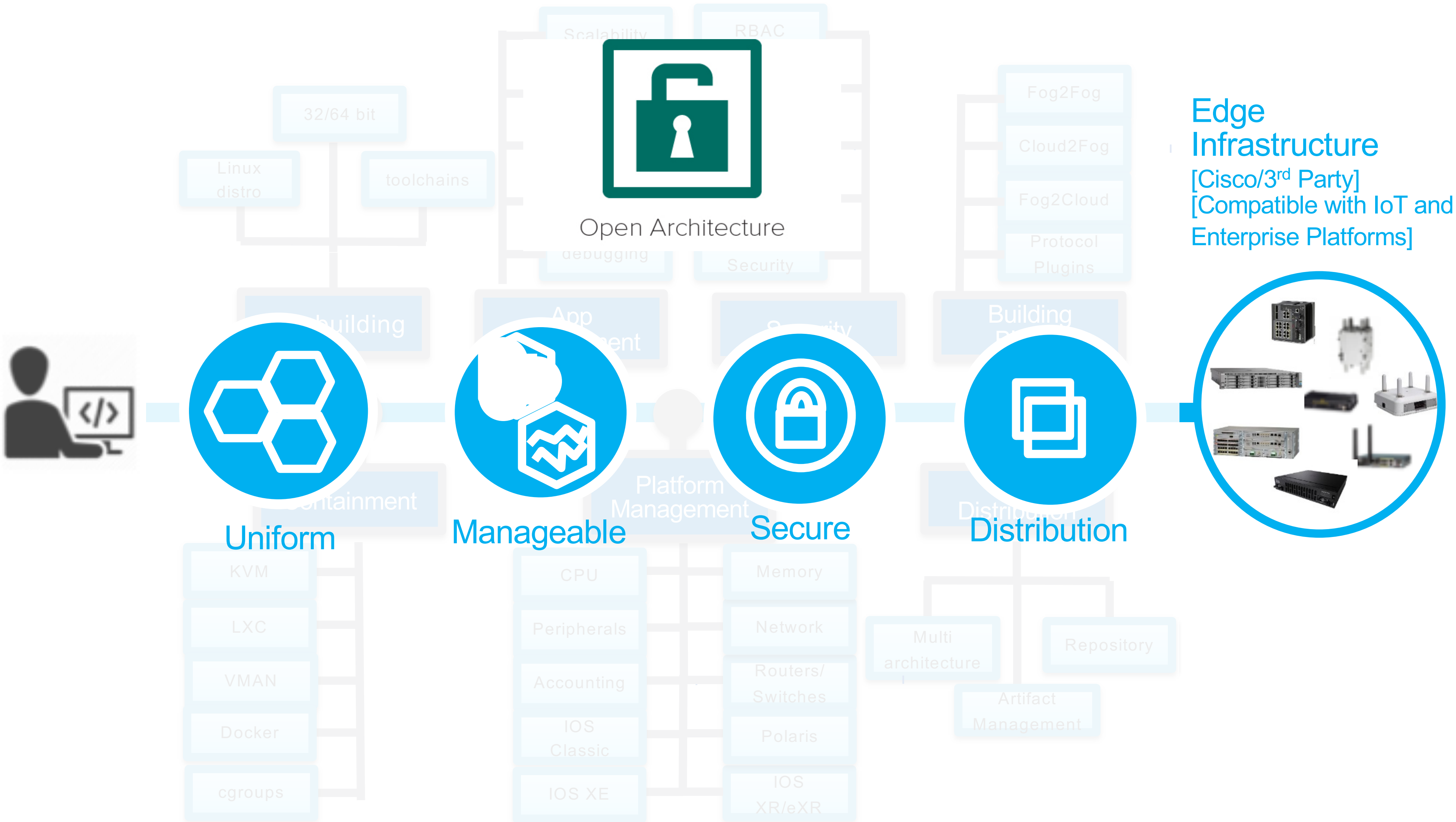
Why Cisco in Edge/FOG computing

- Edge/FOG compute is natural extension to Cisco platforms
  - Campus and IoT implementations need networks first
    - “Cloud/DC” computing is a result of compute coming to “data-at-rest”
      - “Edge” computing is compute coming to “data-in-motion”
        - Reminds me of Sun Microsystems tagline ”Network is the computer”
    - General purpose compute and enterprise class storage elements are siloed in data centers
    - Only distributed hardware platforms today are network elements in IT
      - They already have compute, memory and storage
      - No need to truck roll and separately manage a compute infrastructure
      - All this w/o compromising the core functionality i.e. deliver secure and stable networks
- Just as in real estate – it is “location, location, location”

IOx Value Proposition

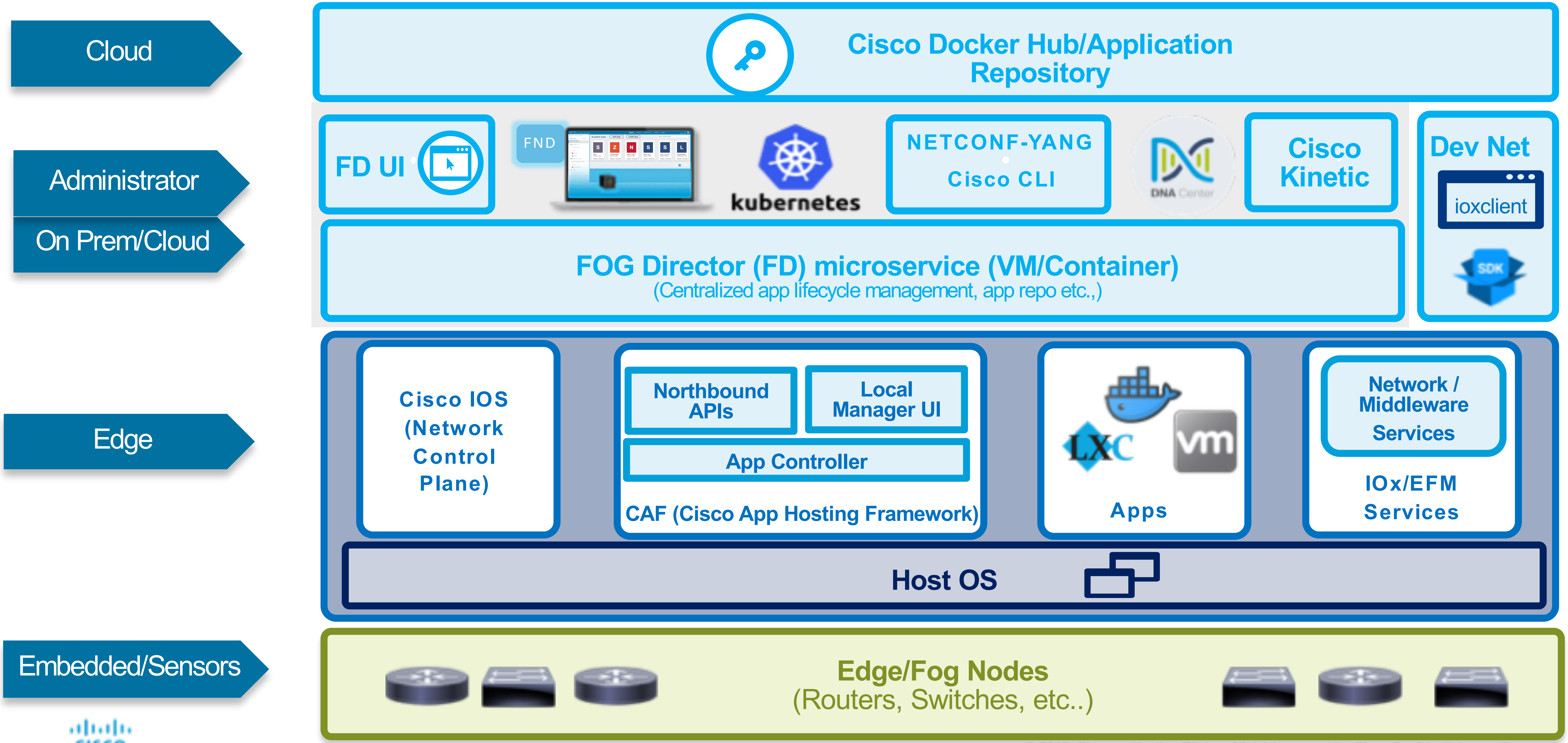
Fog Requirements

App Development
App Hosting
Management
Security
Distribution/Control
Fog Services



Edge Infrastructure
[Cisco/3rd Party]
[Compatible with IoT and Enterprise Platforms]

IOx Architecture Overview



Cloud

Cisco Docker Hub/Application Repository

Administrator

On Prem/Cloud

FD UI

FND

kubernetes

NETCONF-YANG

Cisco CLI

DNA Center

Cisco Kinetic

Dev Net

ioxclient

SDK

FOG Director (FD) microservice (VM/Container)

(Centralized app lifecycle management, app repo etc.,)

Edge

Cisco IOS (Network Control Plane)

Northbound APIs

Local Manager UI

App Controller

CAF (Cisco App Hosting Framework)

LXC

vm

Apps

Network / Middleware Services

IOx/EFM Services

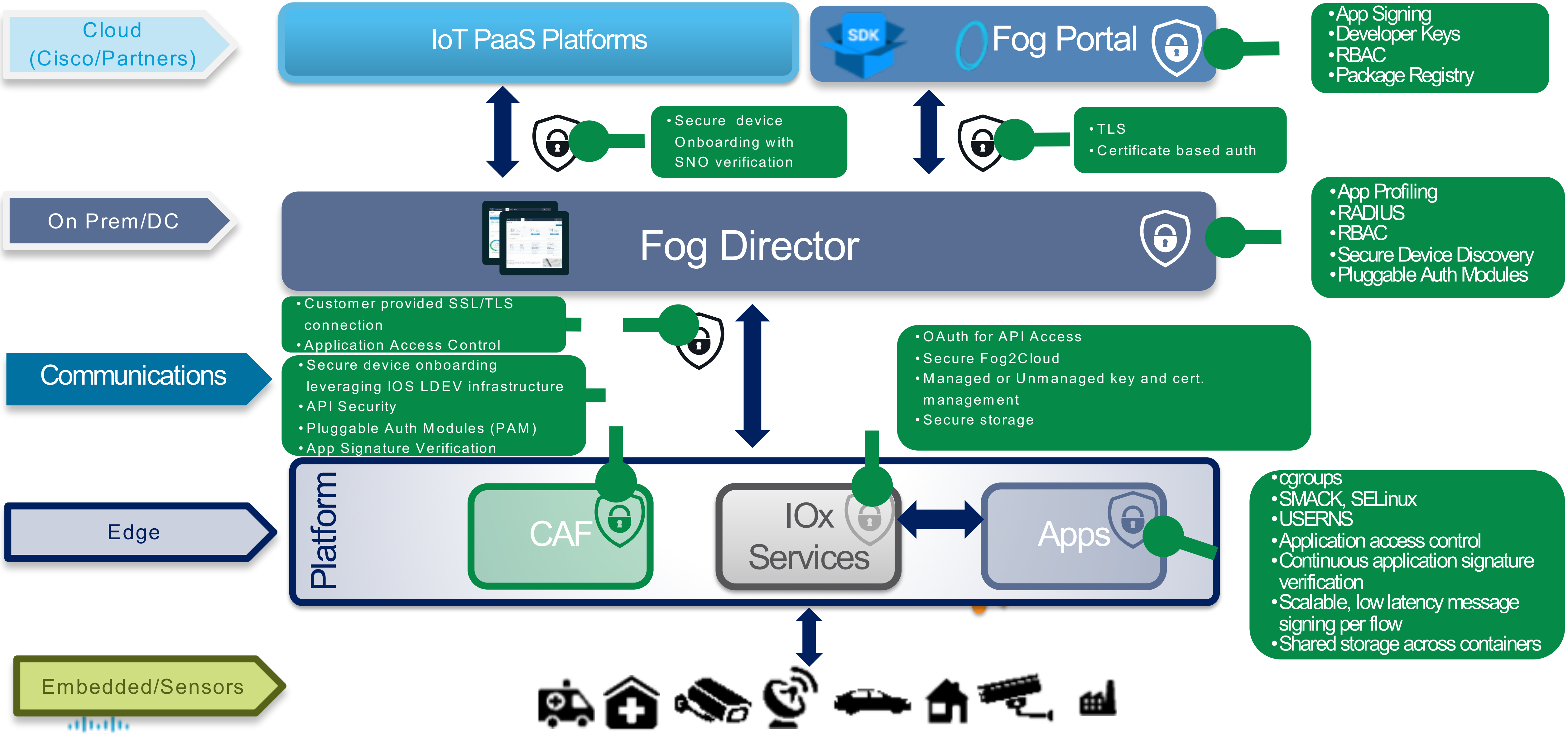
Host OS

Embedded/Sensors

Edge/Fog Nodes

(Routers, Switches, etc..)

Comprehensive Platform Security



Cloud (Cisco/Partners)

IoT PaaS Platforms

SDK Fog Portal

- App Signing
- Developer Keys
- RBAC
- Package Registry

- Secure device Onboarding with SNO verification

- TLS
- Certificate based auth

On Prem/DC

Fog Director

- App Profiling
- RADIUS
- RBAC
- Secure Device Discovery
- Pluggable Auth Modules

Communications

- Customer provided SSL/TLS connection
- Application Access Control

- Secure device onboarding leveraging IOS LDEV infrastructure
- API Security
- Pluggable Auth Modules (PAM)
- App Signature Verification

- OAuth for API Access
- Secure Fog2Cloud
- Managed or Unmanaged key and cert. management
- Secure storage

Edge

Platform

CAF

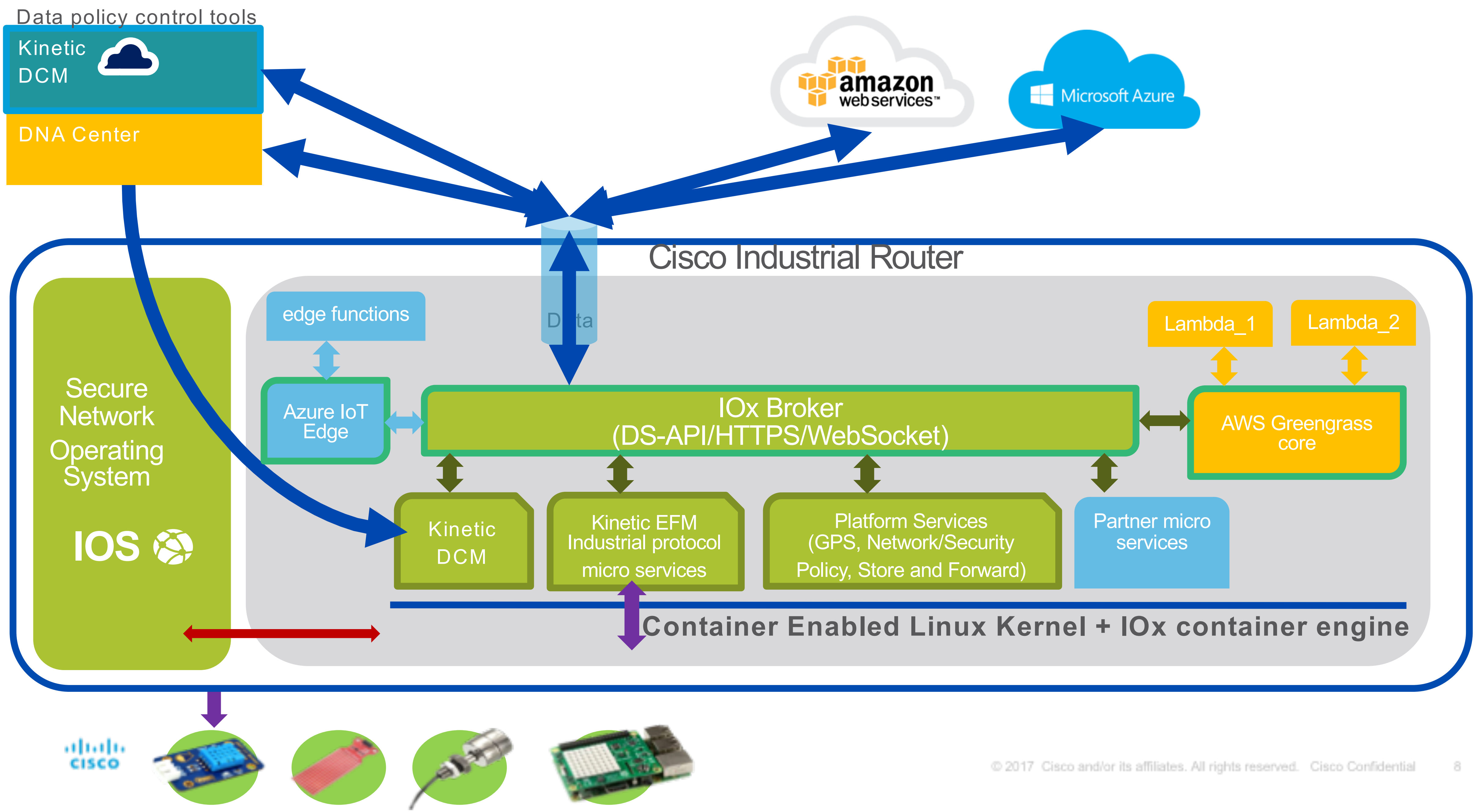
IOx Services

Apps

- cgroups
- SMACK, SELinux
- USERNS
- Application access control
- Continuous application signature verification
- Scalable, low latency message signing per flow
- Shared storage across containers

Embedded/Sensors

Cisco Multi-cloud micro-service centric platform architecture

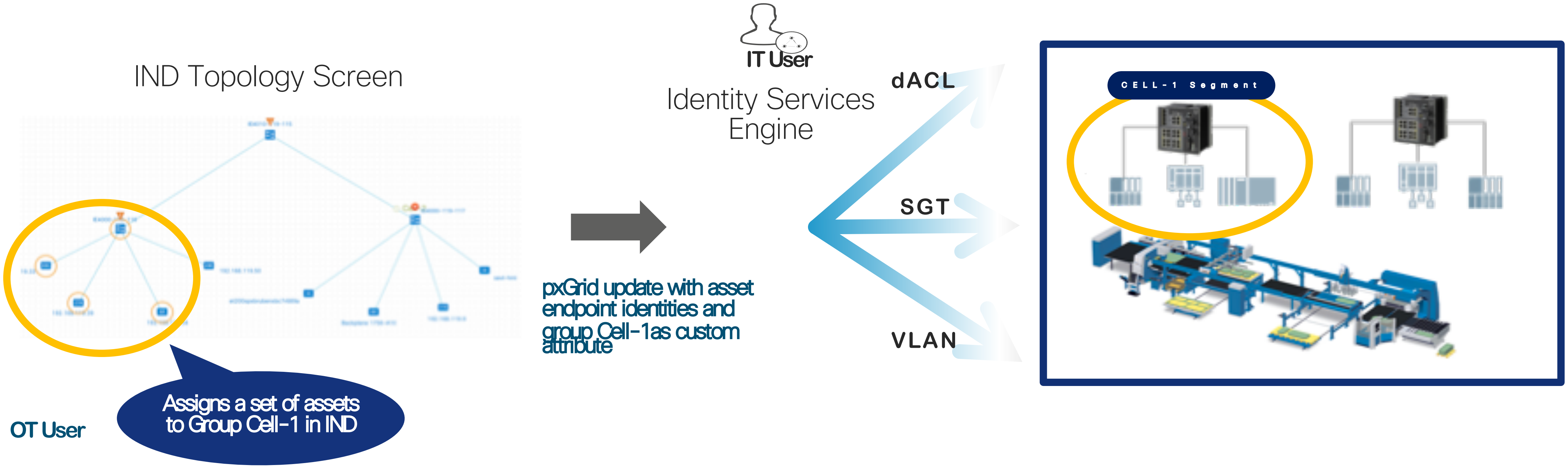

Data policy control tools
Kinetic DCM
DNA Center
amazon web services
Microsoft Azure
Cisco Industrial Router
Data
edge functions
Azure IoT Edge
IOx Broker (DS-API/HTTPS/WebSocket)
Lambda_1
Lambda_2
AWS Greengrass core
Secure Network Operating System
IOS
Kinetic DCM
Kinetic EFM Industrial protocol micro services
Platform Services (GPS, Network/Security Policy, Store and Forward)
Partner micro services
Container Enabled Linux Kernel + IOx container engine

Use Cases

- Network Element Monitoring
  - I.e. Self-monitoring
- Network Management Services
  - Day 0, 1, 2 configurations
  - Optimize Netflow, SNMP MIBS records
- Security
  - Traffic Monitoring
  - Deception Technology (device emulation)
  - Security Policies
  - Firewall
  - IDS/IPS
  - Micro-segmentation
  - DDoS mitigation

- Edge Processing
  - Complex Event Processing (CEP)/ML
    - Preventative Maintenance
    - Bandwidth optimization
  - Cost optimization
    - Network selection based on signal strength, geographic location
- Network Services
  - DHCP
  - Print
- Light Weight Custom Apps
  - Time Sharing
  - Asset Monitoring

Network Segmentation



IND Topology Screen

OT User

Assigns a set of assets to Group Cell-1 in IND

pxGrid update with asset endpoint identities and group Cell-1as custom attribute

IT User

Identity Services Engine

dACL

SGT

VLAN

- Default Auth policy on ISE for switchport is configured as “open access” – i.e no NAC blocking
- PxGrid attribute “**Cell-1**” matches a Profiling policy on ISE and triggers corresponding Authorization policy
- ISE Authorization policy can be used to dynamically apply dACL, SGT or VLAN to switchports to segment the assets
- OT user and IT user are working with asset identities rather than IP addresses

MUD- Key Questions to Ask

What is this thing?

Who is responsible for it?

How do I protect it and my business?

Is it doing what it should be doing?

Manufacturers Usage Description

- MUD: IETF Standard: draft-ietf-opsawg-mud-22 *standards track*
- *The goal of MUD is to provide a means for end devices to signal to the network what sort of access and network functionality they require to properly function. The initial focus is on access control. Later work can delve into other aspects.*

https://tools.ietf.org/id/draft-ietf-opsawg-mud-22.html cisco