Mission Critical OT Network Best Practices

Using Private-5G Wireless Services

Derick Linegar - Technical Solutions Architect

BRKSPM-3581

Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

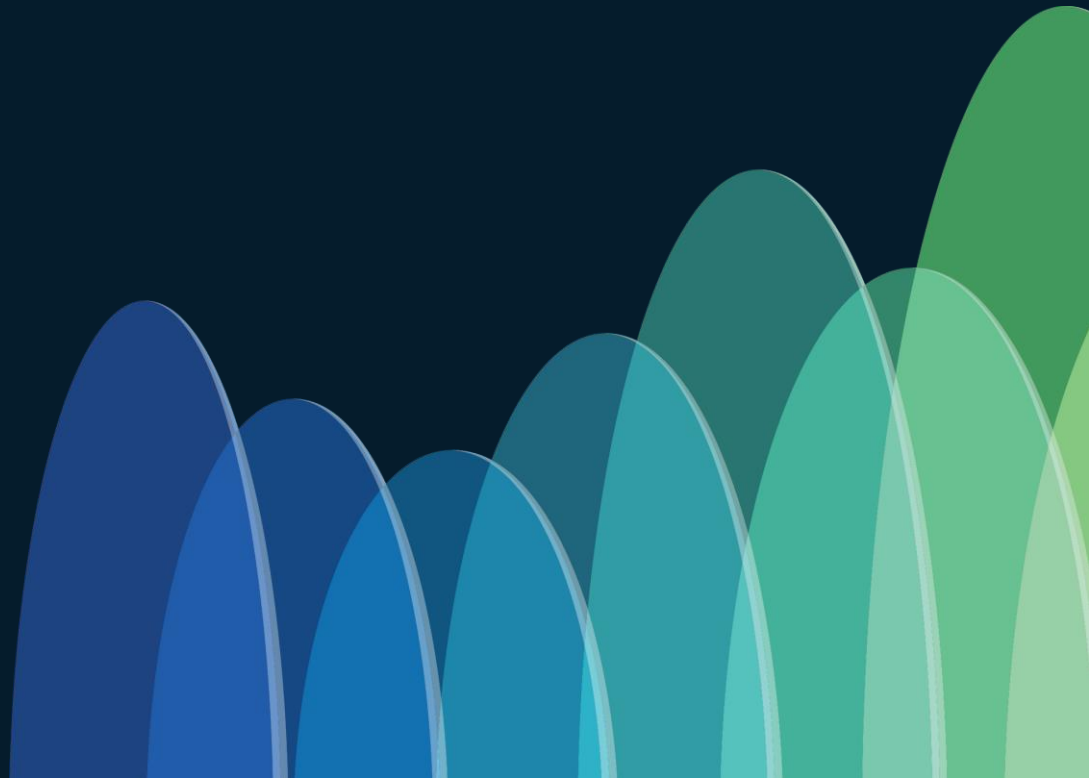
1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

Agenda

- OT Industry & Networking Review
- OT Demanded Security Approach
- Cisco P5GaaS Architecture and Security Deep-Dive
- Cisco P5G Integration & applicability for OT
- Deployment of OT Wireless using P5G as-a-Service
- Conclusion

OT Industry & Networking



cisco Live!

Critical Infrastructure Providers

Applicable to many Verticals...

Industry / Manufacturing

- Non-Stop Operation
- Flexible Layout Change
- Deterministic Control
- Security

Utility

- Long distance connection
- Harsh environment
- 4G Backhaul
- 4G/5G Private Wireless

Transportation/Public Safety

- Incident Response
- Traffic/Signal Monitoring
- Passenger WiFi
- Physical Security
- Video Surveillance

Oil & Gas

- Pipeline Monitoring
- Long distance operation
- Extreme weather
- 3G/4G Backhaul

Municipality

- Intelligent Traffic System
- Surveillance
- City-wide WiFi
- Lighting/Energy Mgmt

Extending Intelligence to Operational Networks (OT)

Ruggedized | Security | High Availability | FOG & FAN

Industry / Manufacturing: Discrete or Process?

Impact on Networking & Security

Discrete Manufacturing	Process Manufacturing
• Products are comprised of components that can be touched and counted.	• Products are manufactured using formulas or recipes
• Parts can be broken down & disposed of or recycled after production	• Products cannot be broken down back into raw materials
• Uses Bills-of-Material	• Uses formulas or recipes
• Assembles in a linear or routing way	• Blends in a batch
• Involves joining, attaching, fixing, assembling etc.	• Involves grinding, boiling, mixing, churning, etc.
• Doesn't involves change of volume or density	• Volume, density, mass, physical properties all get changed here

Type of Manufacturing Dictates Architecture etc...

Source: info@from-sensor-to-data.com

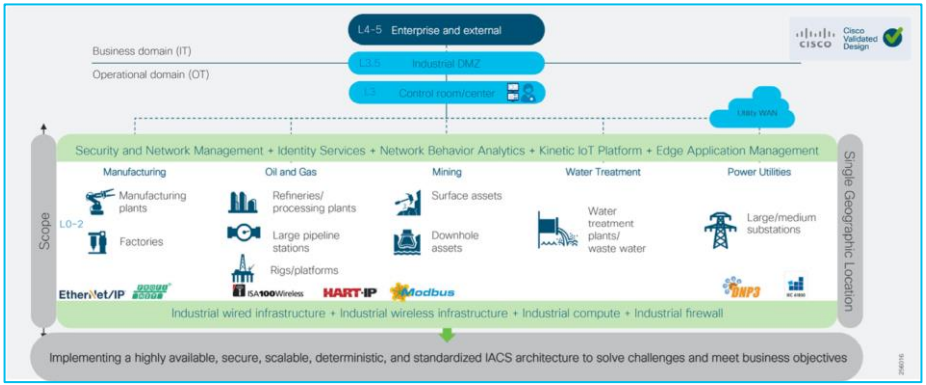
Note: Control loop timing is very different in these examples

Both process and discrete are often used together.. Consider Food production

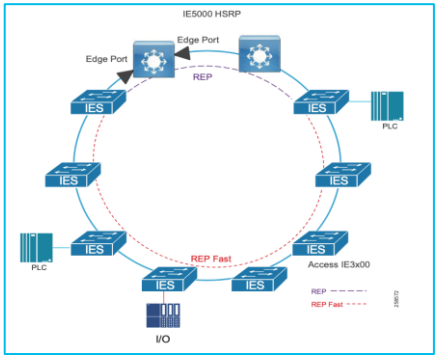
Cisco Validated Designs: OT Network & Architectures

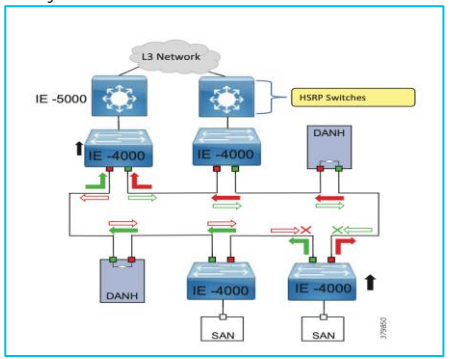
Aim to add Private Wireless…

Vertical Coverage:

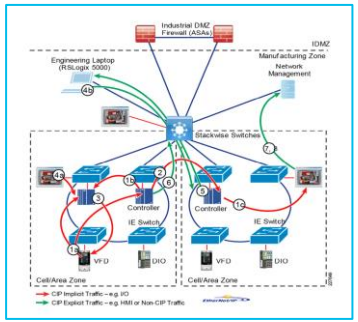


Resiliency:

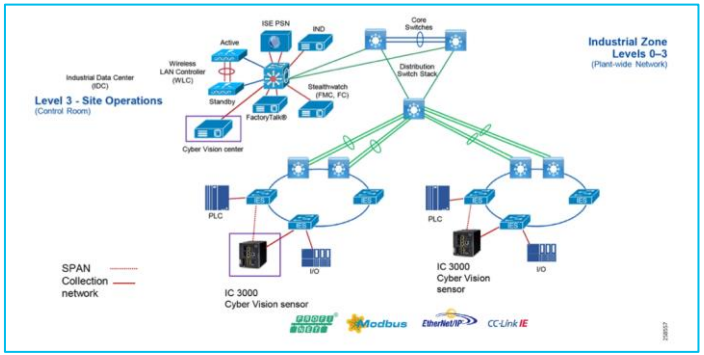




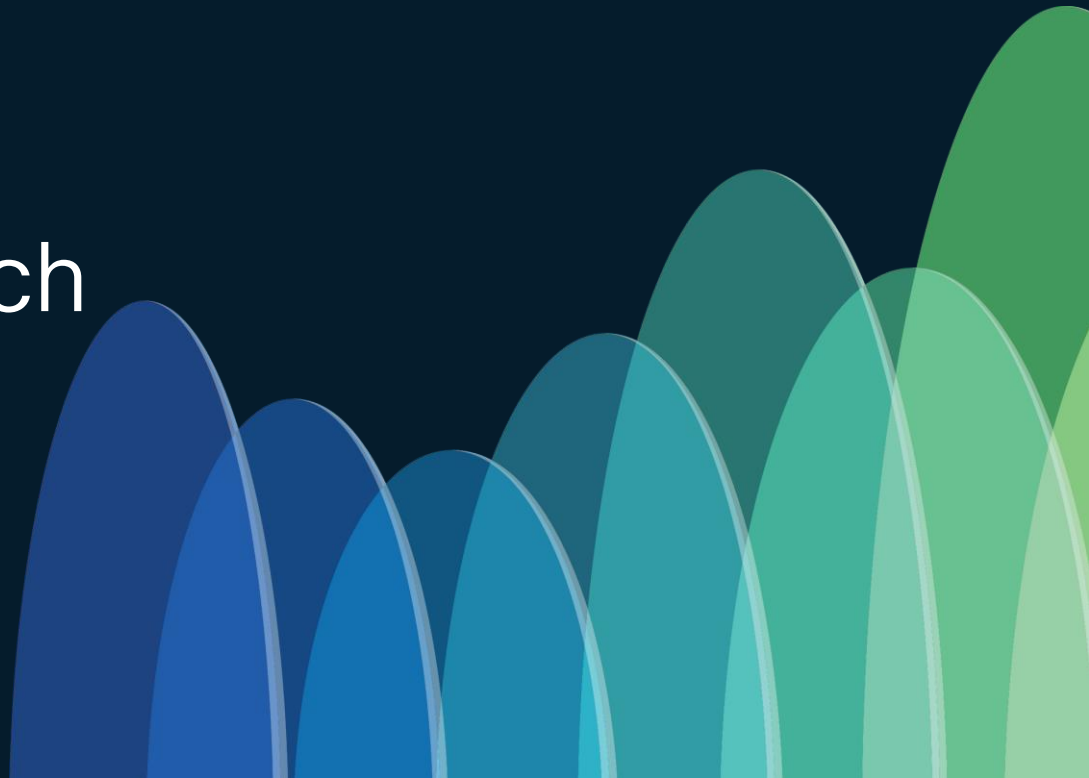
Topology and QoS:



Security:



OT Demanded Security Approach



cisco Live!

OT Operational Domain Security Challenges

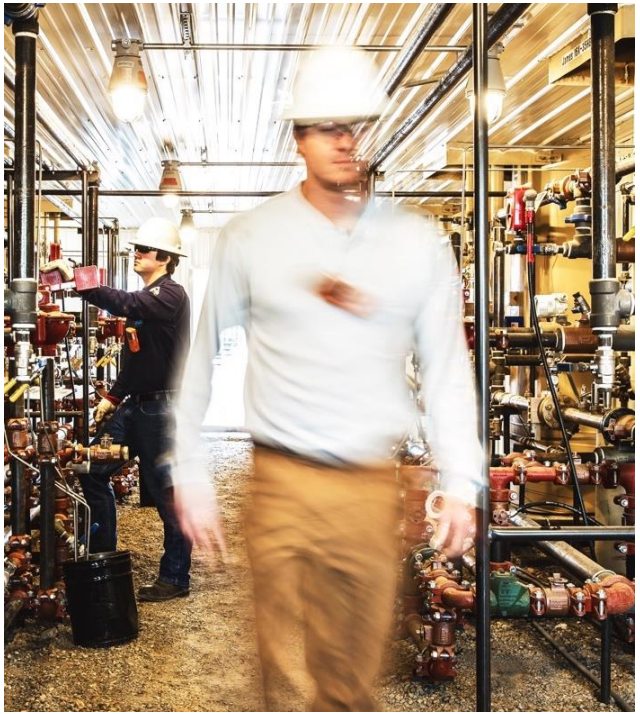
Necessitates a Security Focused Design

- Fragile TCP/IP Stacks – NMAP, Ping Sweep lockup
- Little or no device level authentication
- Poor network design – daisy chains, hubs
- Windows based IA servers – patching, legacy OS
- Unnecessary services running – FTP, HTTP
- Open environment, no port security, no physical security of switch, Ethernet ports
- Limited auditing and monitoring of access to IA devices
- Unauthorized use of HMI, IA systems for browsing, music/movie downloads
- Lack of IT expertise in IA networks, many blind spots

The ‘OT Security’ Exam Question

‘We need to converge our IT and OT networks, where do we start with securing our Operational Network?’

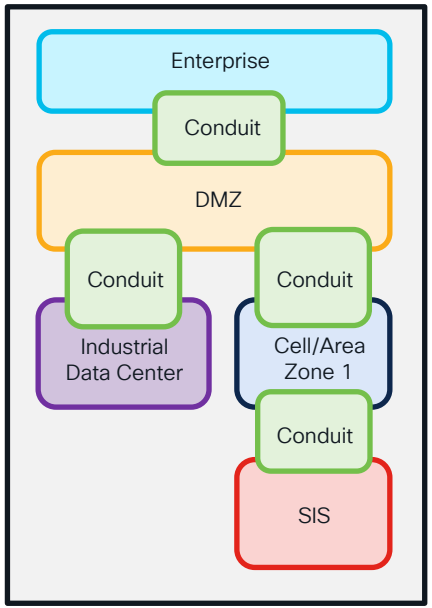
- Primary Drivers
  - Business demanding visibility from OT plant for efficiency and flexibility gains
  - Historically ‘air gapped’ systems are now more connected – exposing many new risks to the revenue earning parts of the business
  - Systems are in place for potentially multiple decades exposing a large and weak attack surface
    - Vulnerabilities across plant and aging control systems (Windows 7 and potentially older)
- And now ..
  - New EU Legislation in the form of NIS2 will mandate organizations clean up cyber hygiene or be fine. This now impacts an expanded set of customers – compliance by 2024 required – this includes supply chain



Segmentation is the key to protect OT assets

Use NIST and ISA/IEC 62443 Guidelines

ISA/IEC 62443



NIST Zero Trust Guidance

3.1.2 ZTA Using Micro-Segmentation

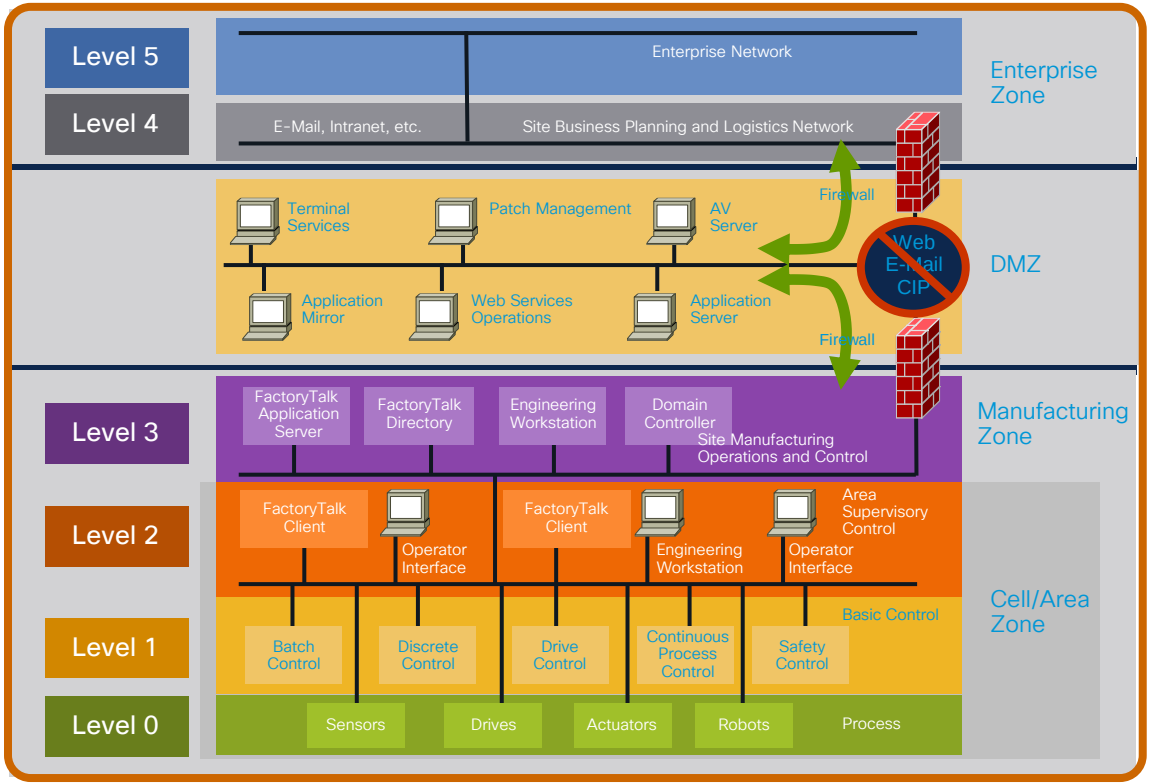
An enterprise may choose to implement a ZTA based on placing individual or groups of resources on a unique network segment protected by a gateway security component. In this approach, the enterprise places infrastructure devices such as intelligent switches (or routers) or next generation firewalls (NGFWs) or special purpose gateway devices to act as PEPs protecting each resource or small group of related resources. Alternatively (or additionally), the enterprise may choose to implement host-based micro-segmentation using software agents (see Section 3.2.1) or firewalls on the endpoint asset(s), These gateway devices dynamically grant access to individual requests from a client, asset or service. Depending on the model, the gateway may be the sole PEP component or part of a multipart PEP consisting of the gateway and client-side agent (see Section 3.2.1).

This approach applies to a variety of use cases and deployment models as the protecting device acts as the PEP, with management of said devices acting as the PE/PA component. This approach requires an identity governance program (IGP) to fully function but relies on the gateway components to act as the PEP that shields resources from unauthorized access and/or discovery.

The key necessity to this approach is that the PEP components are managed and should be able to react and reconfigure as needed to respond to threats or change in the workflow. It is possible to implement some features of a micro-segmented enterprise by using less advanced gateway devices and even stateless firewalls, but the administration cost and difficulty to quickly adapt to changes make this a very poor choice.

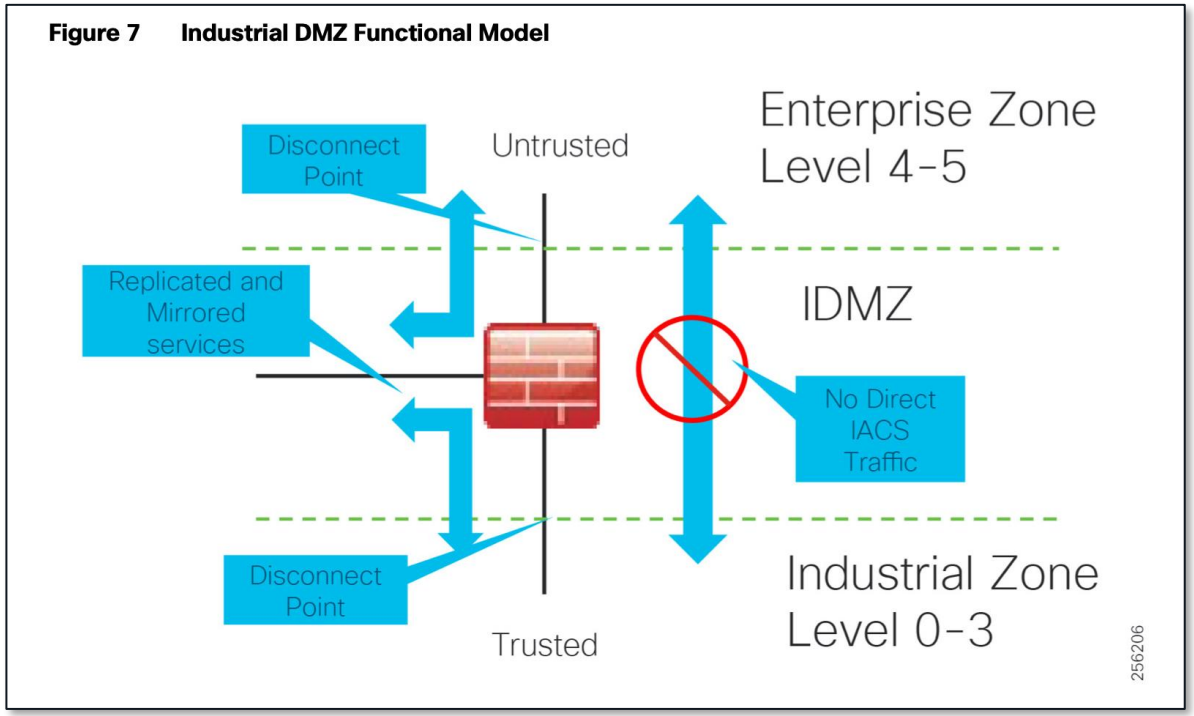
Industry Standards to the Rescue:

ISA 99 – IEC 62443 approach – level 3.5 IDMZ

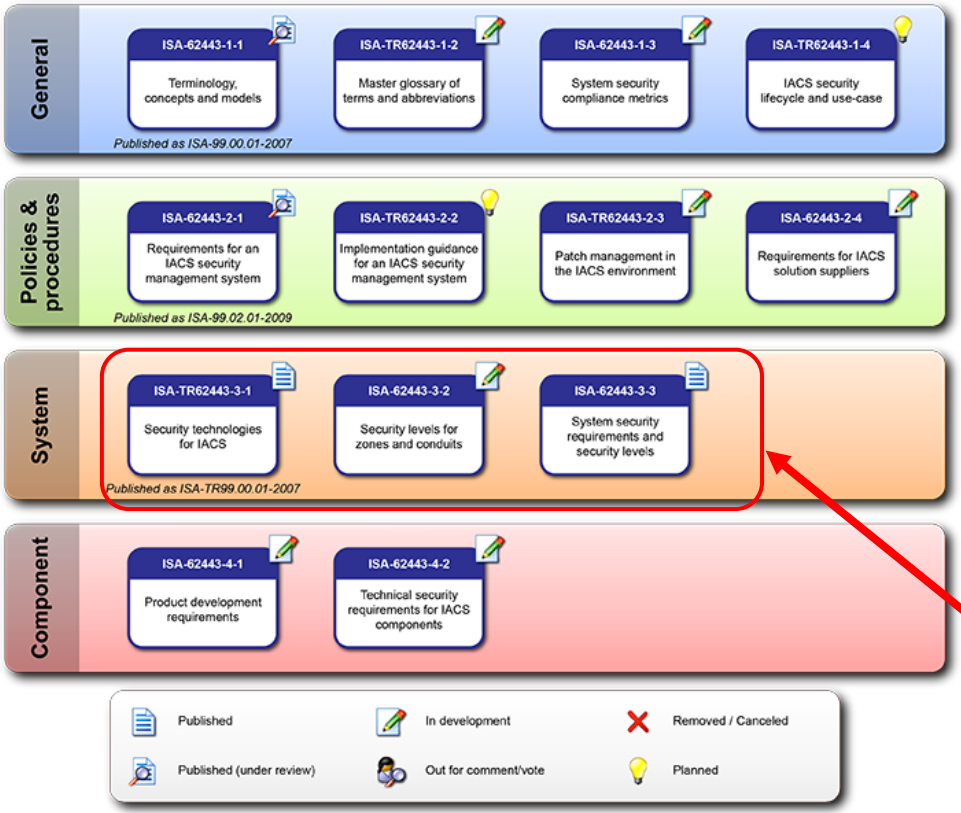


Industry Standards to the Rescue:

ISA 99 – IEC 62443 approach – level 3.5 IDMZ



ISA 62443-Security Blueprint for OT Networks



It is a range of security standards for IACS

The purpose of the ISA99 committee is to develop and establish standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure industrial automation and control systems and security practices and assessing electronic security performance.

Areas of architectural relevance

Cisco CVD are aligned from a security perspective

Example: Key Standards for Oil & Gas Security

Mandated by Customer defined regulatory framework

- ISA95 / Purdue Model of Control
- ISA99 / IEC 62443
- NIST Cybersecurity Framework
- NERC-CIP
- Industry specific eg. *American Petroleum Institute API Standard 1164* for SCADA security

Functions	*Categories*
IDENTIFY (ID)	Asset Mangement (AM)
	Business Environment (BE)
	Governenace (GV)
	Risk Assessment (RA)
	Risk Management Stategy (RM)
PROTECT (PR)	Access Control (AC)
	Awareness and Training (AT)
	Data Security (DS)
	Information Protection Processess and Procedures (IP)
	Maintenance (MA)
	Protective Technology (PT)
DETECT (DE)	Anomolies and Events (AE)
	Security Continuos Monitoring (CM)
	Detection Processes (DP)
RESPOND (RS)	Incident Response Planning (RP)
	Communications (CO)
	Analysis (AN)
	Mitigation (MI)
	Improvements (IM)
RECOVER (RC)	Recovery Planning (RP)
	Improvements/Gap Remediation (IM)
	Communications (CO)

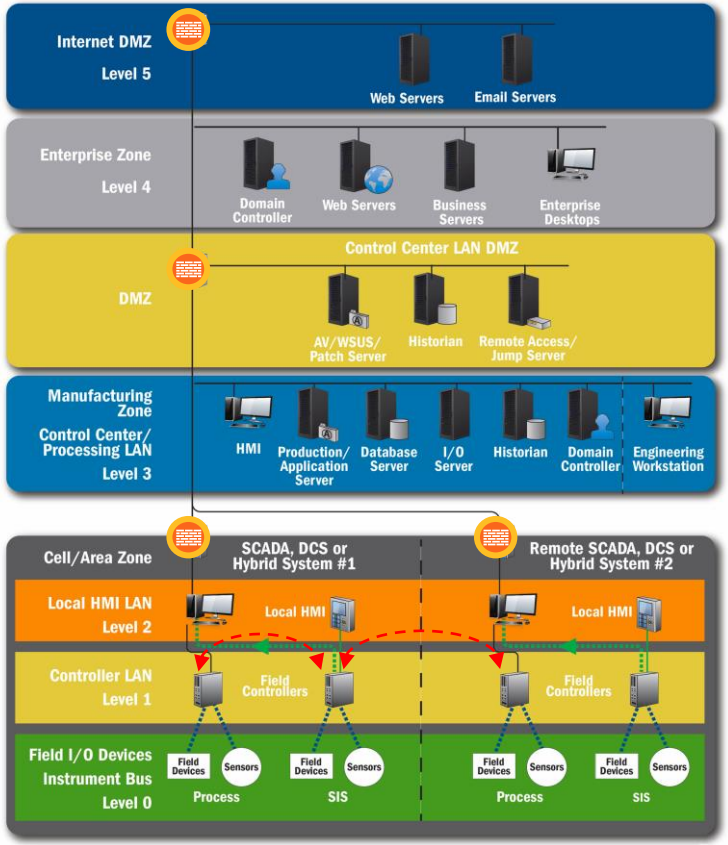
Callout: Purdue Model:

ISA95 Reference Hierarchy

Architecture of enterprise networks with industrial control systems

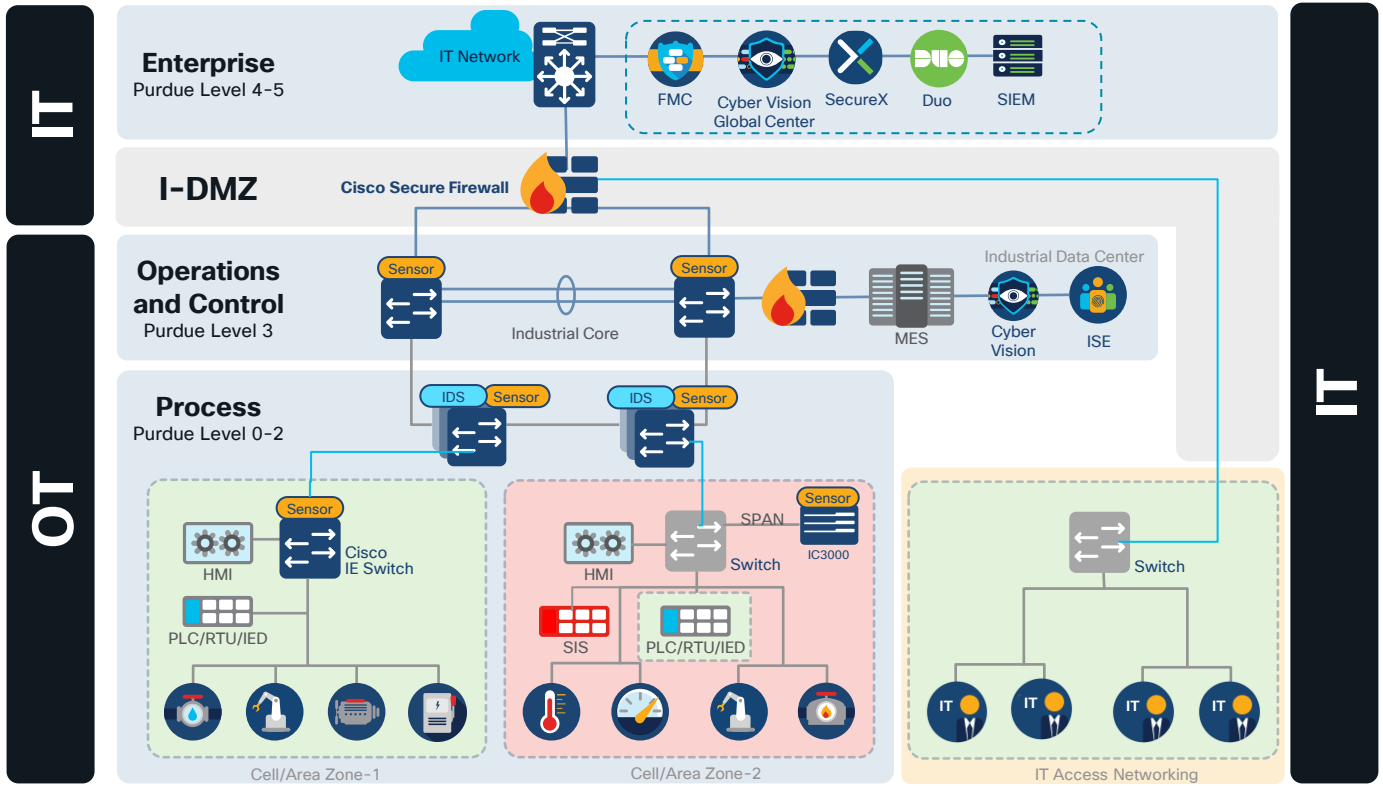
- Level 0 is the closest to the industrial process, Levels 4 and 5 are the closest to the IT network

- IT /OT convergence:
  - The requirement to ‘actively’ join Purdue levels 3 and below to the Enterprise internally and potentially externally (Cloud, IoT, etc)



Source: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95

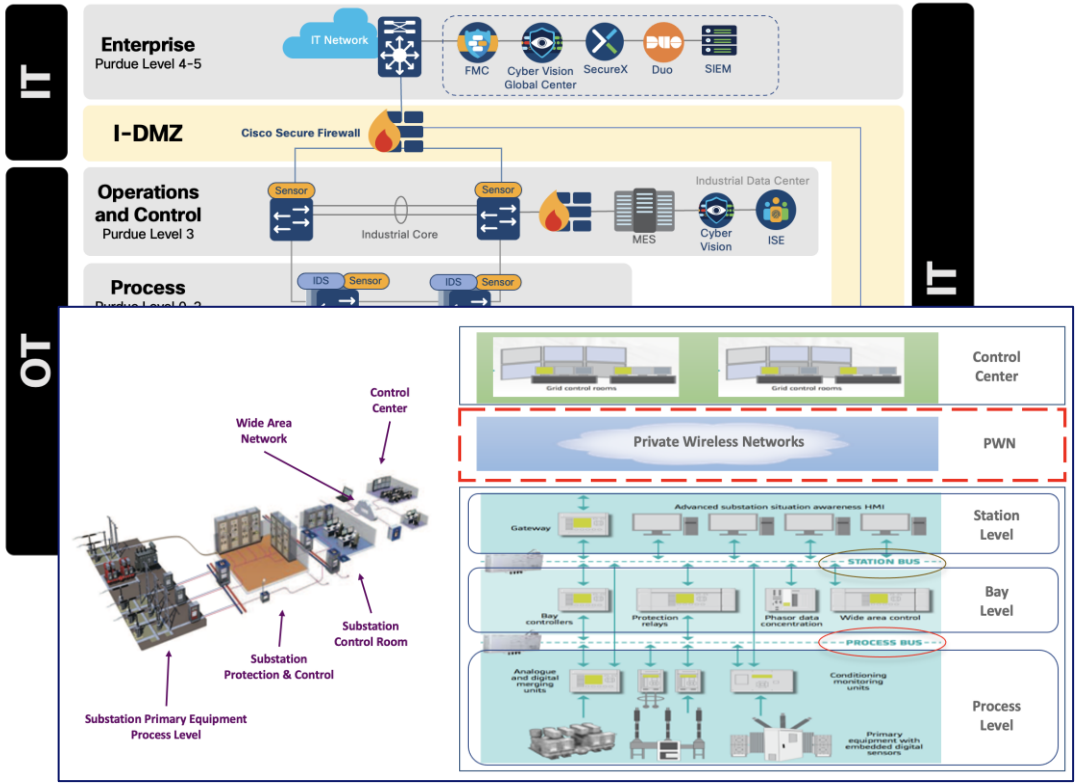
Callout: Typical PLC Networking Requirements



- Networking for IT/OT tends to drive toward a converged approach.
- OT networks are still handled separately due to more recent ISA 62443-Security requirements.
- The approach is to have clearly defined entry/exits per Purdue Level definitions, with security enhancements for improved security posture assessment and validation (Cybervision, ISE etc)

Source: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95

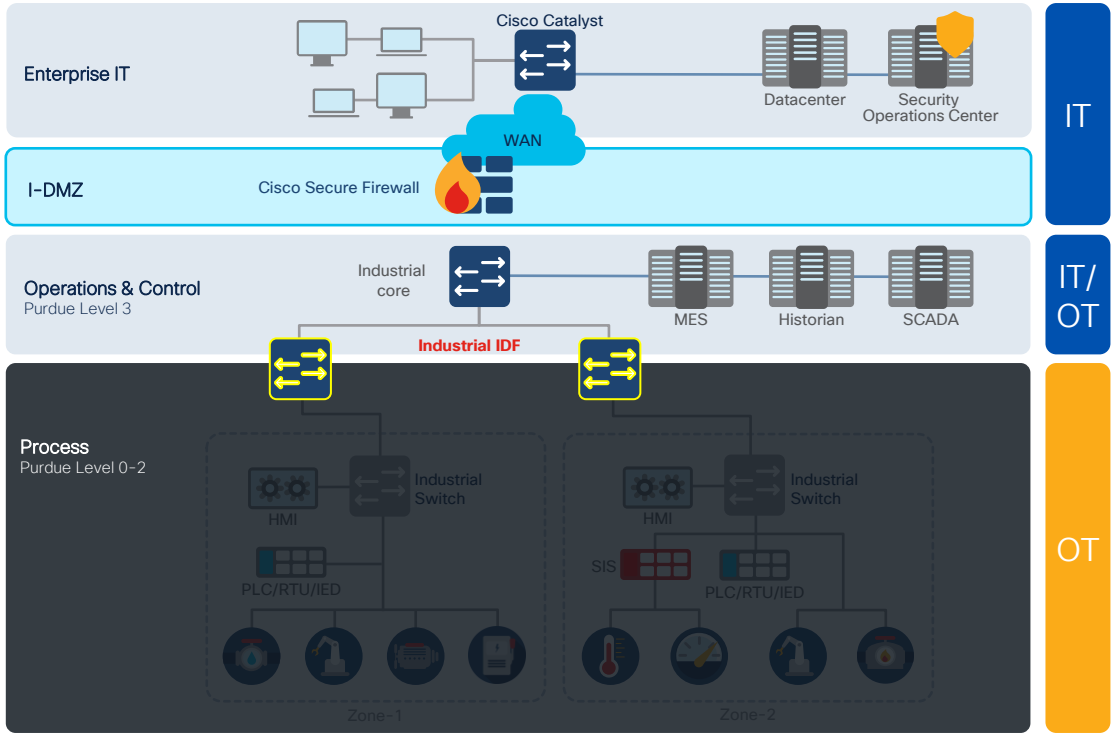
Callout: Critical Infrastructure: IS95/Purdue OT
Networking Architecture



- Critical Infrastructure Networking for IT/OT tends to drive toward a converged approach.
- Hybrid based Multi-Access (wired, licensed/unlicensed wireless) is the de-facto approach to address divergent requirements.

- OT networks are still handled separately due to ISA 95 / Purdue Architecture and more recent ISA 62443 -Security requirements:
  - Level 0 is the closest to the industrial process, Levels 4 and 5 are the closest to the IT network
- The approach is to have clearly defined entry/exits per Purdue Level definitions, with security enhancements for improved security posture assessment and validation (Cisco Cybervision, Splunk, Cisco ISE etc)
- For Utilities, specific requirements such as IEC 61850 Substation Networking Requirements is required.

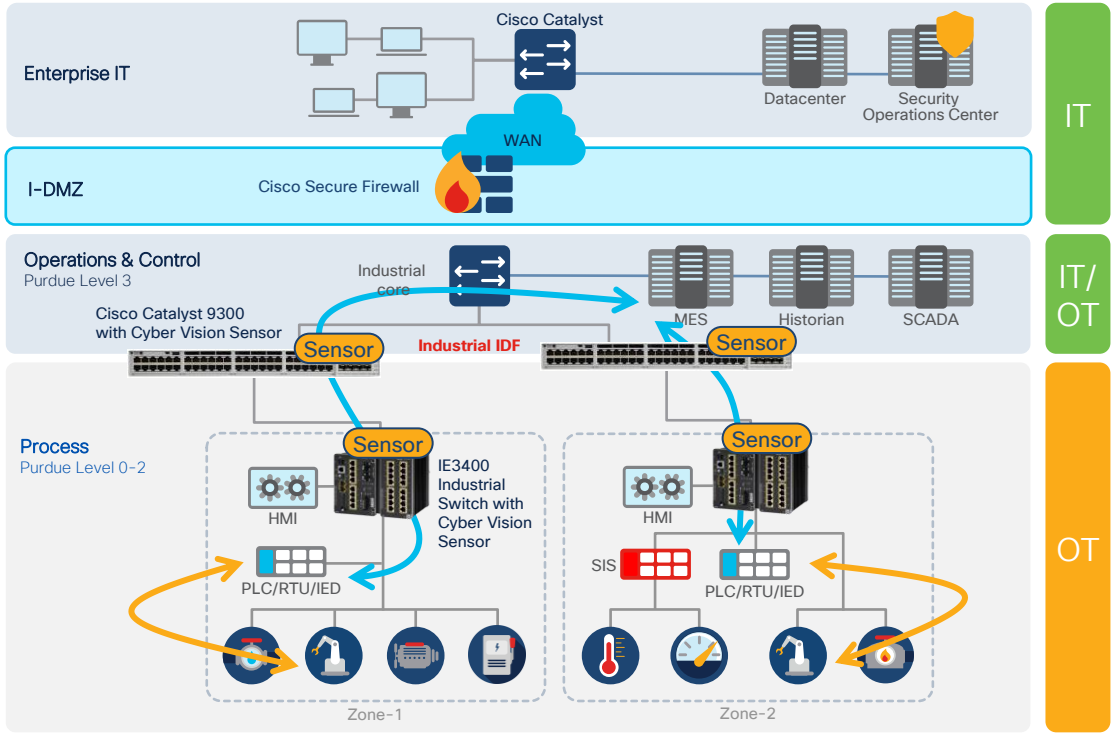
IT has no visibility below the Industrial IDF



How can IT leverage network equipment it owns to gain visibility into OT?

Source: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95

Gain full visibility to improve your security posture



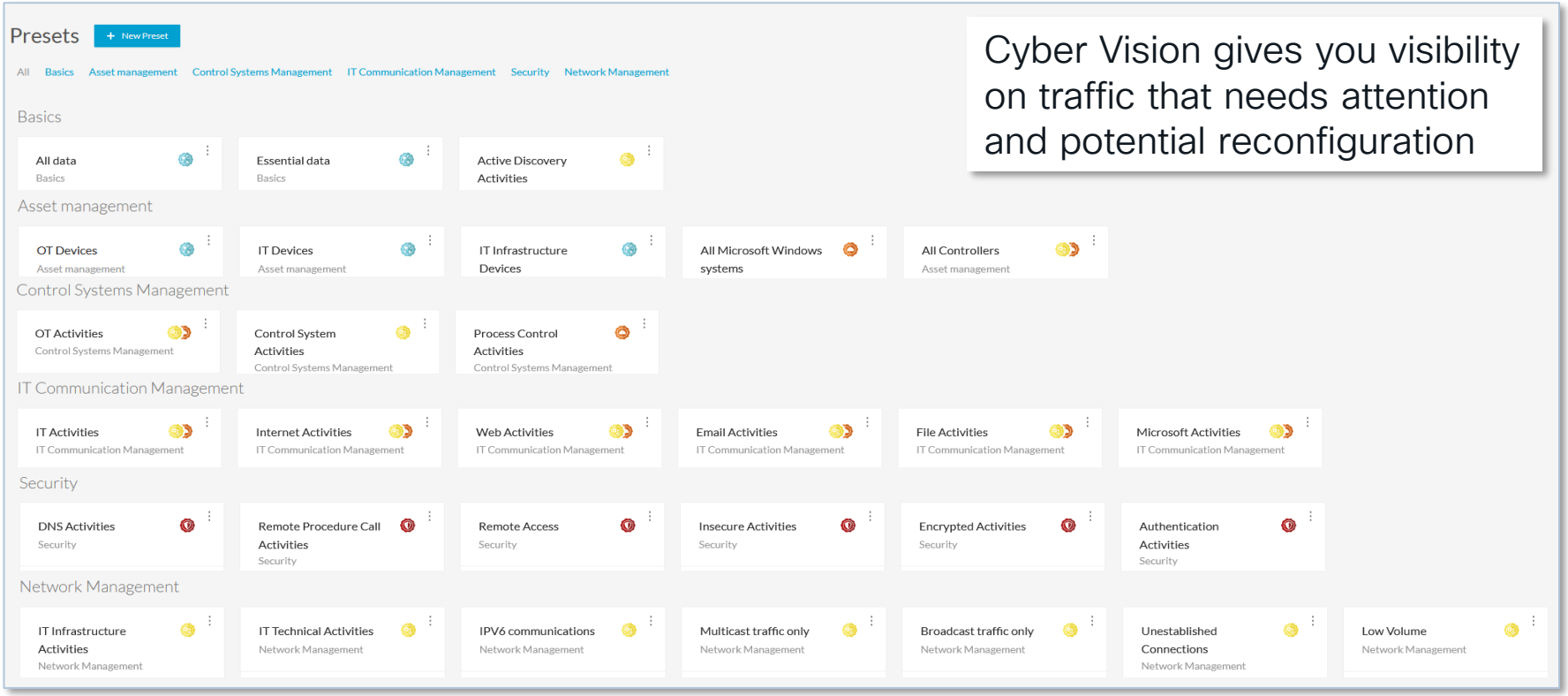
Source: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95

Example: Replace critical switches with Cisco IE Switch running Cyber Vision sensor to see the entire OT network

Note: You don't need to replace all industrial switches, just the ones connecting to PLC's

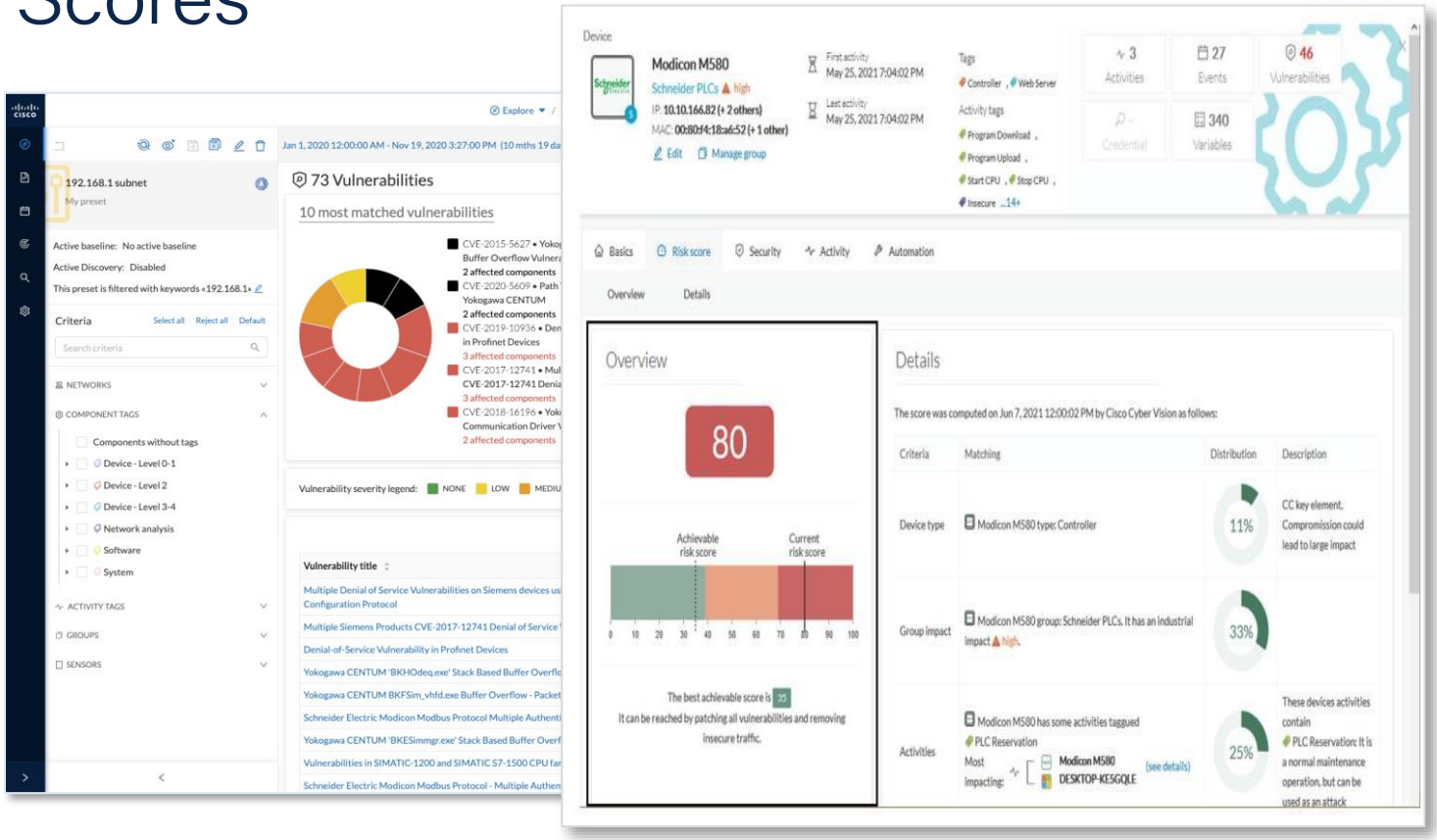
OT View of Security Posture

Cisco CyberVision

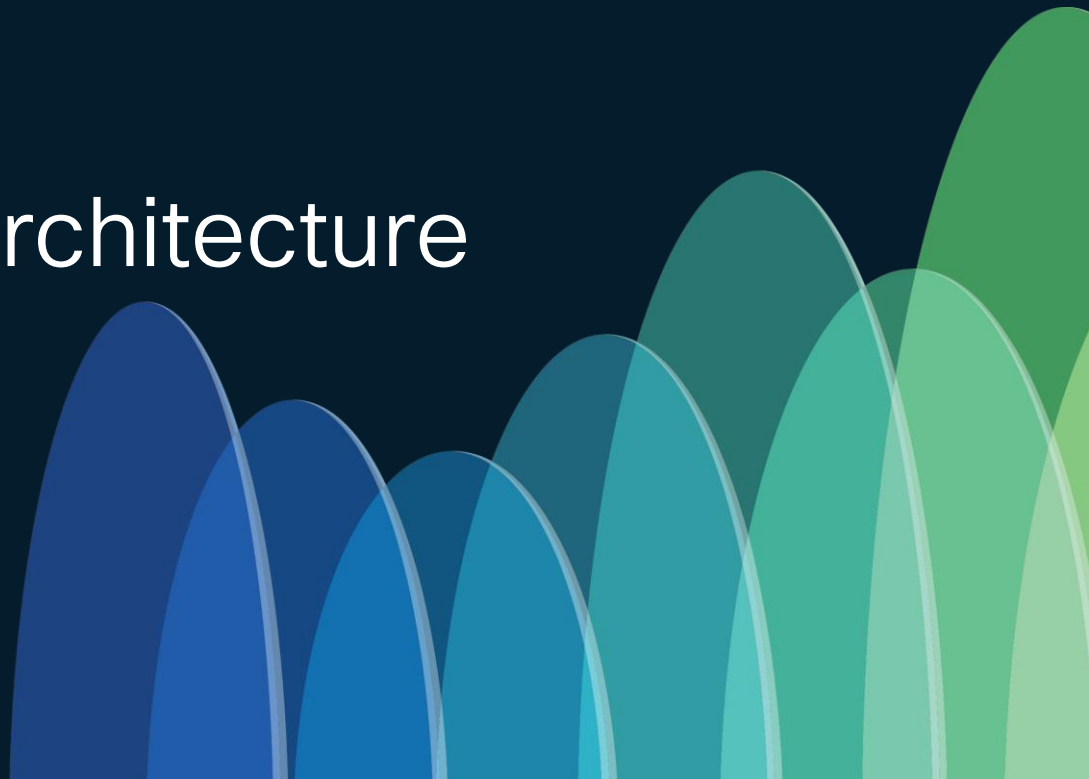


Cyber Vision gives you visibility on traffic that needs attention and potential reconfiguration

Automatically identify asset vulnerabilities & Assign Scores

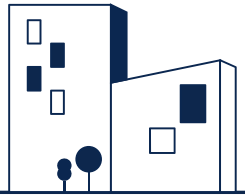


Cisco P5GaaS Architecture



cisco Live!

Typical Private Cellular Areas to Address



Enterprise and Service Provider Access

- Policy and Service Configuration
- Subscriber Provisioning
- Usage Reporting
- SIM and Identity Provisioning

Enterprise Domain

- Devices
- Applications

Enterprise + Cloud / Service Provider Domain

- 4G/5G Mobility Management
- 4G/5G Session Management
- Unified Data Manager
- Unified Data Repository
- Radios (Radio Unit)
- User Plane Function
- Home Subscriber Server
- Authentication Function
- 4G/5G Distributed Unit
- 4G/5G Centralized Unit
- 4G/5G Mobility Management
- 4G/5G Session Management

Provisioning ⟷

Logging ⟷

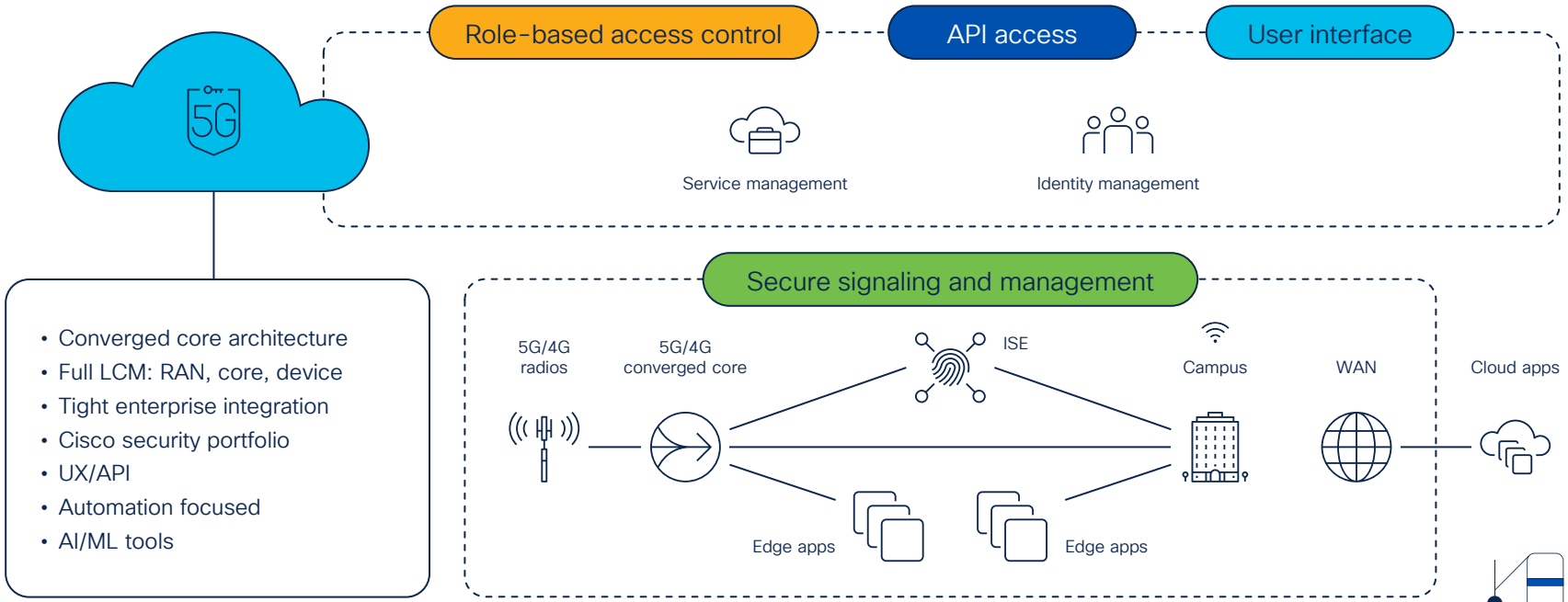
Metrics / Events ⟷

Management

- Automation Tools
- RBAC
- Software Life Cycle Management
- SLA Management
- Radio mgt

Not all functions shown

Cisco Private 5G in the enterprise



- Converged core architecture
- Full LCM: RAN, core, device
- Tight enterprise integration
- Cisco security portfolio
- UX/API
- Automation focused
- AI/ML tools

Key Cisco solution blocks

P5G edge

Deployed per enterprise site

Anchor 4G and 5G device support

Secure onboarding via edge proxy

- TLS connection to cloud

Integration with RAN and enterprise network components

- Provides backend data for UI
- Enables cloud based continuous monitoring and management

Orchestration and automation

REST APIs

Cisco control center

Geo-redundantly deployed across the continents

Enterprise and MSP portals (UI/UX)

- Role based access control
- Multi-tenancy across the board
- E2E network management

SIM device management (SDM)

- AUSF, UDM, and UDR for 5G
- HSS for 4G

Charging function

Robust API platform

Device management and monitoring

Cloud native deployment platform

Deployed at CSP's availability zones

P5G edge management and monitoring

- NF lifecycle management
- Orchestration and automation

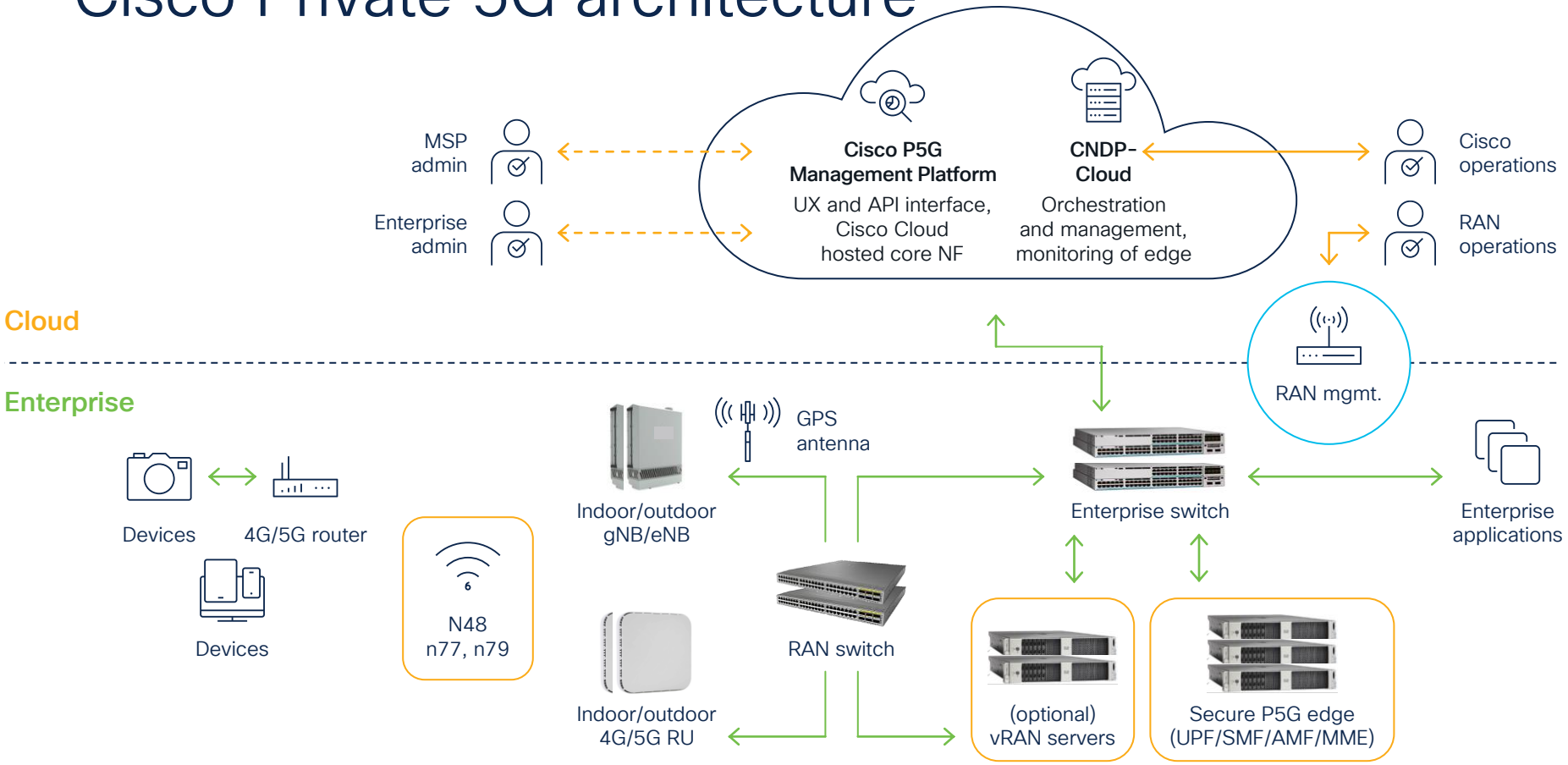
CI/CD

Secure edge onboarding via cloud proxies

- TLS endpoints

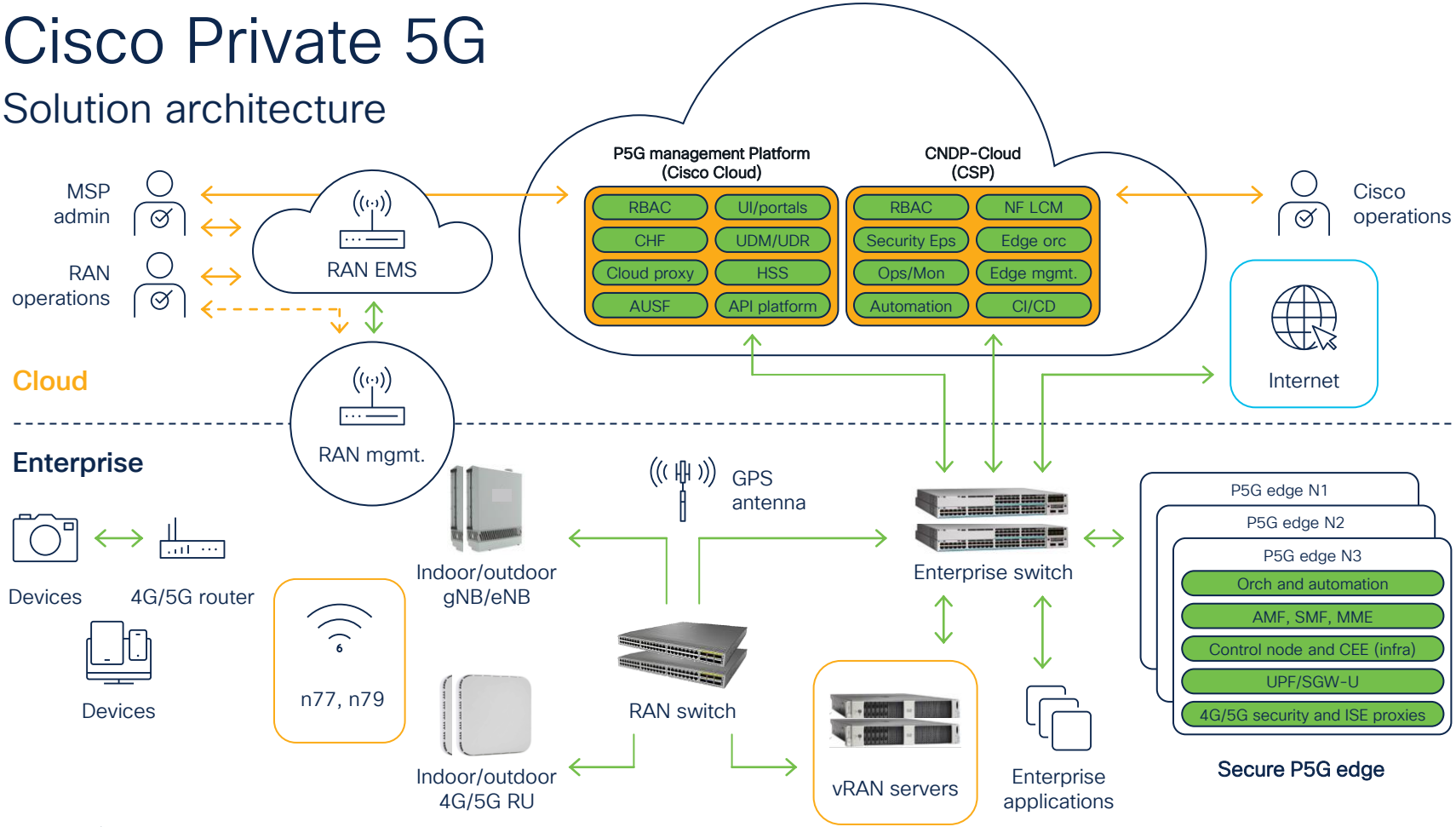
Multi-tenant platform

Cisco Private 5G architecture

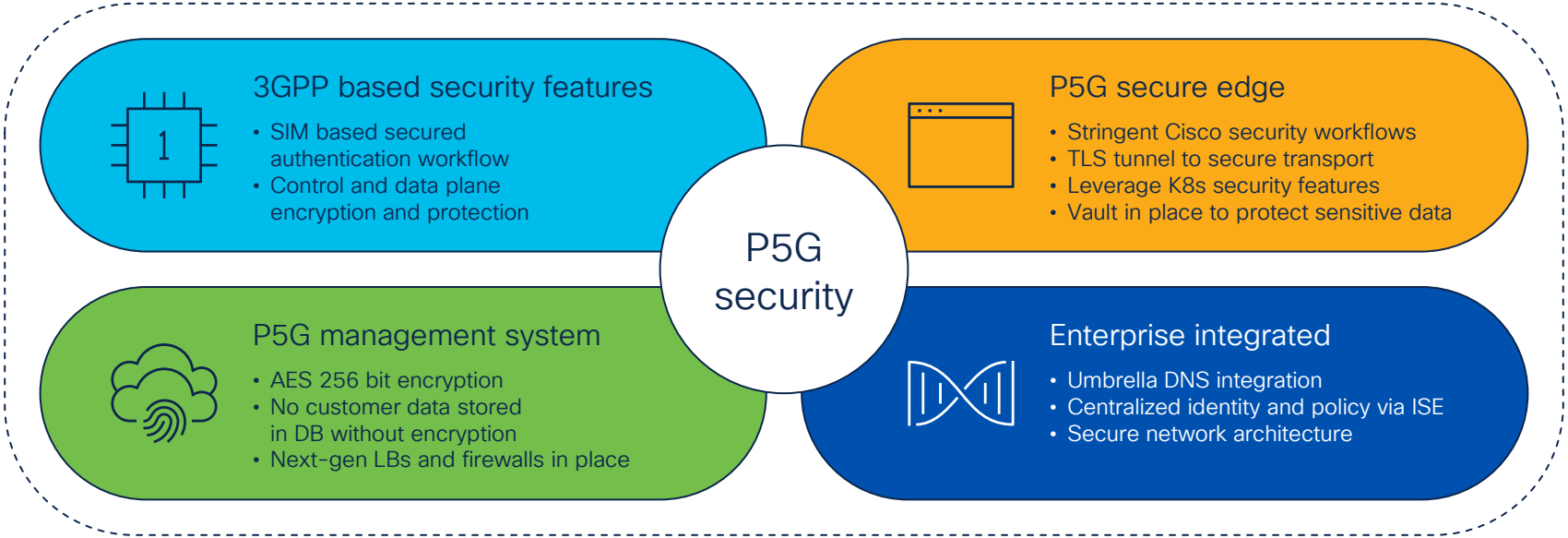


Cisco Private 5G

Solution architecture

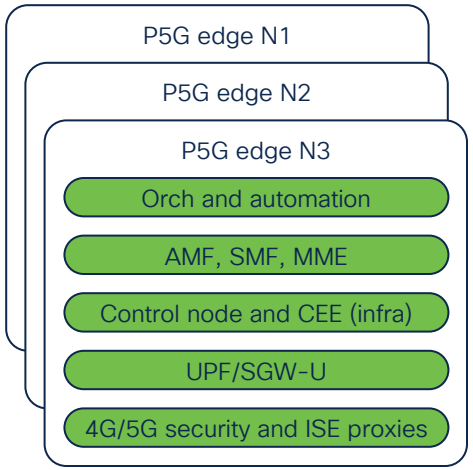


Security across the portfolio



Enterprise grade security across the board

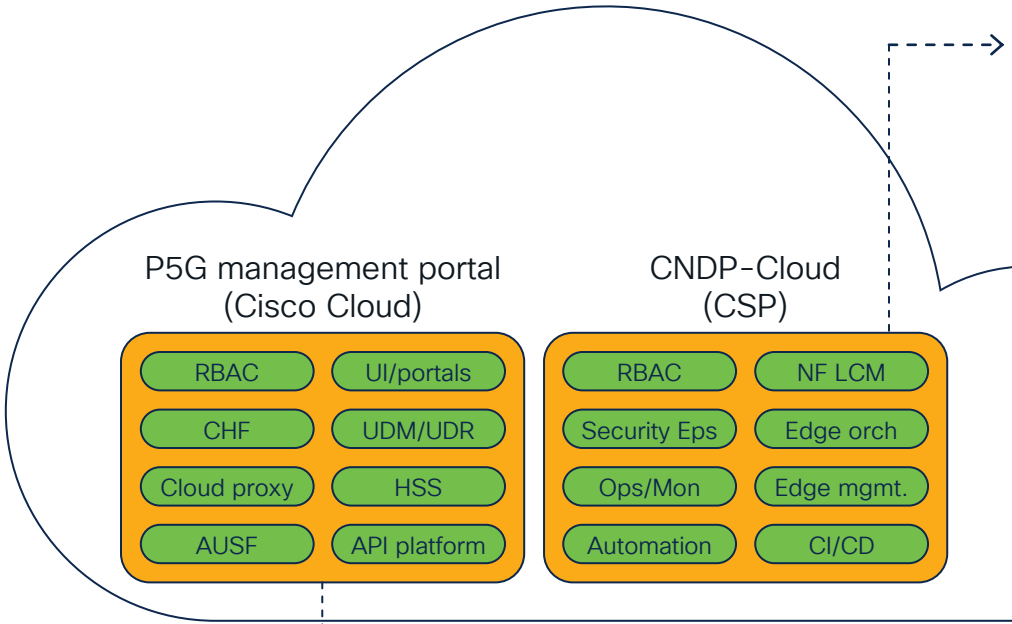
P5G edge security



Secured P5G edge

- Hardened microservices
- TLS connectivity between components
- No remote connection
- AES 256 volume encryption for data at Rest
- Enhanced app layer security over HTTPS via Secure proxy
- Frequent key rotation

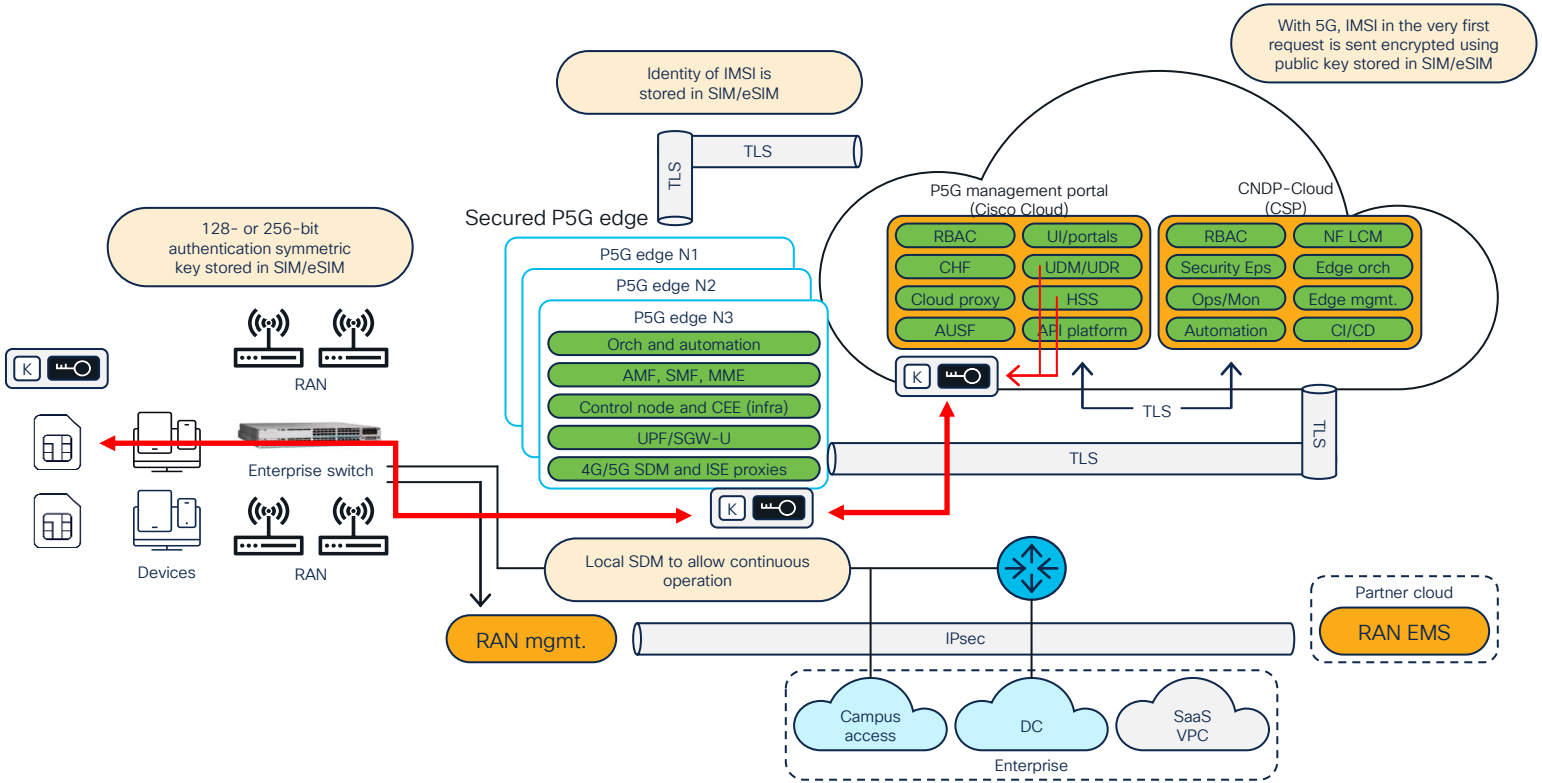
P5G cloud security



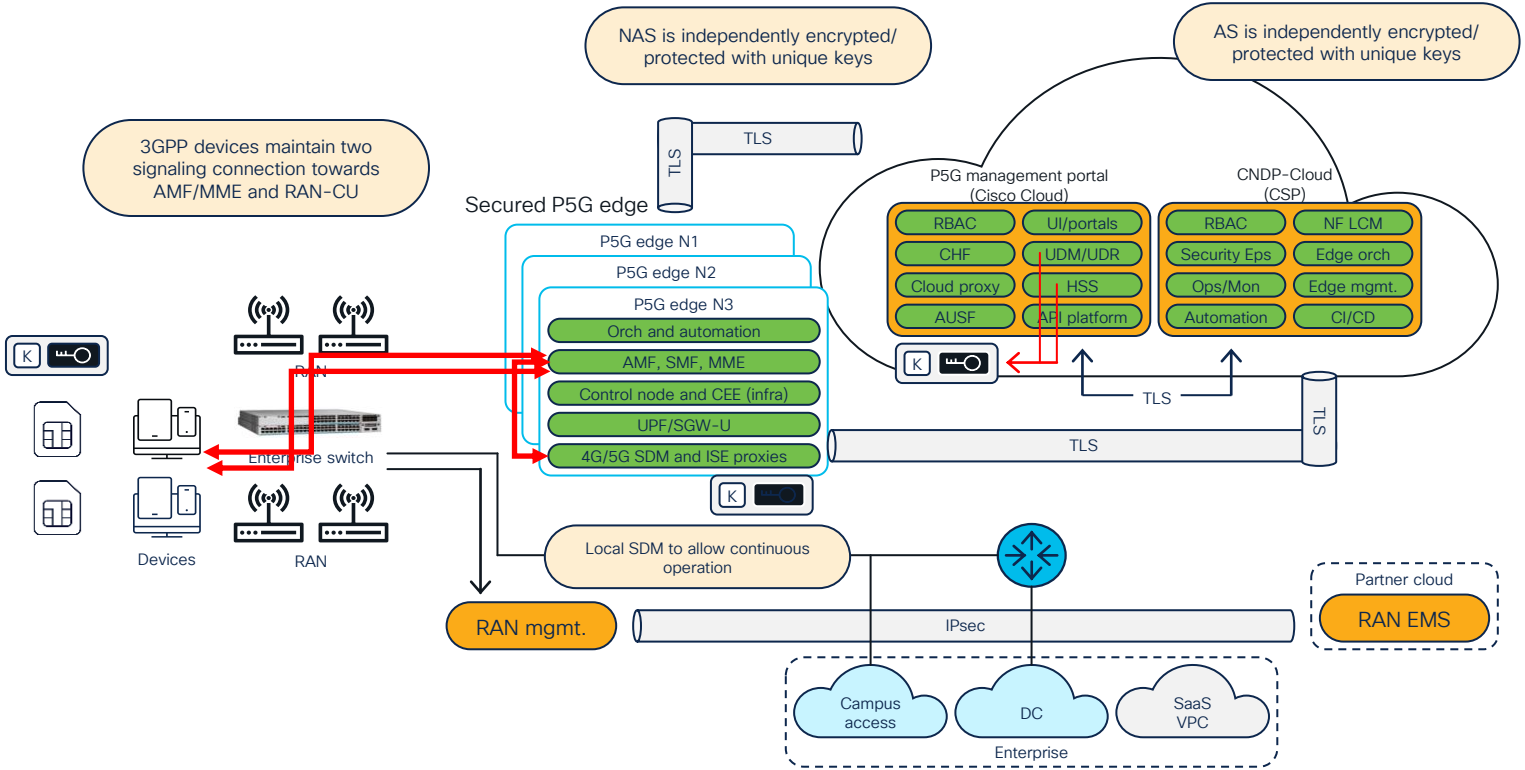
- AES 256 volume encryption for data at Rest
- Multi-tenant environment
- Frequent key rotation
- Encrypt/decrypt data before transmission using Vault; All customer data encrypted before storage

- Advanced load balancers and firewalls in place
- Hardened Microservices
- Geo-Redundant and Multi-tenant cloud environment
- Data remains isolated per enterprise tenant and secured to ensure separation of metrics

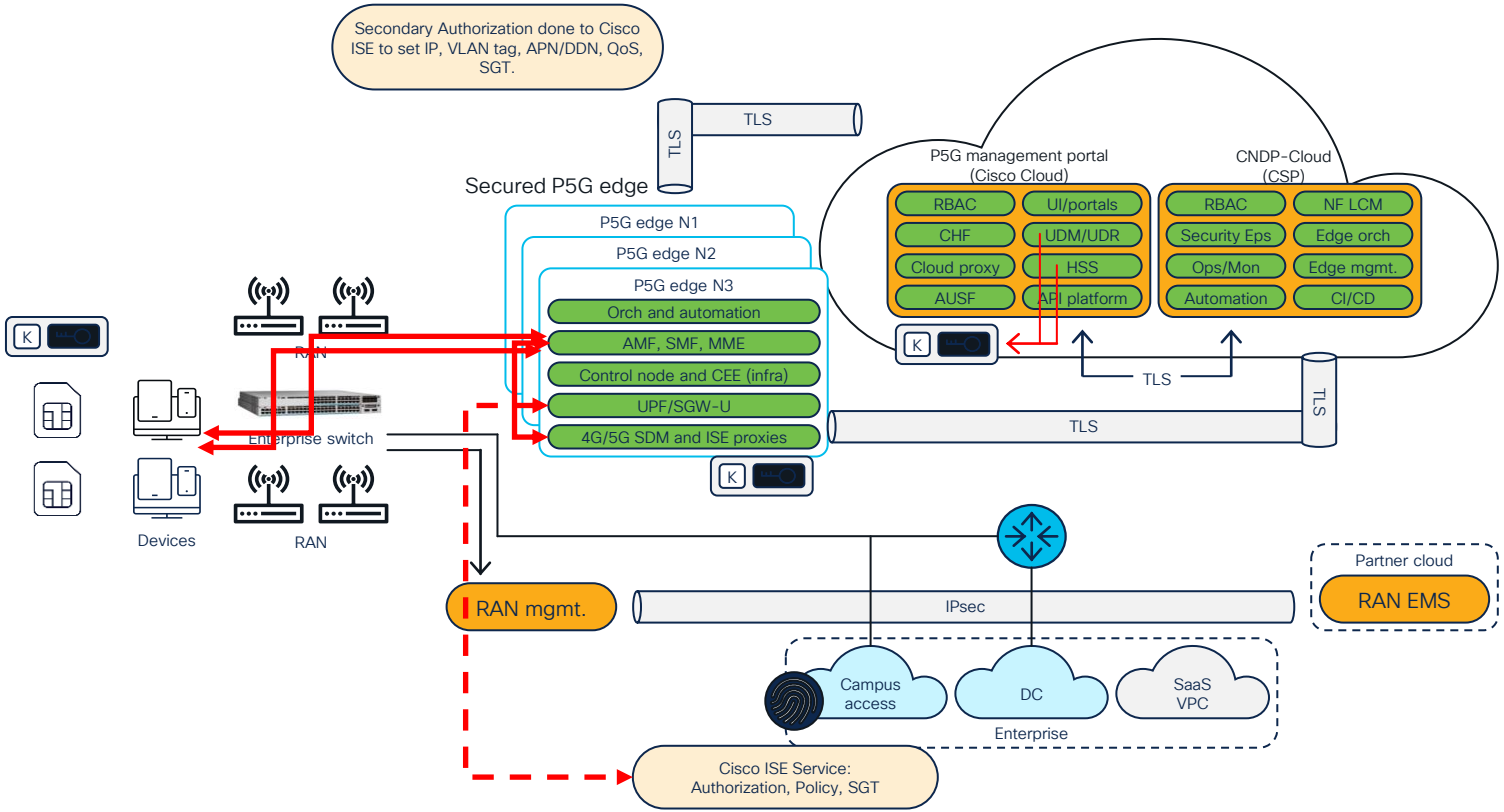
P5G Security Standards: SIM profiles



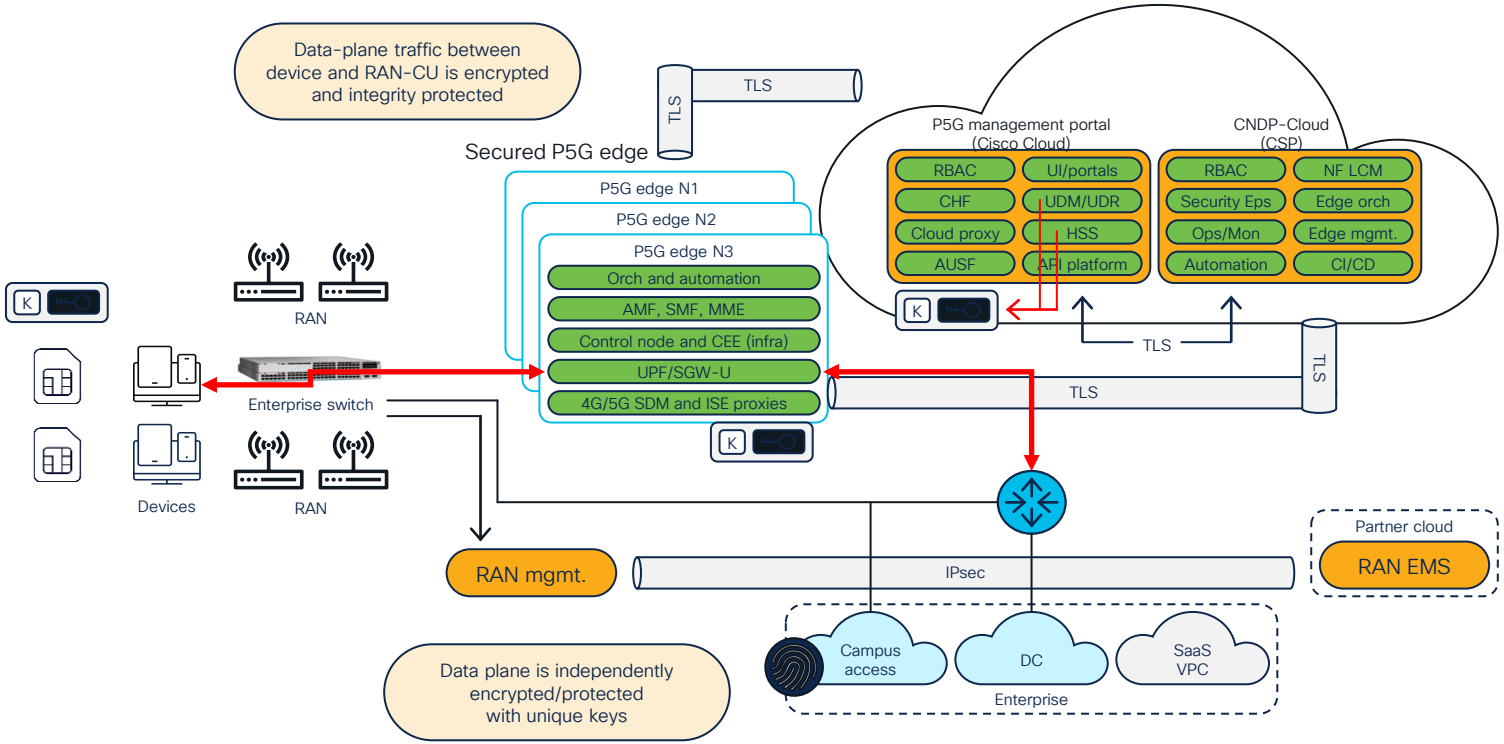
P5G Security Standards: Authentication



P5G Security Standards: 2nd Authorization



P5G Security Standards: Bearer Traffic



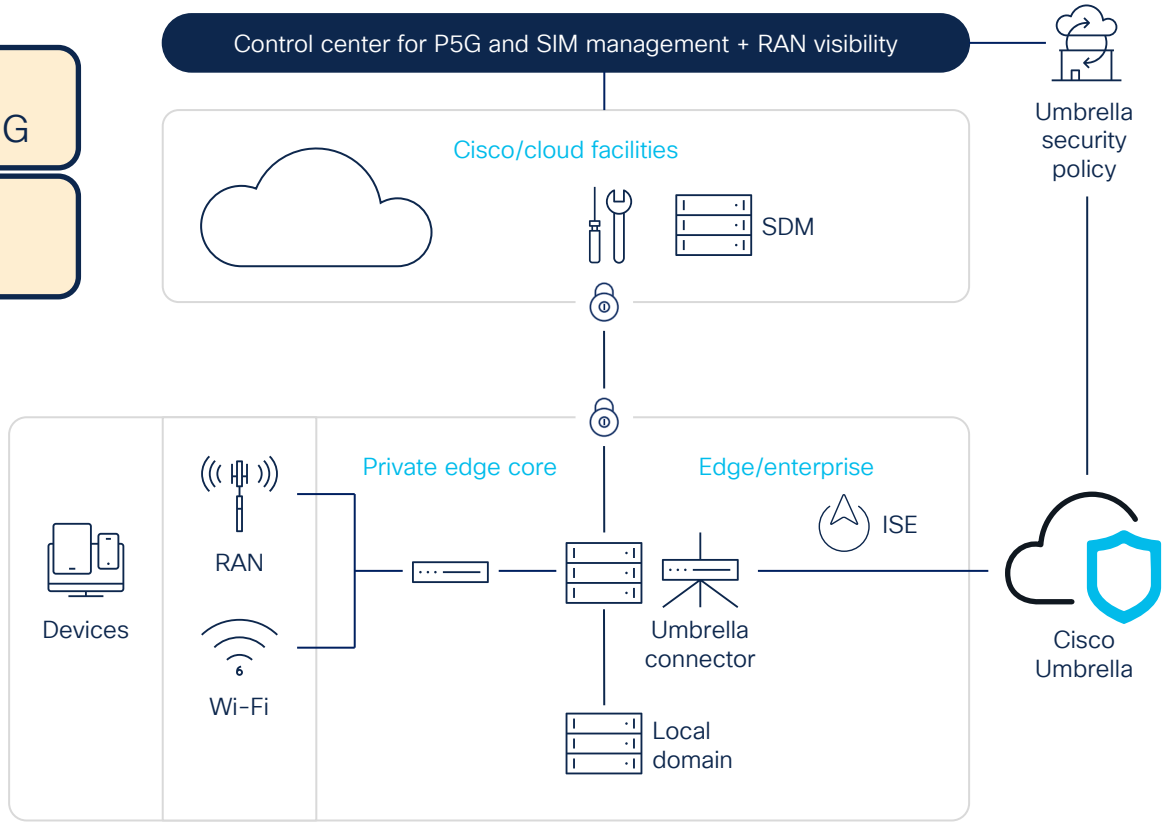
Extending security via Umbrella

Common security models for existing Wi-Fi access + private 5G

Leveraging existing enterprise infrastructure when applicable

Capability examples*

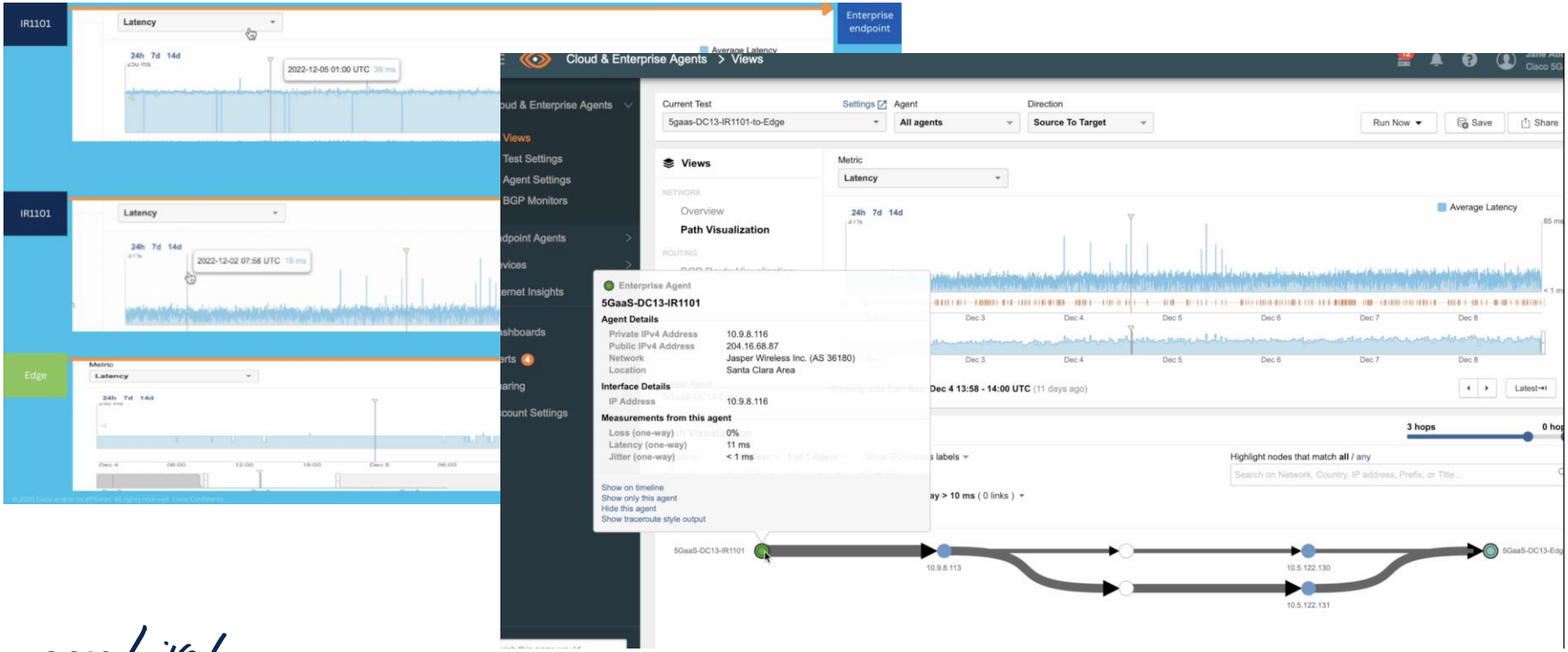
- Basic redirect
- Allow/deny list
- Centralized v/s global access list
- Limit content access
- Control applications
- Common onboarding / accounting
- Local domain offload



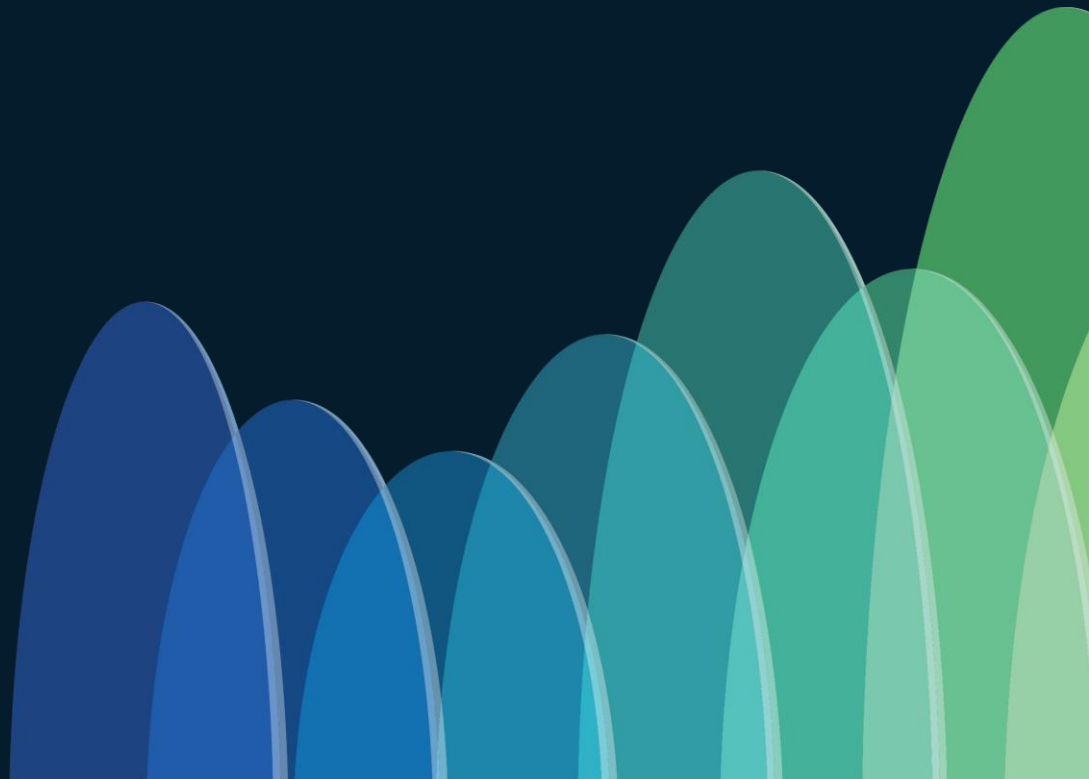
Assisted Operations

User Experience: Service Assurance

- Using ThousandEyes to provide visibility & Service Assurance for P5G deployments



P5G & OT Technology Integration



cisco Live!

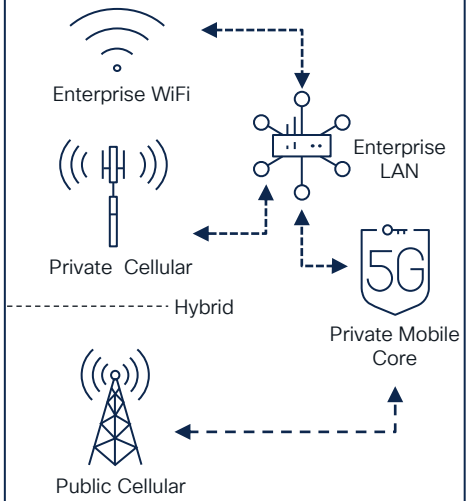
Cisco P5GaaS Solution Integration Business Value

Hybrid Integrated Private Wireless Solutions

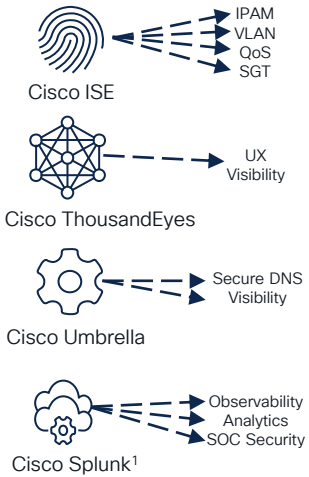
across Enterprise Applications

Private Wireless Networks | **Cisco Control Center** | **Enterprise backend integrations & Use-Cases**

Integrated Private Wireless Network



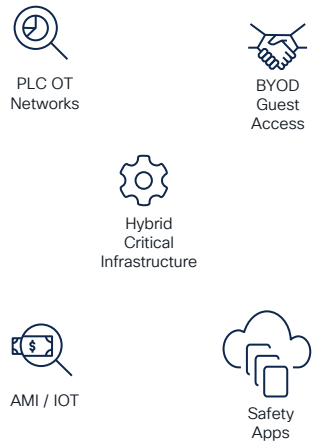
Deep Network Integrations



IT Network Integration

OT Network Integration

Use Cases

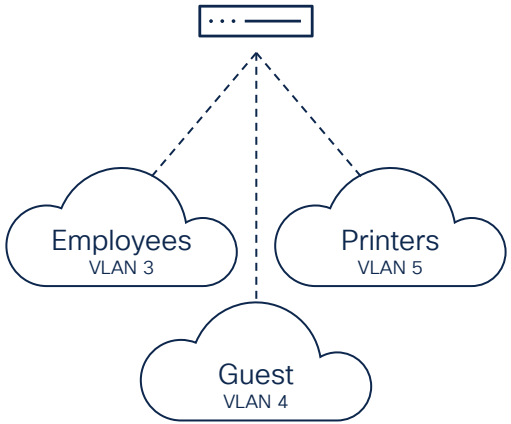


[1] Roadmap item

Authorization enforcement options

VLANs

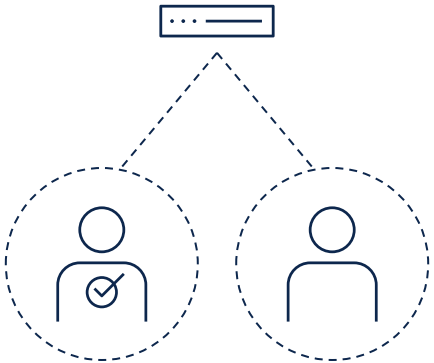
Dynamic VLAN assignments



Per port / per domain / per MAC

ACLs

Access Control Lists



Employee

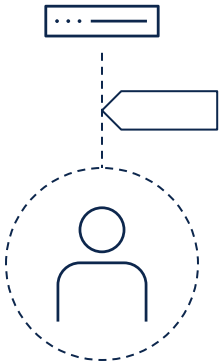
permit ip any any

Contractor

deny ip host <critical>
permit ip any any

SGTs*

Cisco group-based policy

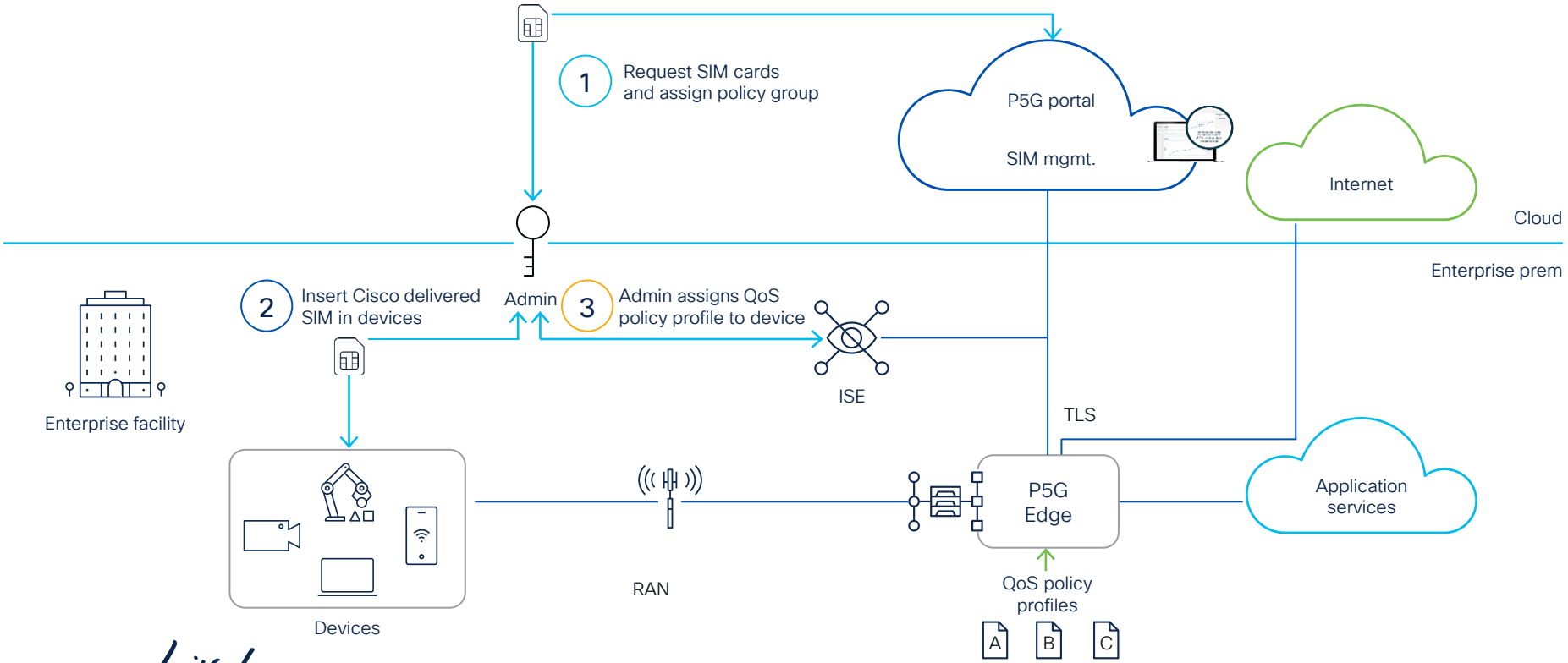


16-bit SGT assignment and
SGT based access control

* Coming soon

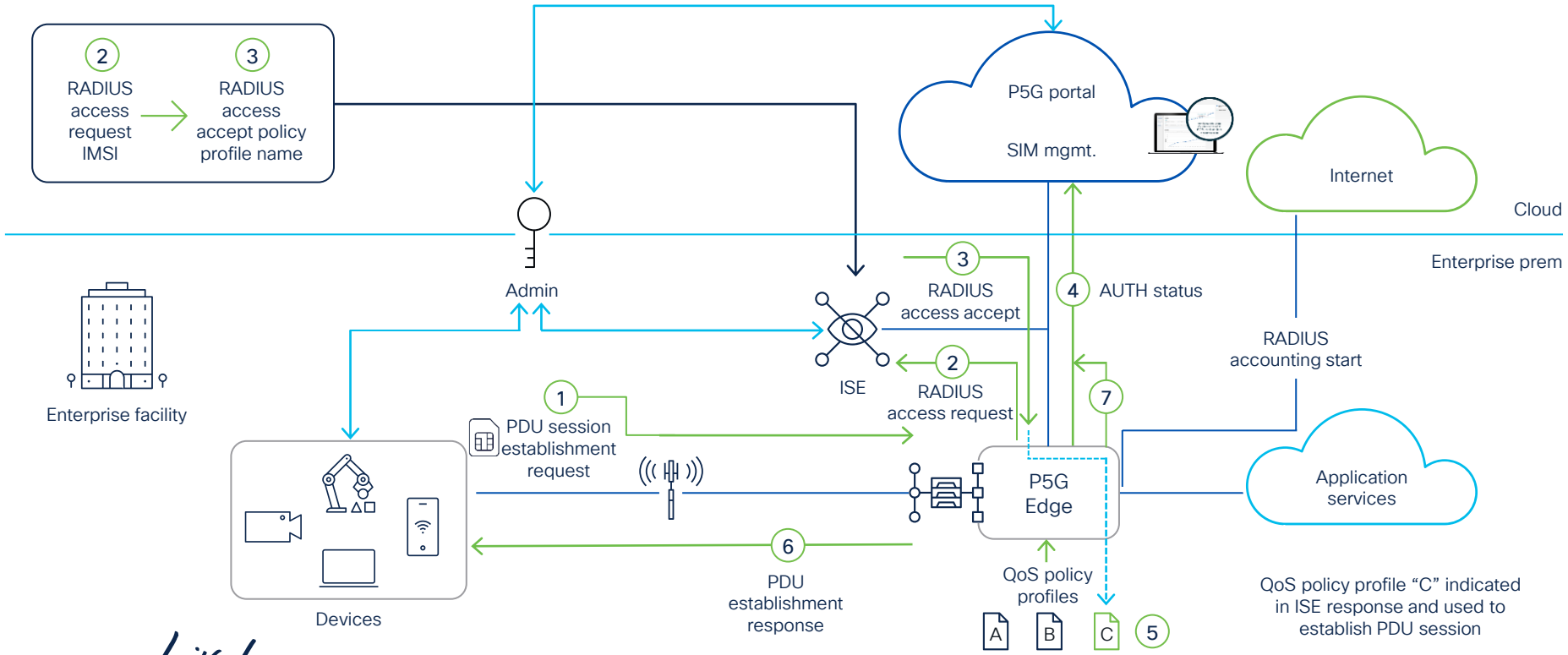
P5G and ISE integration

Overview



P5G and ISE integration

Secondary authorization workflow



ISE enables zero trust in P5G

Enterprise

Endpoints

- Users
- Devices
- Things

Network devices

- Switches
- WLCs / APs
- VPN
- P5G

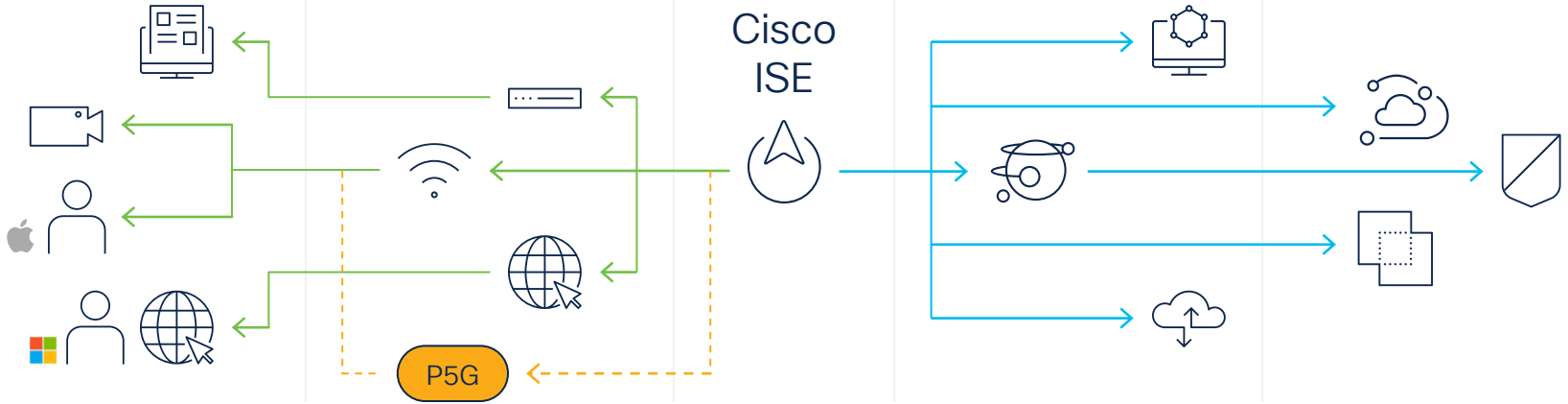
Security

Identity services

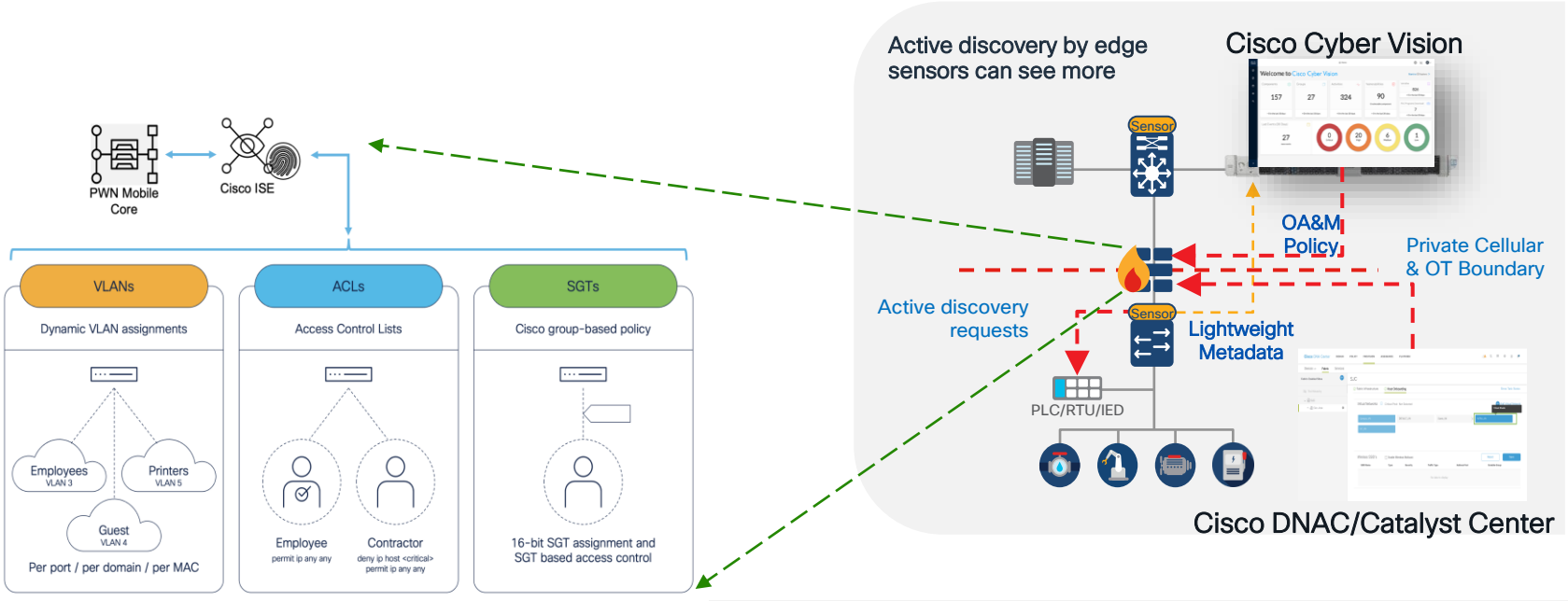
- Azure/AD/LDAP
- MDM
- SAML/MFA

Security services

- Cloud analytics
- Secure firewall
- Partners

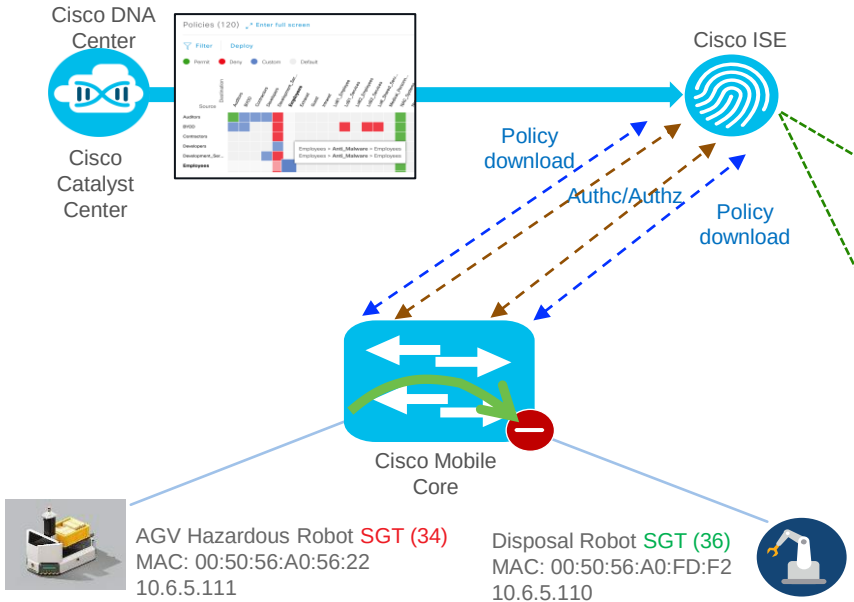


Security Across Access and Network



Enterprise grade security across the board

Integrated Dynamic Policy based on SGT

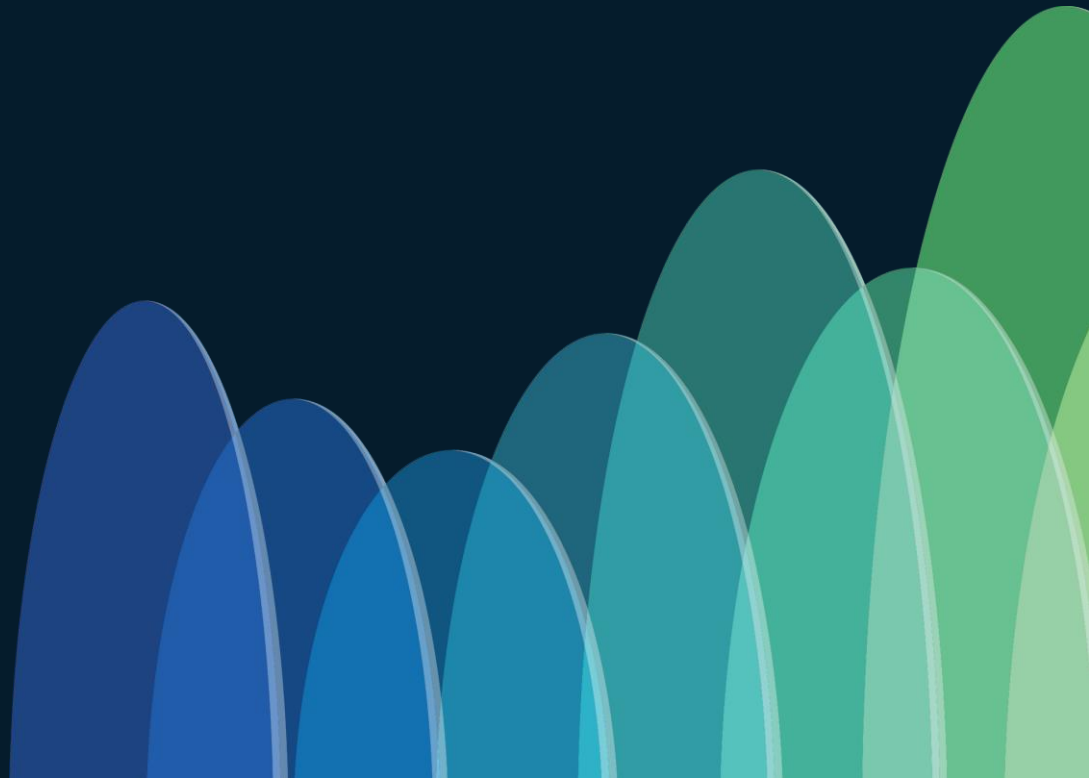


Nuclear Power Plant Controlled Policy:

- Cisco ISE Classification: Dynamic
- Src SGT found, Dst SGT found
- Enforcement: At Egress
  (PWN Mobile core, existing Router/Switches)

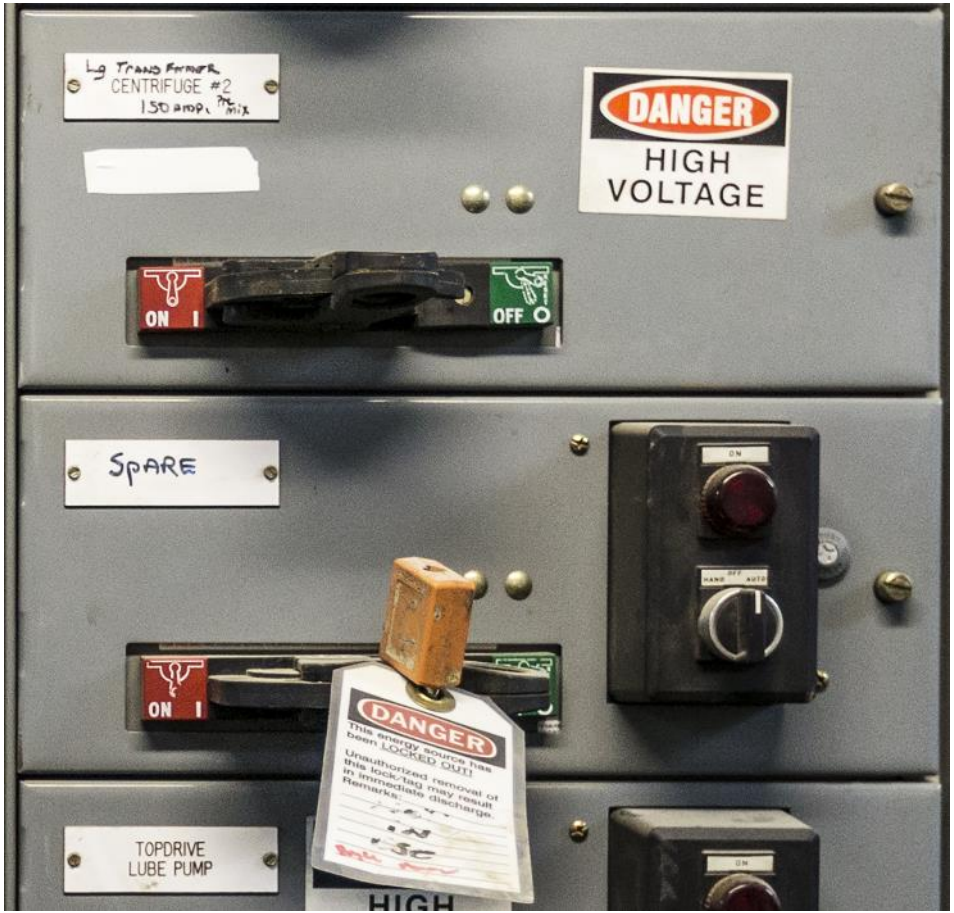
Egress Policy	Destination: AGV Vehicle APP	Destination: Disposal Robot
Source: AGV Vehicle	Permit All	Deny All
Source: Disposal Robot	Deny All	Permit All

OT Wireless: Leveraging P5GaaS



cisco Live!

Critical: Safety Is EVERYTHING



OT Industrial automaton – Oil and Gas

Secure network for refinery and process plants

Combining industrial wired and wireless networks and security for operational excellence

Challenge:

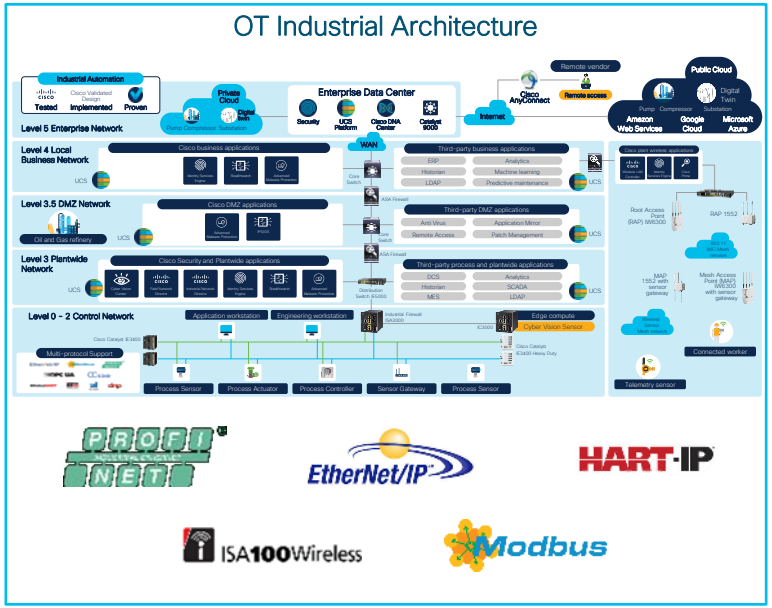
Complex network silos creating downtime, data isolation, and vulnerabilities. Inflexible and high TCO.

Critical needs:

- Scalable, converged network
- Security built in
- Simple to deploy and troubleshoot
- Highly available
- Worker mobility and safety
- Enable edge applications
- Ruggedized

What's new:

- P5GaaS with P5G/WiFi Session Persistence
- IW6300 Class1/Div 2 AP for hazardous locations
- 802.15.4 wireless instrumentation with industry-leading partners
- Worker mobility over 802.11 Wi-Fi
- IACS device visibility and anomaly detection – Cisco® Cyber Vision



Business outcomes

Securely connect plant floor to enable:

- Reduced downtime
- Improved OEE
- Improved safety and security
- Workforce enablement
- Digitization / Refresh

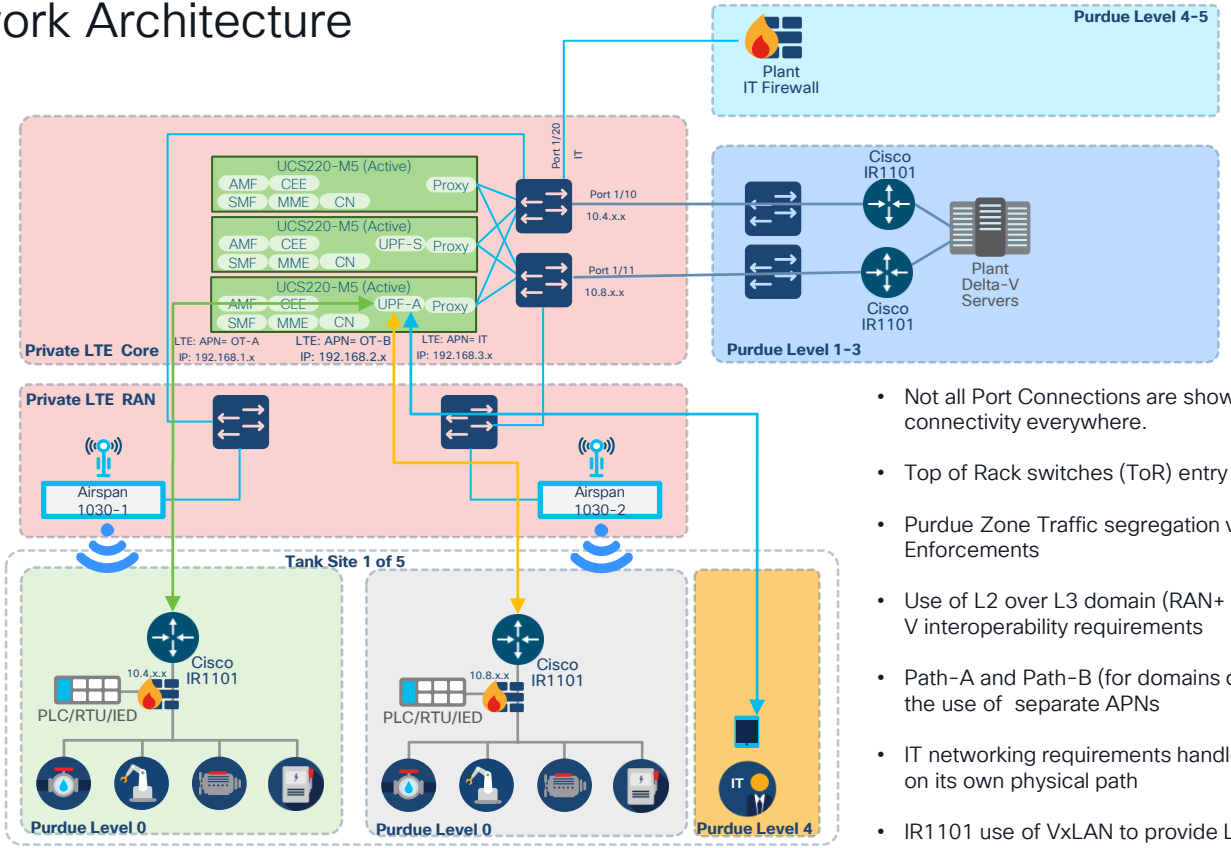
Cisco P5GaaS: Chemical Plant Customer

Success Story

- Chemical Product Manufacture of **Chlor Alkali Products & Vinyl's** and **Epoxy**.
- Plant Operator: USA
- Uses Emerson Delta-V Process control system, PLC to MMI handled via Cisco P5GaaS
- Success Criteria:
  - Critical Infrastructure: Needed dual RF/backhaul & Aggregation path for each PLC
  - Security following Purdue zone-based architecture
  - Support IT wireless traffic separately, following Purdue Framework
  - Outdoor based Infrastructure: Challenging RF environment

Cisco P5GaaS for Chemical Plant

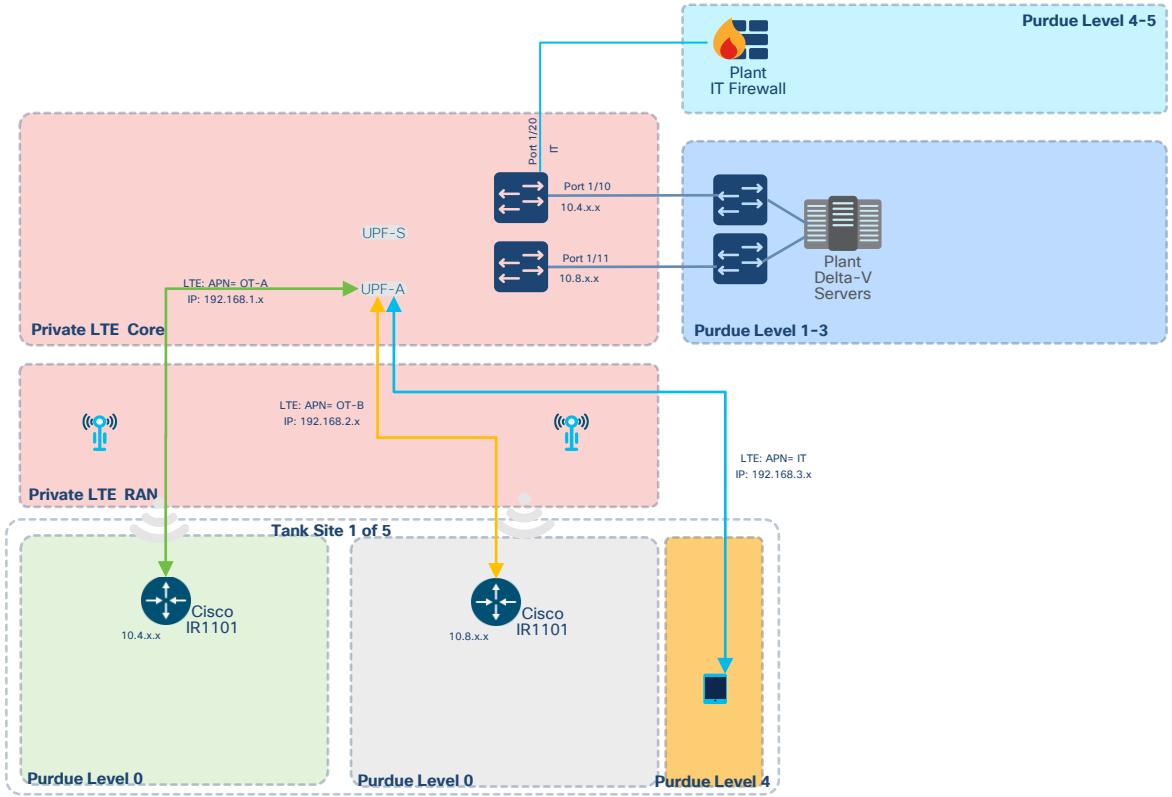
Network Architecture



- Not all Port Connections are shown, HA Architecture requires dual-port connectivity everywhere.
- Top of Rack switches (ToR) entry and exit points for P5GaaS Servers
- Purdue Zone Traffic segregation via L2 domains, & QoS Security Policy Enforcements
- Use of L2 over L3 domain (RAN+ LTE Core) to minimize Emerson Delta-V interoperability requirements
- Path-A and Path-B (for domains on 10.4.x.x and 10.8.x.x) handled via the use of separate APNs
- IT networking requirements handled separately using IT APN terminated on its own physical path
- IR1101 use of VxLAN to provide L2 over IP for Emerson Delta-V Systems

Cisco P5GaaS for Chemical Plant

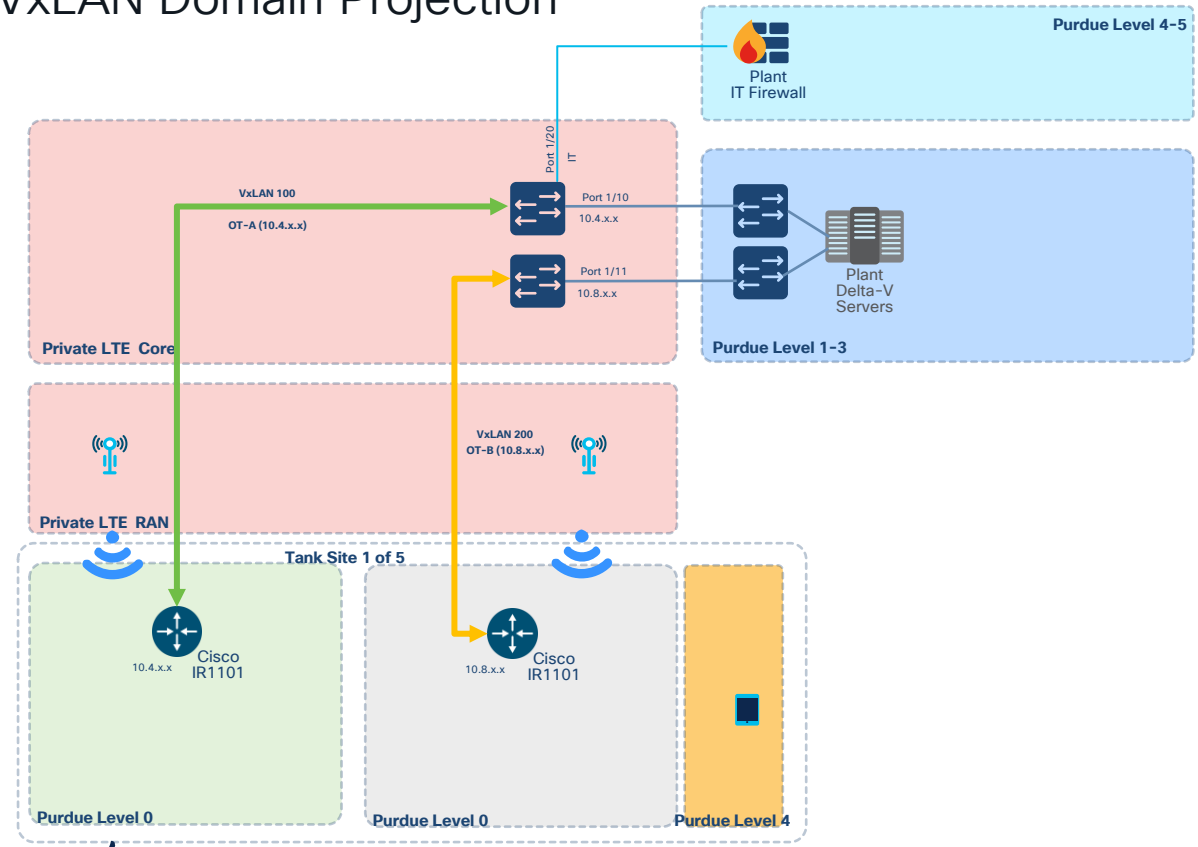
RAN Traffic Segregation



- Not all Port Connections are shown, HA Architecture requires dual-port connectivity everywhere.
- Top of Rack switches (ToR) entry and exit points for P5GaaS Servers
- Purdue Zone Traffic segregation via L2 domains, & QoS Security Policy Enforcements
- Use of L2 over L3 domain (RAN+ LTE Core) to minimize Emerson Delta-V interoperability requirements
- Path-A and Path-B (for domains on 10.4.x.x and 10.8.x.x) handled via the use of APNs
- IT networking requirements handled separately using IT APN terminated on its own physical path

Cisco P5GaaS for Chemical Plant

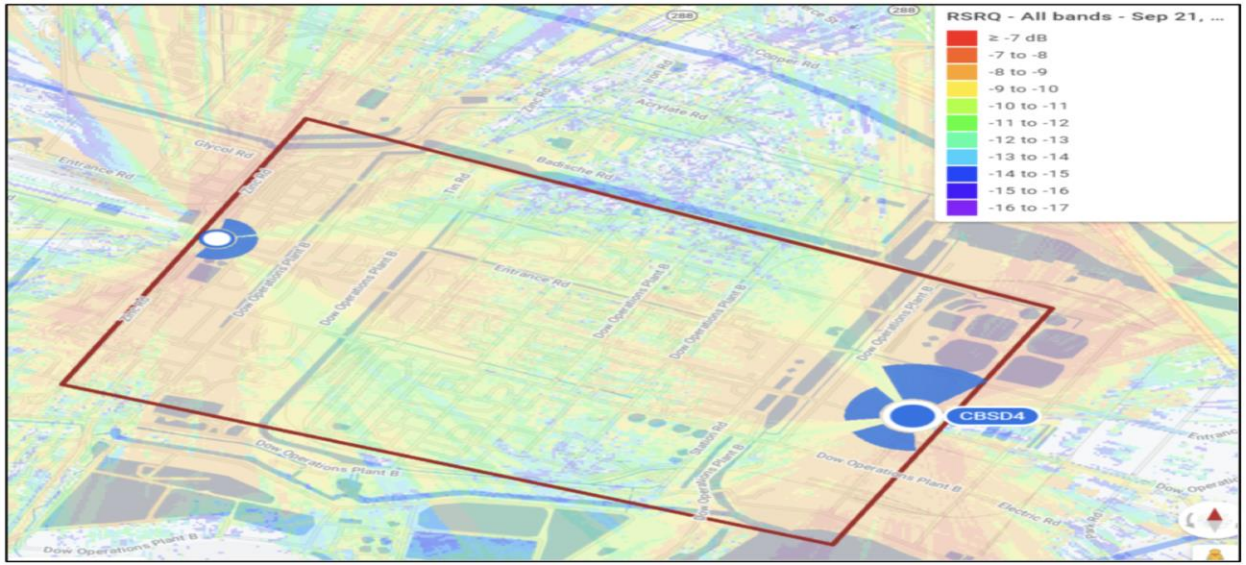
VxLAN Domain Projection

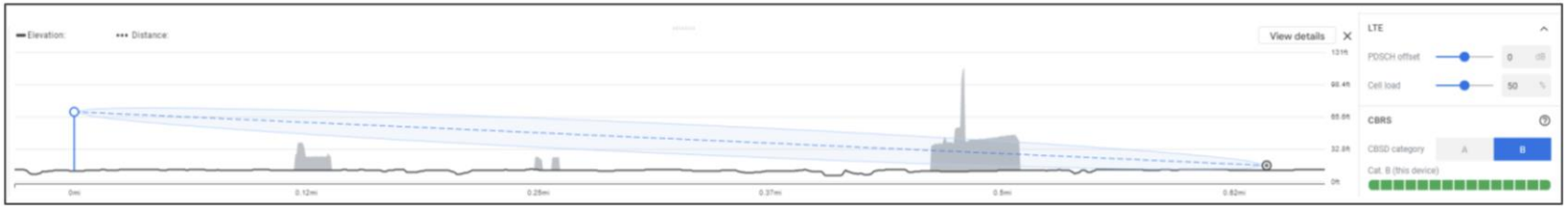


- Not all Port Connections are shown, HA Architecture requires dual-port connectivity everywhere.
- Top of Rack switches (ToR) entry and exit points for P5GaaS Servers
- Purdue Zone Traffic segregation via L2 domains, & QoS Security Policy Enforcements
- Use of L2 over L3 domain (RAN+ LTE Core) to minimize Emerson Delta-V interoperability requirements
- Path-A and Path-B (for domains on 10.4.x.x and 10.8.x.x) handled via the use of APNs
- IT networking requirements handled separately using IT APN terminated on its own physical path

Cisco P5GaaS for Chemical Plant

RF Site Survey

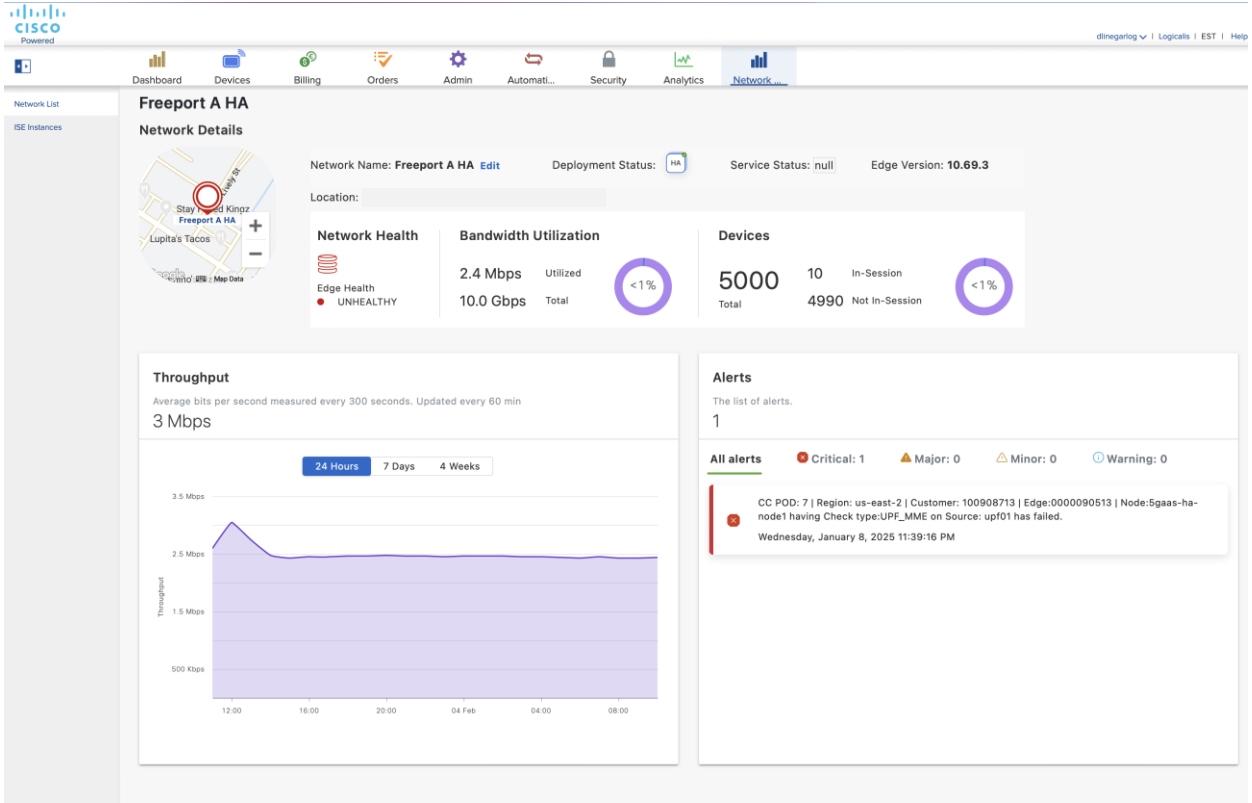




- Outdoor, 2 sq-km Tank farm based operation.
- Using CBRS spectrum, 120-degree Sectorized LTE radios.
- Coverage is over 1 Kms per 120-degree sector, 5 radios, 2 towers
- 2-degree down tilt, 100-foot towers, 75% coverage (per design)
- CBRS spectrum use near Naval base (GAA versus Incumbent) → No service Interruptions due to Frequency Changes.
- Bottom Graph showcases Elevation/Distance with 130-foot tank farm obstruction

Cisco P5GaaS for Chemical Plant

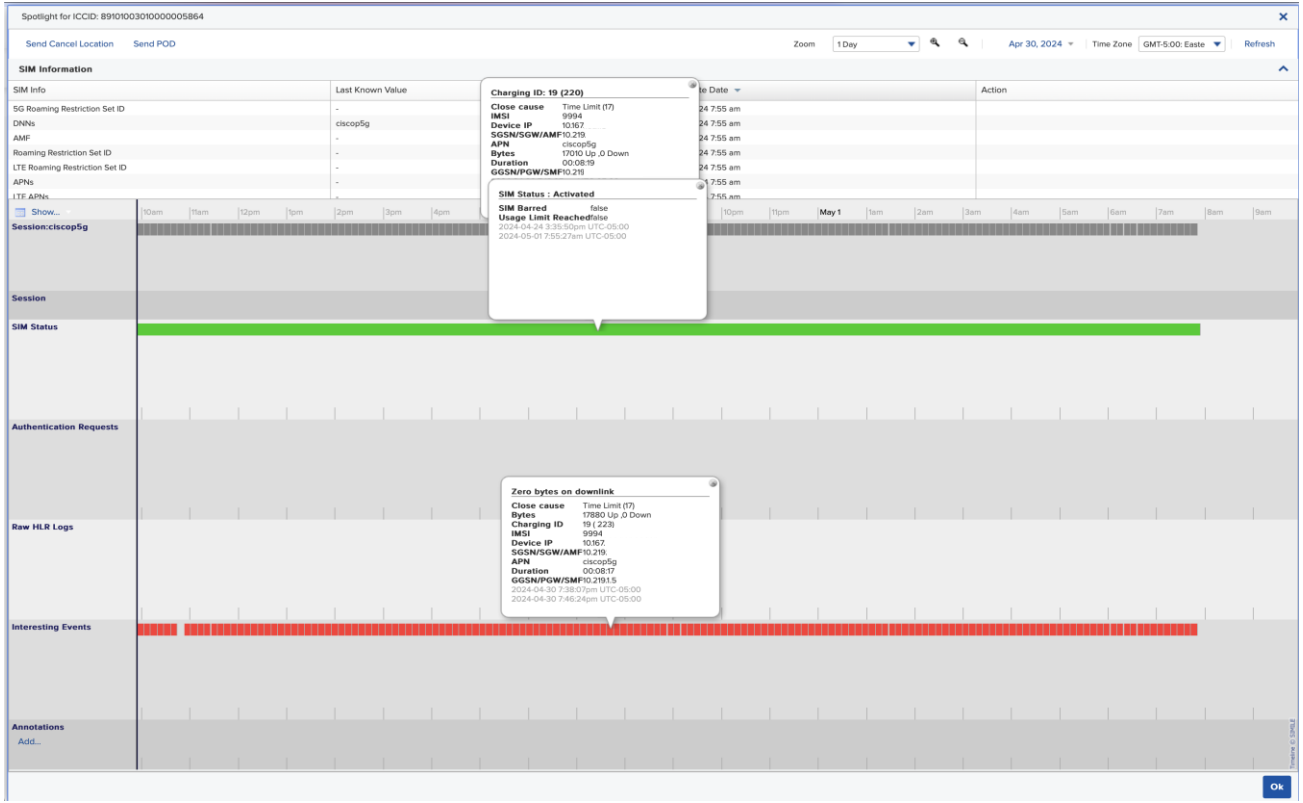
OT Network OAM



- Initial Trial of 8 active OT devices, generating around 300 Mbps of traffic (Emerson Delta-V, VxLAN based)
- IT/OT Segregation of traffic over 3 APN
- Using CBRS spectrum, 120-degree Sectorized LTE radios.
- Coverage is over 1 Kms per 120-degree sector, 5 radios, 2 towers
- CBRS spectrum use near Naval base (GAA versus Incumbent) → No service Interruptions due to Frequency Changes.
- S/W Updates/ Errors handled without Service Impacts: Proven ISSU and HA architecture.

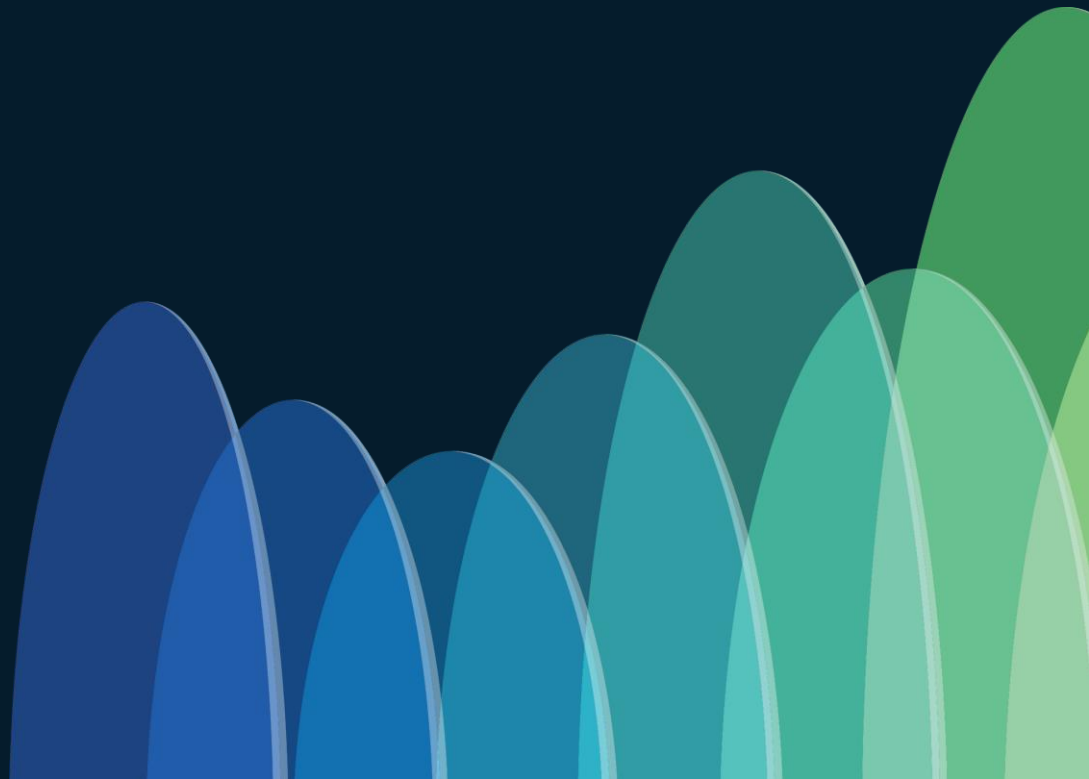
Cisco P5GaaS for Chemical Plant

OT Network OAM



- Plant Operator has control of Device provisioning, Policy and can do their own “OAM”
- Access to Individual Device Operational History
- “Spotlight” collects and displays all relevant events on a timeline
- Allows us to correlate across End-to-End system

Closing, Q&A



Practical Steps to Success: Key takeaways

1

Gaining visibility into your OT is the key

- Beware of hidden costs. Only network sensors can scale.
- Leverage Cyber Vision in your industrial network to get buy-in from OT.

2

Leverage Private Cellular Wireless for OT

- Mission Critical, Deterministic Radio Behaviour, Secured access
- Provide necessary security framework for OT

3

Extend IT security to your OT industrial operations

- Drive network segmentation by using Cyber Vision with ISE.
- Drive Integrated Security Policy, Visibility with P5GaaS, ISE and CyberVision
- Gain visibility on the global enterprise by sharing OT context with IT security tools.

Webex App

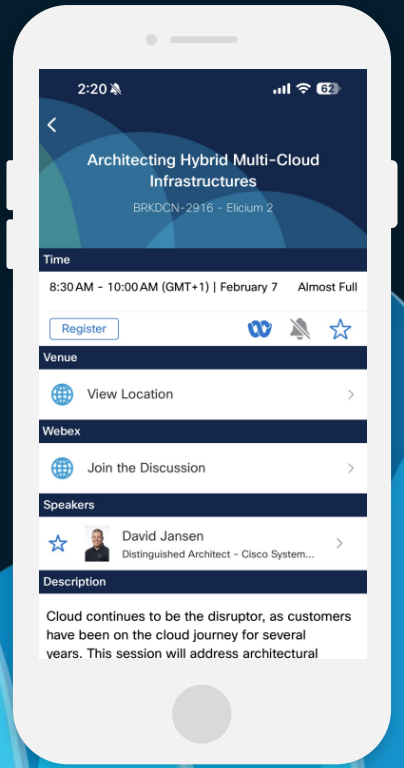
Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.



Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

Content Catalog

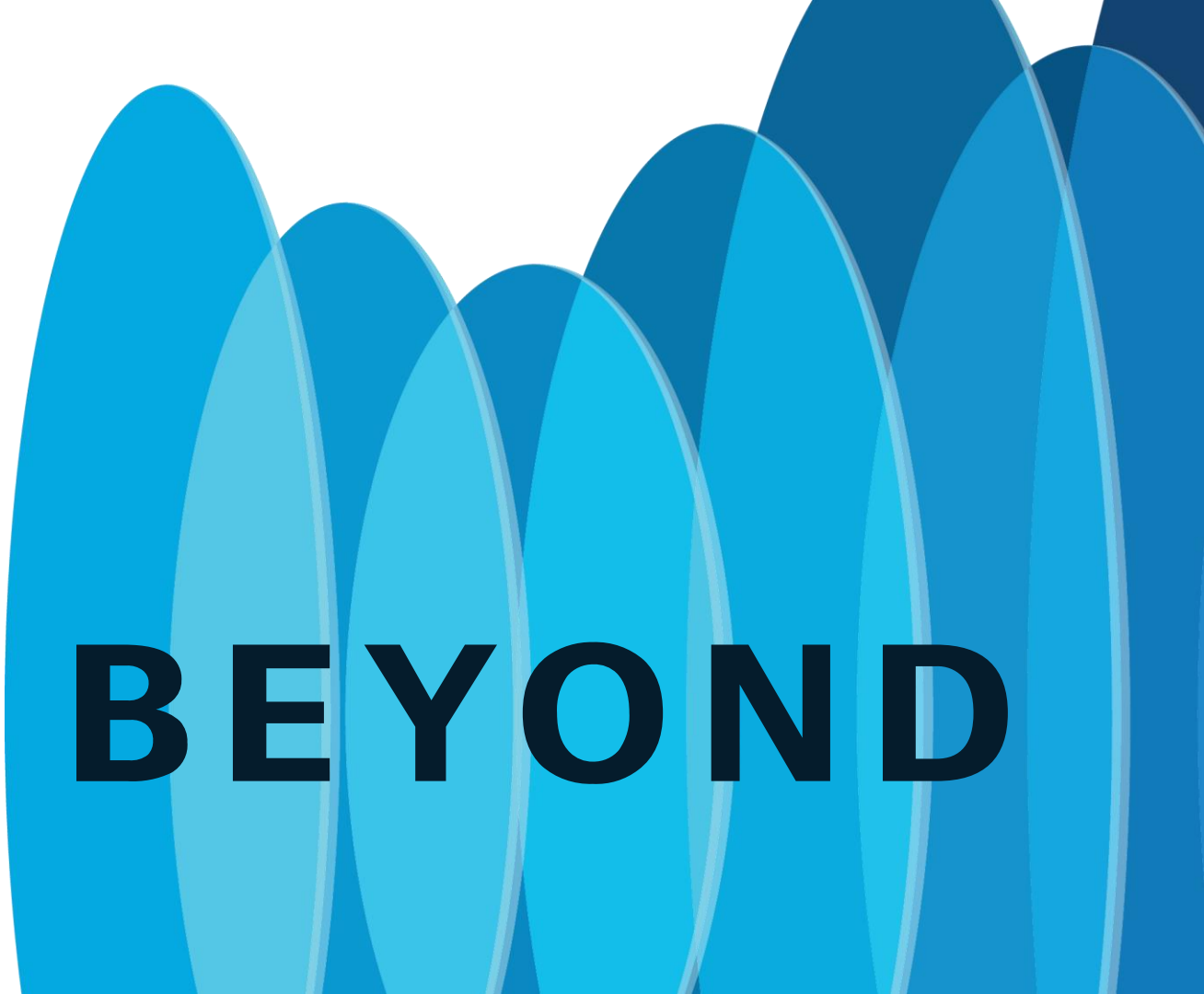
Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Thank you

cisco Live!

cisco Live!



GO BEYOND