Cisco and IOT

Mohamed Bahardeen – mbaharde@cisco.com

IoT TSA

3/10/2022

Agenda

- How IOT is defined at Cisco

- Differences between IT and OT

- Common IOT use cases & How Cisco helps address these use cases
  - Extending networks with wireless
  - Secure Equipment Access
  - OT Network Security - Zero Trust / NAC outside of Enterprise Networks

- Quick Snapshot of the Cisco IOT portfolio

Cisco IoT

IOT at Cisco

Indoor IOT
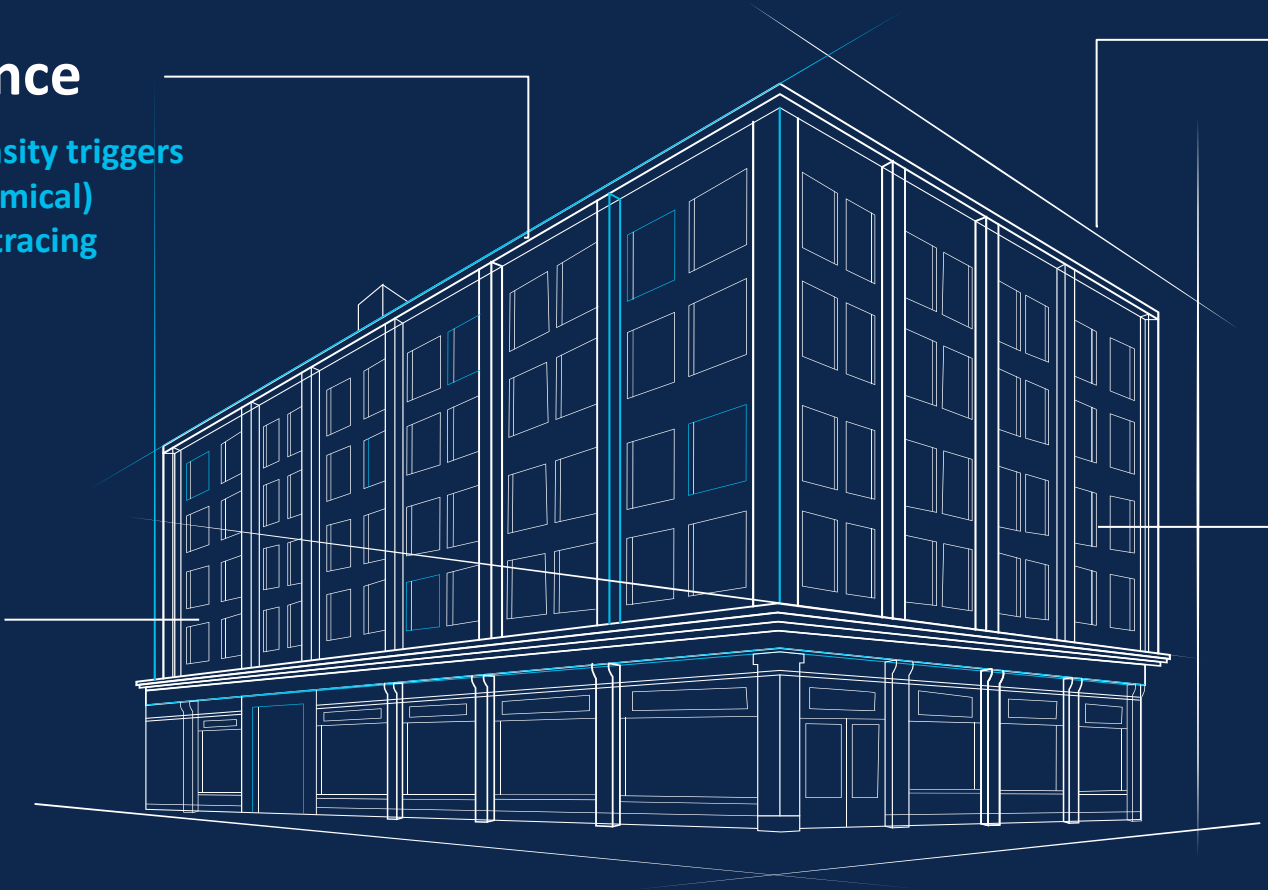
Industrial IOT

Indoor IOT at Cisco

Indoor IOT aka Smart Buildings

Safety & Compliance

- **Real time occupancy & Density triggers**
- **Safe Sterilization (UVC/Chemical)**
- **Proximity alerts & contact tracing**

Automation & Optimization

- **Environmental Monitoring**
- **Asset Tracking**
- **Energy Savings**

Space Utilization

- **Space occupancy & utilization**
- **Location Analytics**
- **Resource planning**

User Experience

- **Meeting room experience**
- **Hot desking**
- **Personalized environments**

Indoor IOT Use Cases

Asset Management

Locate valuable assets in real-time and monitor asset utilization

Room finding

Find, navigate to and schedule available conference rooms

Employee Safety

Keep employees safe with real time notifications & location updates

Environmental Monitoring

Monitor environmental conditions for sensitive assets and zones

Space Utilization

Allocate space based on occupancy and right-size your real estate portfolio
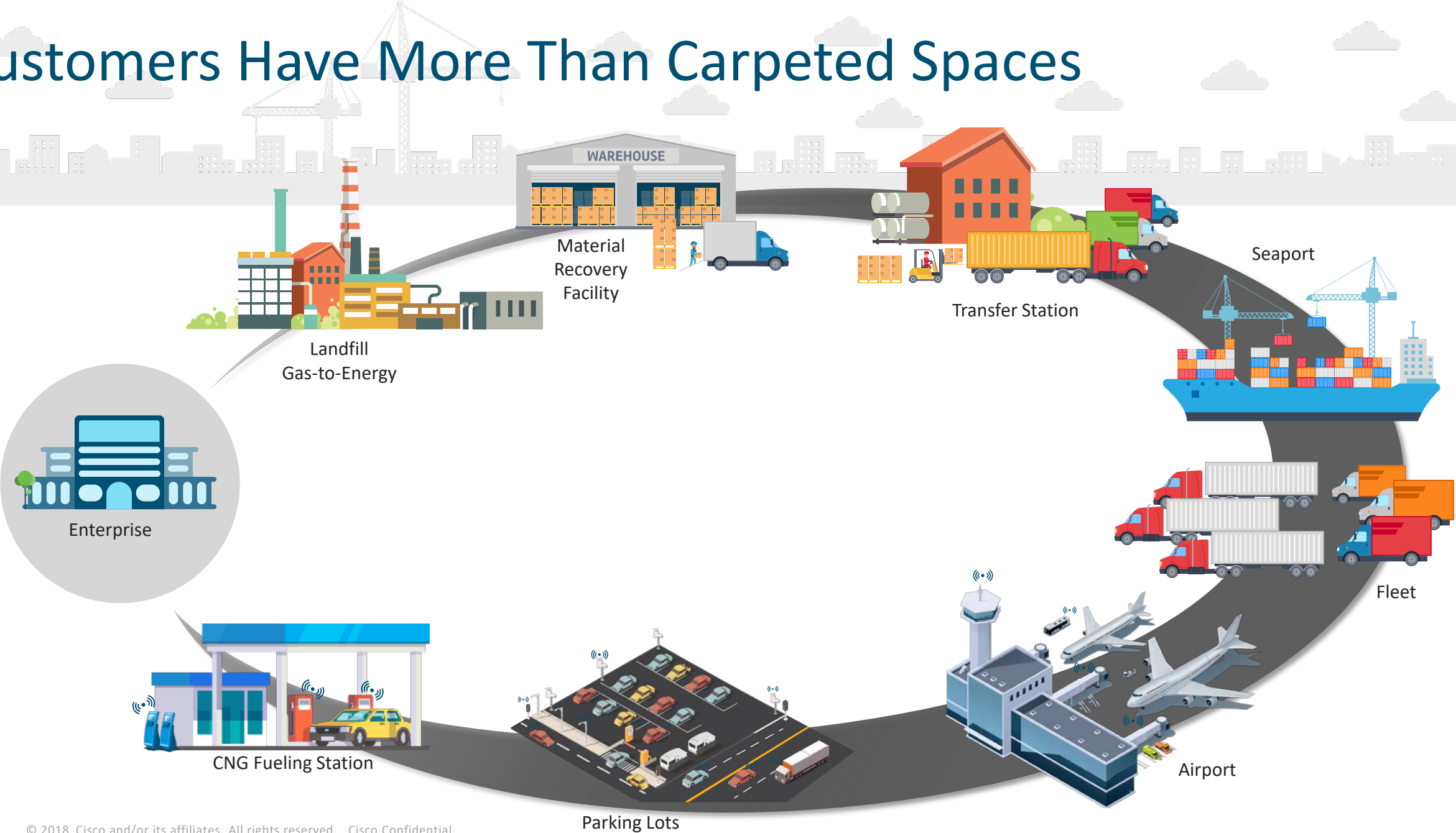
Work in Progress Tracking

Manage and track workflows for optimal efficiency and monitoring

Industrial IOT at Cisco

Customers Have More Than Carpeted Spaces

Enterprise

Landfill Gas-to-Energy

Material Recovery Facility

WAREHOUSE

Transfer Station

Seaport

Fleet

Airport

Parking Lots

CNG Fueling Station

Cities
Real-time traffic updates

Energy
Worker safety

Industrial IOT

Manufacturing
Predictive maintenance

Warehouses
Asset monitoring

Agenda

- How IOT is defined at Cisco

- Differences between IT and OT

- Common IOT use cases & How Cisco helps address these use cases
  - Extending networks with wireless
  - Secure Equipment Access
  - OT Network Security - Zero Trust / NAC outside of Enterprise Networks

- Quick Snapshot of the Cisco IOT portfolio

ENTERPRISES REQUIRE NETWORK CONNECTIVITY OUTDOORS
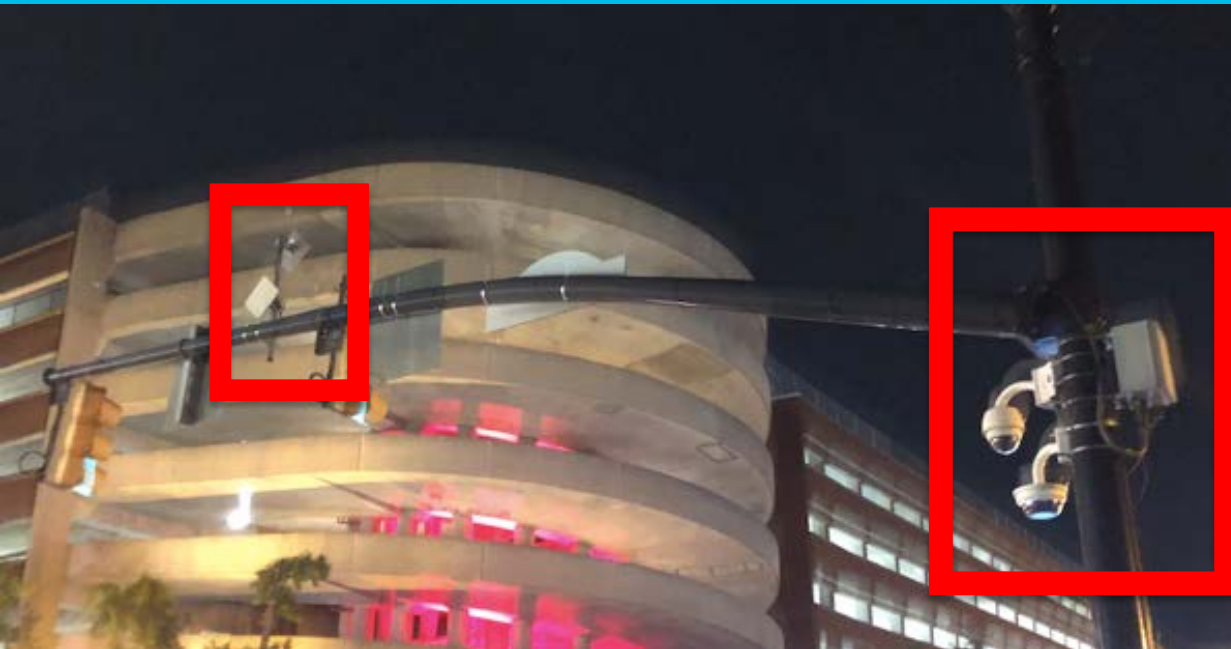
Challenges of extending wired technologies outside the enterprise building

Average costs of laying fiber is about
US$ 27,000 per mile

Building wiring costs
can range from
US$ 1 to US$ 6 per foot

Trenches and local authorizations extend fiber deployment time up to 8-18 months

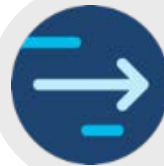# Wireless Backhaul Defined

Long range and high bandwidth connectivity
(up to 15 miles / 500 Mbps)

Fast and accurate handoff
(0ms handoff, up to 225 Mph)

Support for real-time sensitive traffic

Support fixed and mobile architectures

Parking lots, outdoor malls and campus environments

Enhance safety and security in outdoor spaces

Challenge

- To quickly deploy video protection in large outdoor areas
- Road works with fiber to collect cameras flow connection is the most expensive part of the project
- Road works extend the delivery time of the project

Solution highlights

- Easy and fast connectivity deployment with ultra-reliable low-latency wireless connectivity (Cisco Ultra-reliable Wireless Backhaul instead of fiber)
- Meraki MV smart cameras

Outcomes

- Easy and quick to install bundled solution
- No road works giving customer satisfaction of simple deployment
- Easy extension by adding cameras and Cisco Ultra-Reliable Wireless Backhaul in new areas

Temporary deployments
Enhance safety and security for festivals, races and other events

Challenge

- To quickly deploy video protection for temporary deployments such as festivals, races and other entertainment events
- Fiber connectivity not readily available
- Fiber deployment not justified due to temporary nature of deployment

Solution highlights

- Easy and fast connectivity deployment with ultra-reliable low-latency wireless connectivity (Cisco Ultra-reliable Wireless Backhaul instead of fiber)
- Meraki MV smart cameras

Outcomes

- Easy and quick to install bundled solution
- No road works giving customer satisfaction of simple deployment
- Easy extension by adding cameras and Cisco Ultra-Reliable Wireless Backhaul in new areas

Quick Demo

Agenda

- How IOT is defined at Cisco

- Differences between IT and OT

- Common IOT use cases & How Cisco helps address these use cases
  - Extending networks with wireless
  - Secure Equipment Access
  - OT Network Security - Zero Trust / NAC outside of Enterprise Networks

- Quick Snapshot of the Cisco IOT portfolio

Cisco IoT

Traditional Remote Access

Segmenting with Visibility & Policy Analytics
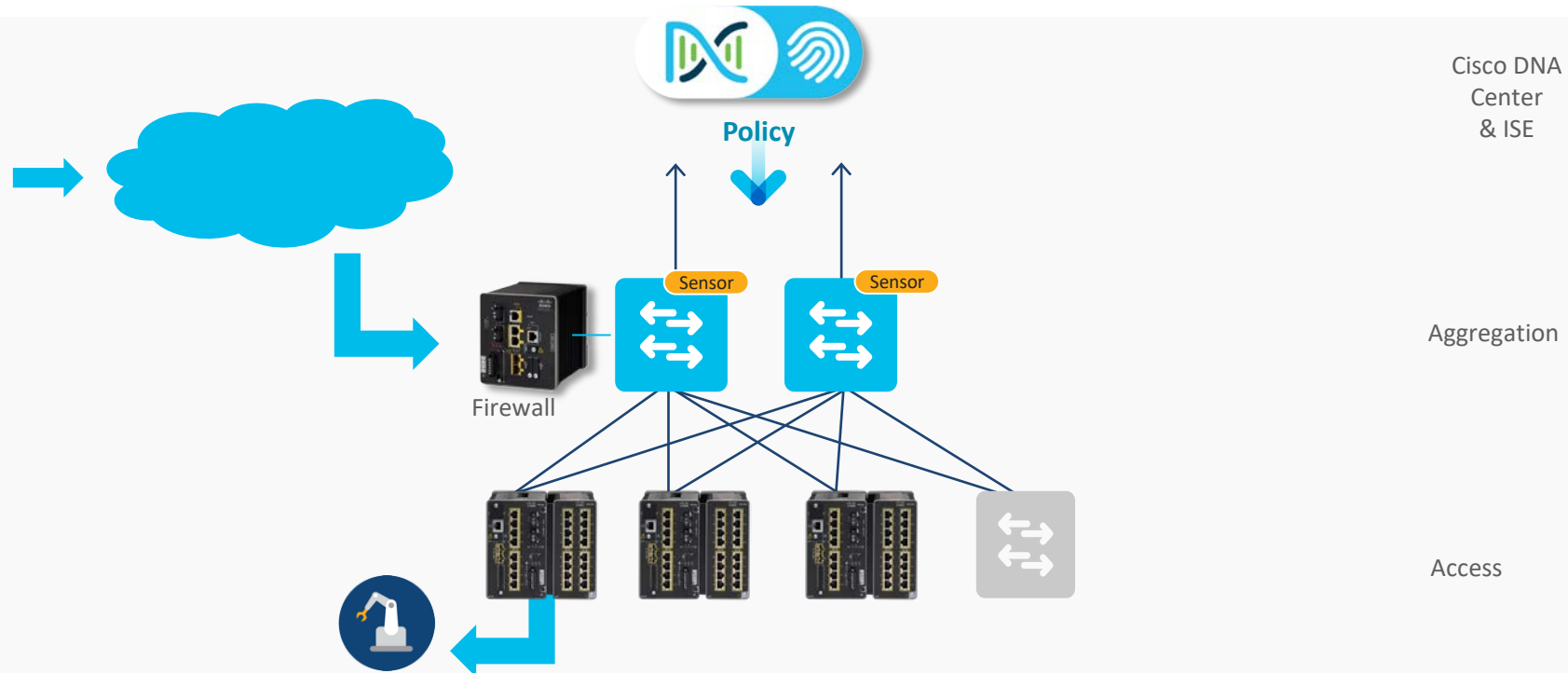
Cisco DNA Center & ISE

Policy

Sensor

Sensor

Aggregation

Firewall

Access

Traffic from endpoints like PLC, IO in industrial control loops is highly localized within a machine or cell

Cisco IoT

The Easy Button - Secure Equipment Access (SEA)

SEA on IoT Operations Dashboard

Remote Access User

From Anywhere on any Device

SEA
IoT Operation Dashboard

Enterprise Network

Site A

Meter-01

Site B

Robot-01

Cisco IoT

Quick Demo

Agenda

- How IOT is defined at Cisco

- Differences between IT and OT

- Common IOT use cases & How Cisco helps address these use cases
  - Extending networks with wireless
  - Secure Equipment Access
  - OT Network Security - Zero Trust / NAC outside of Enterprise Networks

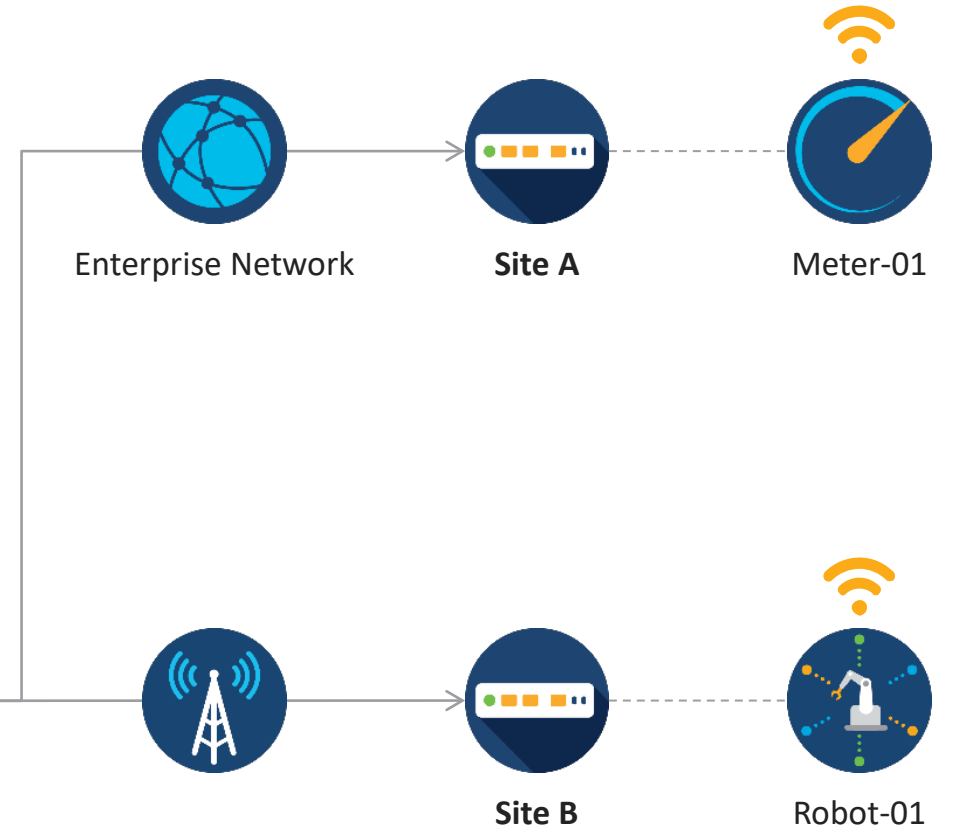- Quick Snapshot of the Cisco IOT portfolio

Cisco IoT

Extending Workplace Zero Trust to Industrial Settings

Endpoint
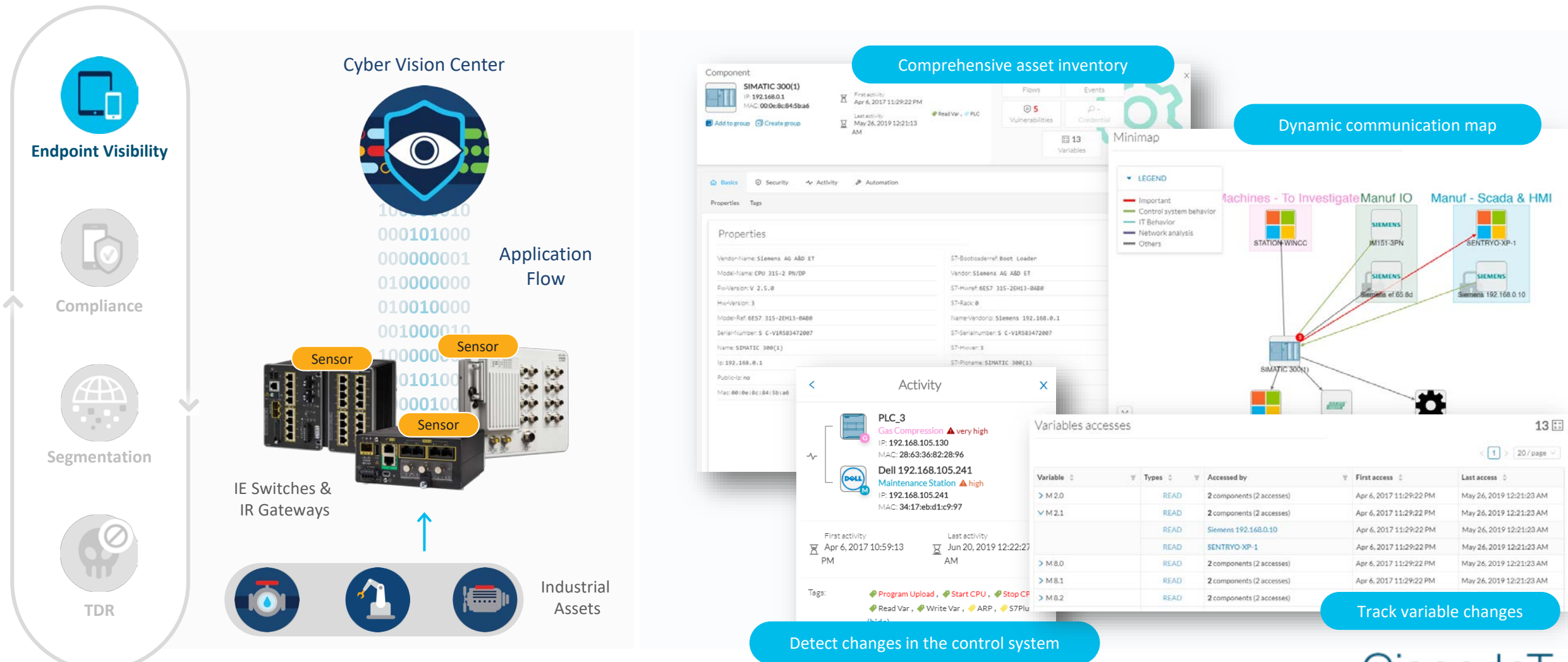Visibility

Endpoint
Compliance

Network
Segmentation

Threat Detection
& Response

Cisco IoT

Industrial Endpoint Visibility

Endpoint Visibility

Compliance

Segmentation

TDR

Industrial Control System device visibility based on application-level decoding of industrial protocol traffic and behavior modeling of industrial endpoints

Cisco IoT

Industrial Endpoint Visibility with Cyber Vision

Endpoint Visibility

Compliance

Segmentation

TDR

Cyber Vision Center

Application Flow

Sensor

Sensor

Sensor

IE Switches & IR Gateways

Industrial Assets

Comprehensive asset inventory

Dynamic communication map

Detect changes in the control system

Track variable changes

Cisco IoT

Segmentation

View application relationships to **group endpoints into zones** and **identify conduits** in Cyber Vision

Enable OT users to **dynamically map zones to scalable group tags** of pre-defined TrustSec policies built by IT in ISE

Visualize **traffic activity between scalable groups** in DNAC policy analytics

Deploy group segmentation policy with confidence once you are comfortable with the observed network behavior using DNAC Day-n templates

Endpoint Visibility

Compliance

Segmentation

TDR

Cisco IoT

Identify Zones and Conduits
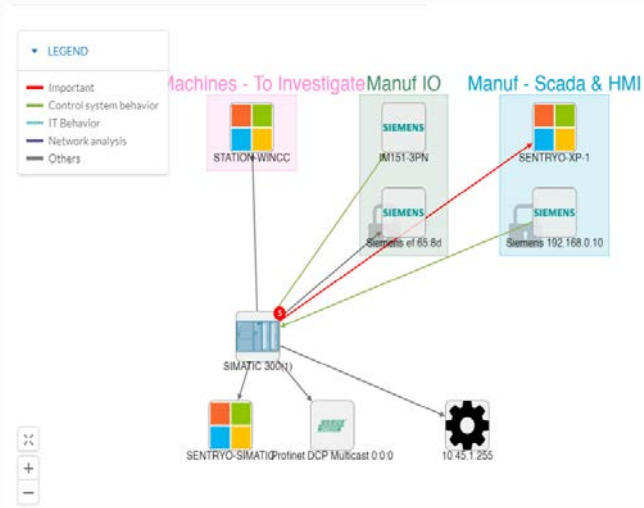

Endpoint Visibility
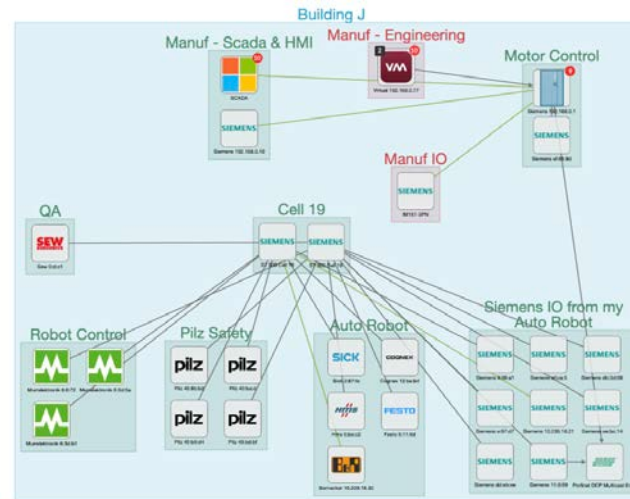
Compliance

Segmentation

TDR

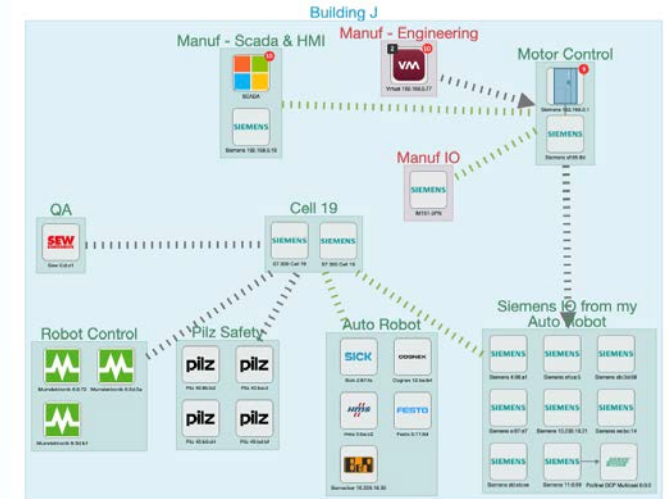**Identify Application Relationships**

Cyber Vision maps traffic flows between endpoints and provides application-level details within the flows

Group endpoints into Zones

Users can leverage these application relations to group endpoints to match the industrial processes they represent

Visualize Conduits between Zones

The traffic flows can be aggregated into conduits which can be used to inform segmentation policies

Cisco IoT

Dynamically map zones to scalable group tags

Cyber Vision Map View

	Cell 1	Cell 2	PLC	MES
Cell 1	✓	✗	✓	✗
Cell 2	✗	✓	✗	✗
PLC	✓	✓	✓	✓
MES	✗	✗	✓	✓

pxGrid

Cisco DNA Center & ISE

ISE profiles endpoints based on "Cell1" custom attribute and assigns SGT in AuthZ policy

RADIUS

Endpoint Visibility

Compliance

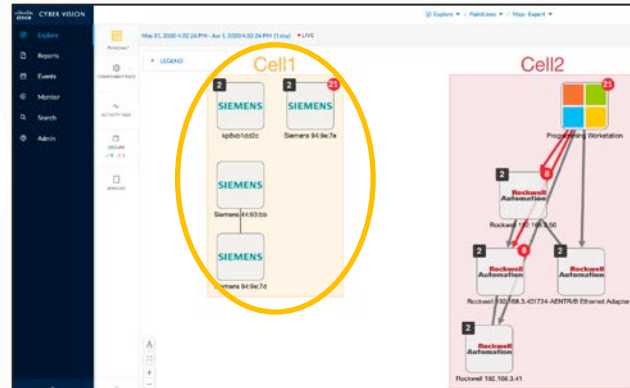**Segmentation**

TDR

1. OT users understands industrial processes

2. They have the context to group industrial endpoint belonging to a specific process / machine into zones

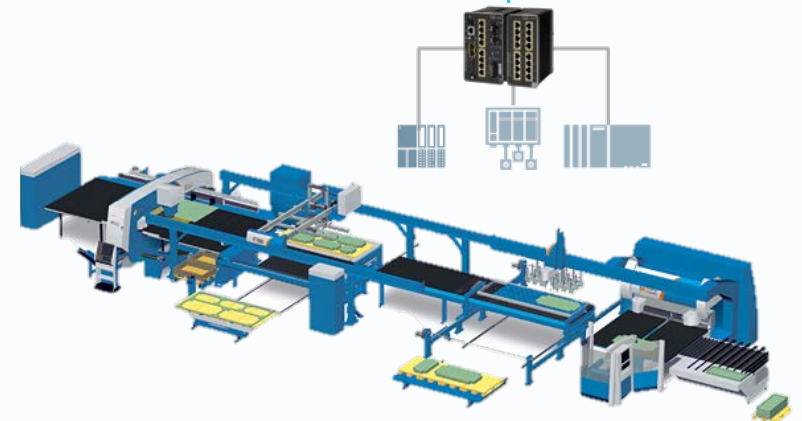3. Cyber Vision send pxGrid update with endpoint identities and group *"Cell1"* to ISE

Cisco IoT

Bringing it all Together
Segmenting with Visibility & Policy Analytics
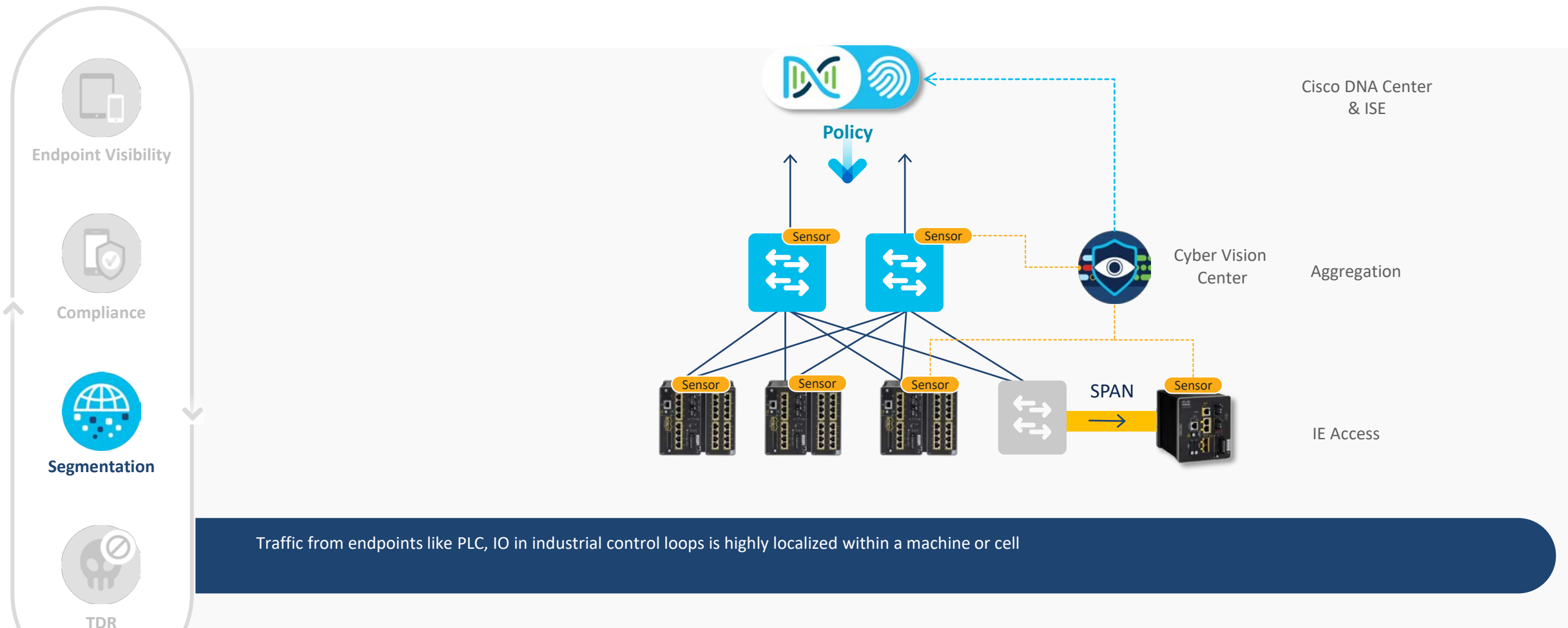
Traffic from endpoints like PLC, IO in industrial control loops is highly localized within a machine or cell

Cisco IoT

Quick Demo

Agenda

- How IOT is defined at Cisco

- Differences between IT and OT

- Common IOT use cases & How Cisco helps address these use cases
  - Extending networks with wireless
  - Secure Equipment Access
  - OT Network Security - Zero Trust / NAC outside of Enterprise Networks

- Quick Snapshot of the Cisco IOT portfolio

Cisco IoT

Cisco Industrial IOT Portfolio Overview

Industrial switching
IE 1K, 2K, 3K, 3200, 3300, 3400, 3400H, 4K, 5K, CGS

IoT gateways
819-MNA, IR807, IR809, IR829, IR1101

Industrial routing
CGR 1000, CGR 2000

Resilient mesh
IR500, DevNet

LoRaWAN
IXM Gateway

Fluidmesh
PTP/PTMP Links

Endo

Mobi

Volo
Endo
Mobi
Fluidity

Industrial wifi
IW3702
IW6300, ESW6300

Embedded IoT
ESS, ESR, EW

Edge Computing
IC3000
IoX, Edge Intelligence

Automation
Field Network Director
Industrial Network Director
Gateway Manager

IoT Security
Cybervision
ISA 3000