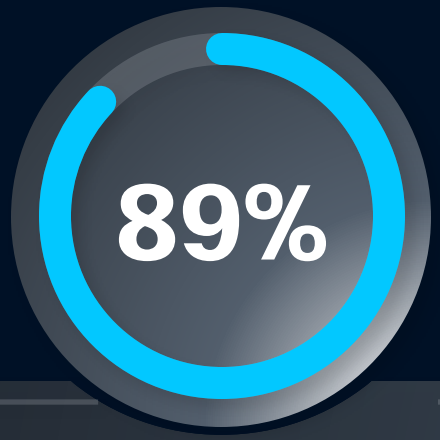
Future Proofing Industrial Networks for AI & Cybersecurity

Blong Moua
Industrial IoT Solutions Specialist
Cisco Systems, Inc.

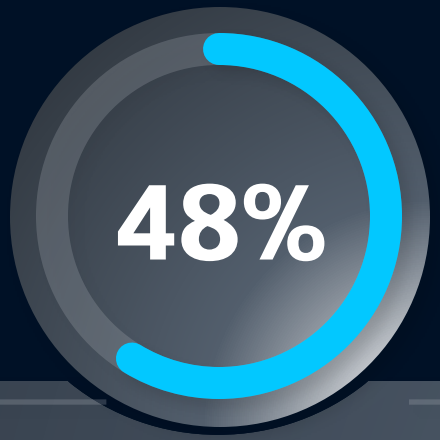
OC Tech Day October 2025

What Manufacturers are telling us

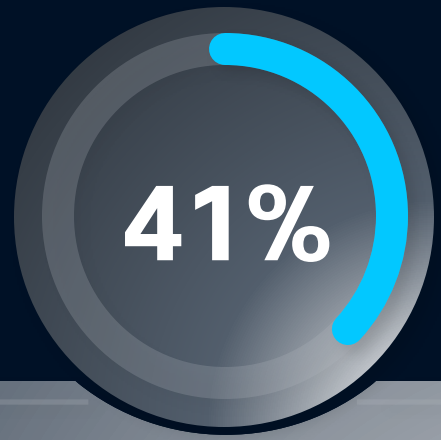
Results from our Voice of the Customer Survey with 1000+ participants



Describe **cybersecurity compliance as critical** for their operational network[1]

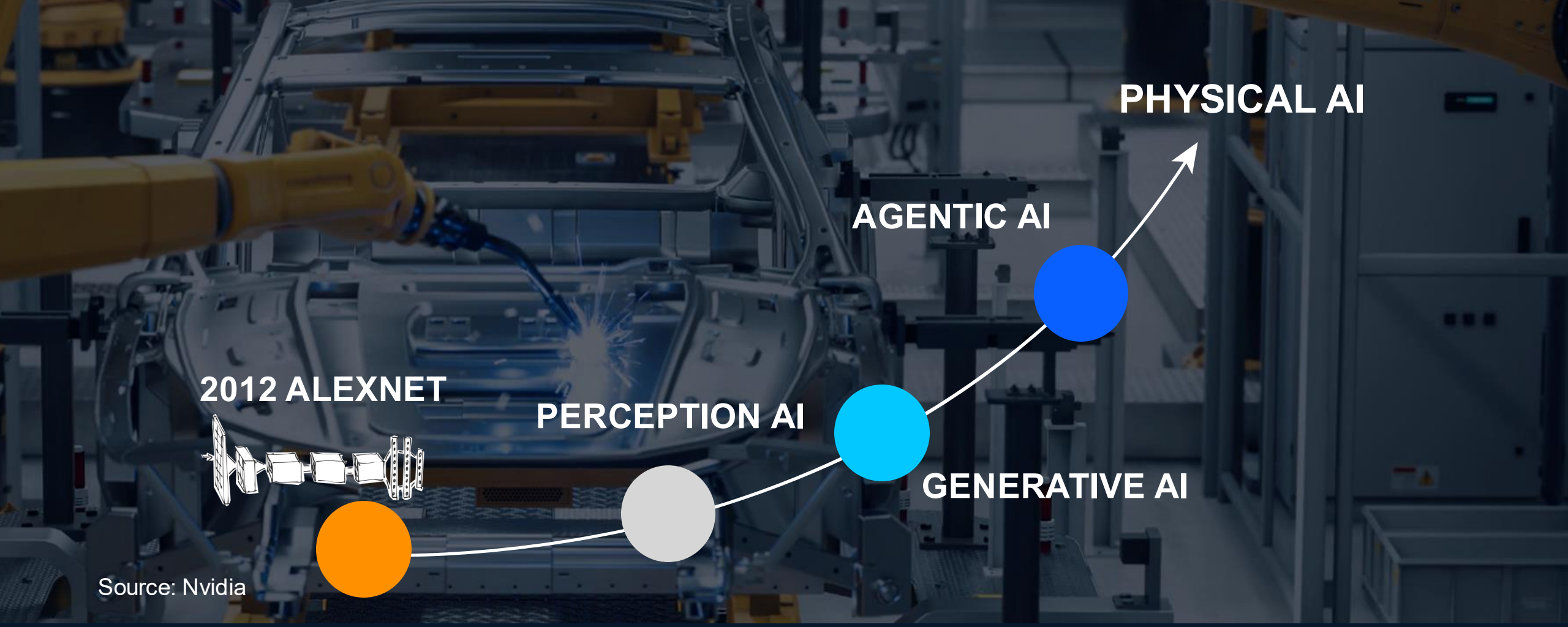


Say AI will have the greatest impact on industrial networking over the next 5 years[1]



of IT and OT teams are working independently[1]

1. Cisco, Cisco 2024 State of Industrial Networking Report, 2024



Physical AI evolution will transform manufacturing and industrial verticals

AI Use Cases in Manufacturing

Machine vision

Making machines smarter
Improving production quality & safety
AI models to see beyond visible

Industrial control virtualization

PLCs and RTUs in virtual machines
Decoupling machine software and hardware to save opex and capex

Industrial data collection

Digital twins & Predictive models
Preventative maintenance
Quality & Sustainability goals

Tele-remote operations

Operating remote machines in harsh environments (mines, ports, oil & gas)
Increasing safety & productivity

AI robotics and cobots

Using AI to control robots
Moving CPU/GPU workload to datacenter for elasticity and scale

Autonomous vehicles

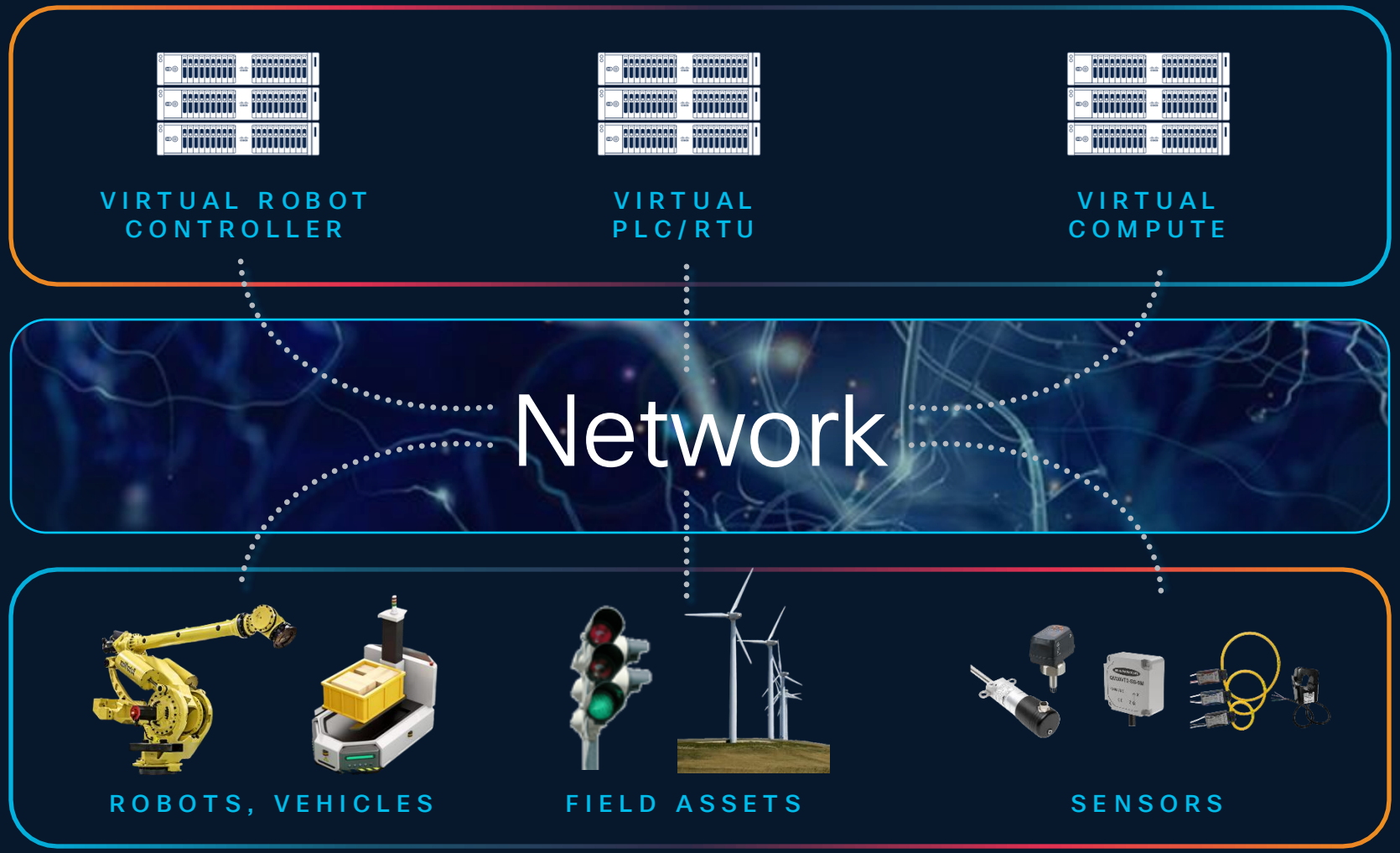
Enhancing productivity in mines, warehouses, manufacturing, etc.
Operations scalability & agility

The Infrastructure is Key to Unlocking AI Potential

Brains
in the data center

Nervous system
is the network

Physical components
in the field



Cisco powers how people and technology work together across the physical and digital worlds

AI-ready data centers

Transform data centers to power AI workloads anywhere

Public and private clouds, on-premises, edge

Future-proofed workplaces

Modernize everywhere people work and serve customers

Campuses, branches, factories, homes, cars, hospitals, stadiums, hotels, and beyond

Digital resilience

Keep your organization secure, reliable, and performing with game-changing security, assurance, and observability across the entire digital footprint

Accelerated by Cisco AI

Helping industries digitize by bringing IT to the OT world

Industrial Strength

Purpose built for harsh/outdoor OT environments

Enterprise Grade

Leverage existing knowledge and investments

Built for harsh and outdoor environments

Industry use-cases and certifications

Industrial protocol support and integrations

Industry-leading end-to-end Cisco security architecture

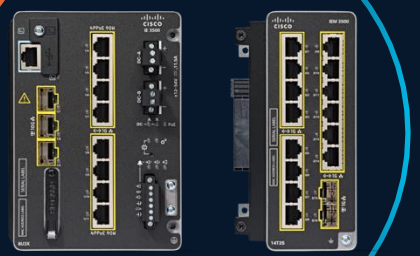
Less complexity at scale: one network architecture

Consistent commercial model – software, licensing

Common OS - IOS XE, Common Automation - Catalyst Center, SD-WAN Manager, Meraki dashboard
Architectural & workforce extensibility

Future proof networking for new industrial use cases

NEW!



IE3500 Rugged Series Switch and Expansion Module

NEW!

IE3500H Heavy Duty Series Switch

NEW!

IE3100H Heavy Duty Series Switch

NEW!

IE3100-4PPoE

NEW!

IE9300- Mix Port

19 new industrial switches enabling new industrial automation use cases

IE3500 Series Switches

Base

IE-3500-8T3S
8x 1GE ports
3x 1GE SFP ports

IE-3500-8P3S
8x PoE/PoE+
3x 1GE SFP ports
360W PoE Budget

Advance

IE-3505-8T3S
8x 1GE ports & 3x 1GE SFP ports
HSR/PRP/DLR

IE-3505-8P3S
8x PoE/PoE+ 3x 1GE SFP ports
HSR/PRP/DLR
480W PoE budget

10G/4PPoE

IE-3500-8T3X
8x 1GE ports
3x 10G SFP ports

IE-3500-8U3X
8x PoE/PoE+/4PPoE (90W)
3x 10G SFP ports
480W PoE budget

Expansion Modules

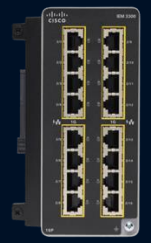
IEM-3500-6T2S
6x 1GE ports
2x 1GE SFP ports

IEM-3500-8T
8x 1GE ports

IEM-3500-8P
8x PoE/PoE+

IEM-3500-8S
8x 1GE SFP

IEM-3500-14T2S
14x 1GE ports
2x 1GE SFP ports



IEM-3500-16T
16x 1GE ports

IEM-3500-16P
16x PoE/PoE+

IEM-3500-4MU
4x 2.5G
PoE/PoE+/
4PPoE (90W)

IE3500H Heavy Duty Series Switches

PoE

IE-3500H-14P2T

2x 1GE ports
14x 1GE PoE ports
240W PoE Budget

IE-3500H-12P2MU2X

2x 10G SFP
2x 2.5G PoE/PoE+/4PPoE (60W)
12x GE PoE/PoE+
240W PoE Budget

FE w/ GE Uplinks

IE-3500H-12FT4T

12x FE D Code ports
4x 1GE X Code ports

IE-3500H-20FT4T

20x FE D Code ports
4x 1GE X Code ports

Full GE

IE-3500H-8T

8x 1GE port
M12 X-Code

IE-3500H-16T

16x 1GE ports
M12 X-Code

IE-3500H-24T

24x 1GE ports
M12 X-Code

Adv.

IE-3505H-16T

16x 1GE X-Code ports
HSR/PRP/DLR

IE3100 Series Switches

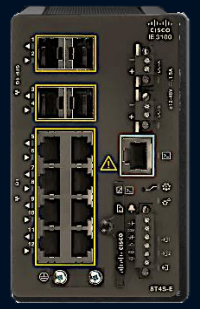
IE3100 Base

IE-3100-4T2S
4x 1GE ports
2x 1GE SFP ports

IE-3100-8T2C
8x 1GE ports
2x 1GE Combo ports

IE-3105-8T2C
8x 1GE ports
2x 1GE Combo ports

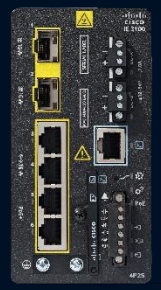
IE-3100-18T2S
18x 1GE ports
2x 1GE Combo ports



IE-3100-8T4S
8x 1GE ports
4x 1GE SFP ports

IE-3105-18T2C
18x 1GE ports
2x 1GE Combo ports

IE3100 PoE

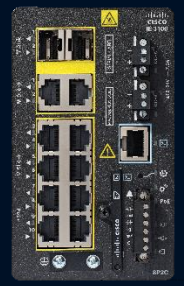


IE-3100-4P2S
4x PoE/PoE+
2x 1GE SFP ports
120W PoE Budget

NEW!

IE-3100-3P1U2S
3x PoE/PoE+, 1x 4PPoE (90W)
2x 1GE SFP ports
120W PoE B

NEW!



IE-3100-8P2C
8x PoE/PoE+
2x 1GE Combo ports
240W PoE Budget

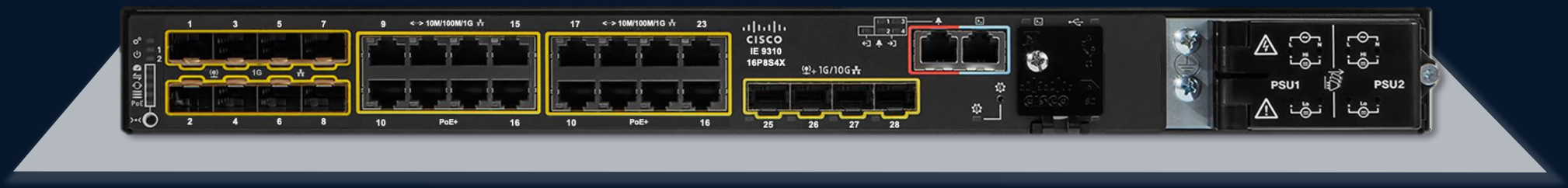
IE-3100-6P2U2C
6x PoE/PoE+, 2x 4PPoE (90W)
2x 1GE Combo ports
240W PoE Budget

IP67

IE-3100H-6FT2T
6x FE ports (M12 D-Code)
2x 1GE ports (M12 X-Code)

IE-3100H-8T
8x 1GE ports (M12 X-Code)

New IE9300 Series with Mixed Ports



Comprehensive connectivity

8x 1GE SFP plus 4x 10G SFP uplinks
16x 1GE with PoE/PoE+

High performance networking

Enterprise-grade Cisco silicon for fiber ring aggregation and high throughput

Cyber resilient

Cyber visibility, zero-trust enforcement, and observability built-in

The most versatile rugged rackmount switch for industrial settings where copper and fiber are needed

IE9300 Series Switches

IE-9310-26S2C

24x 1GE SFP ports (downlinks)
2x 1GE combo ports
4x 1GE SFP ports (uplinks)

IE-9320-24T4X

24x 1GE ports
4x 10G SFP ports
Stackable

IE-9320-24P4S

24x 1GE with PoE/PoE+
Up to 480W PoE budget
4x 1GE SFP ports
Stackable

IE-9320-24P4X

24x 1GE with PoE/PoE+
4x 10G SFP ports
Up to 720W PoE budget
Stackable

IE-9320-26S2C

26x 1GE SFP ports
2x 1GE combo ports
Stackable

IE-9320-22S2C4X

22x 1GE SFP, 4x 10G SFP
2x 1GE combo ports
Timing input
Conformal coating
Stackable

IE-9320-16P8U4X

8x mGig with 90W 4-pair PoE
16x 1GE with PoE/PoE+ ports
Up to 720W PoE budget
4x 10G SFP ports
Stackable

NEW!

IE-9310-16P8S4X

16x 1GE with PoE/PoE+ ports
8x 1GE SFP ports
Up to 480W PoE budget
4x 10G SFP ports

Unified Wi-Fi and URWB

Ultra-Reliable Wireless Backhaul

- Zero packet loss, seamless handoffs
- Near-zero latency (<10 ms)
- Uninterrupted connectivity

Unleash new use cases

Simultaneous Wi-Fi and URWB operation in the same AP, eliminating the need for different wireless infrastructures.

Get ultra reliable, low-latency mobility

Wireless technology you're familiar with, supporting fast mobility, without the cost and complexity of licensed spectrum.

Built AI-ready wireless infrastructure

Seamlessly connect critical industrial machines across indoor, outdoor, and industrial settings to drive success.

Indoor, Outdoor and Industrial Wireless

Wi-Fi 7

CW9176I,
CW9176D1

CW9178I

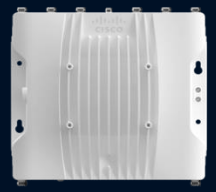
Wi-Fi 6E

CW9136I

CW9166I,
CW9166D1

IW9165E

IW9165D



IW9167E
IW9167E-HZ

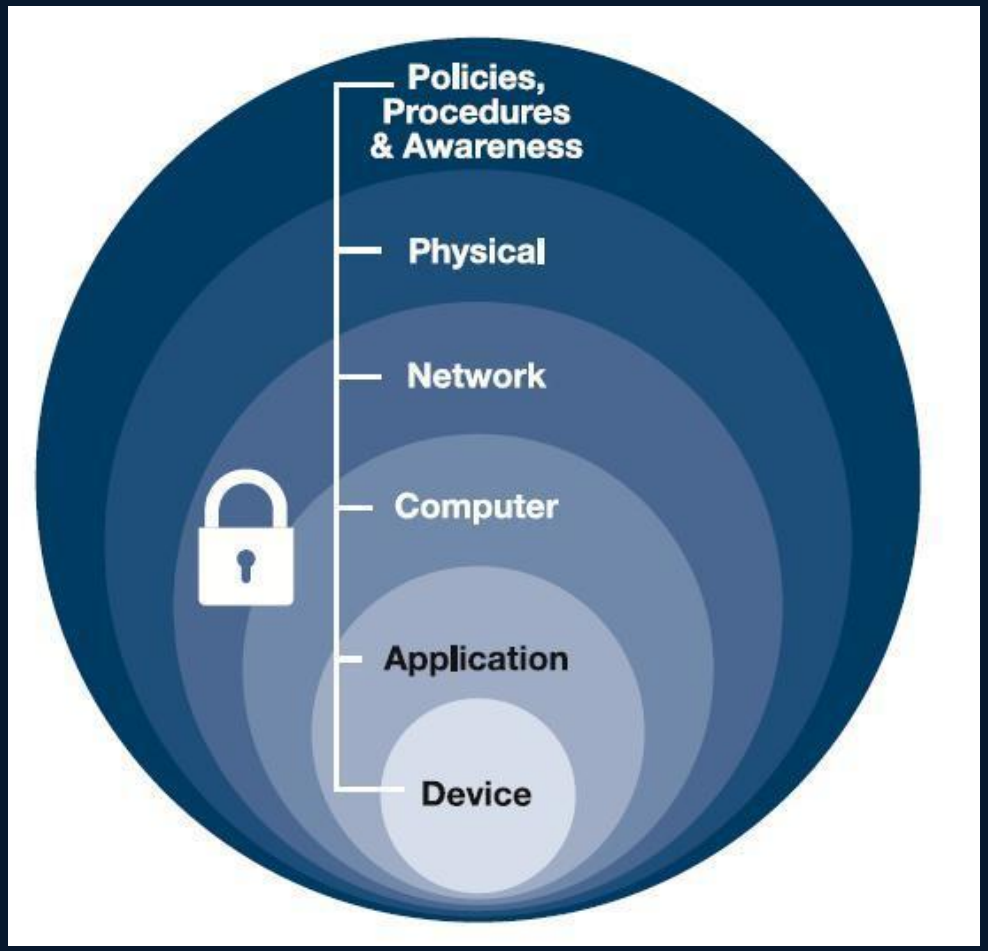
IW9167I

Wi-Fi 6

C9130
(AXE, AXI)

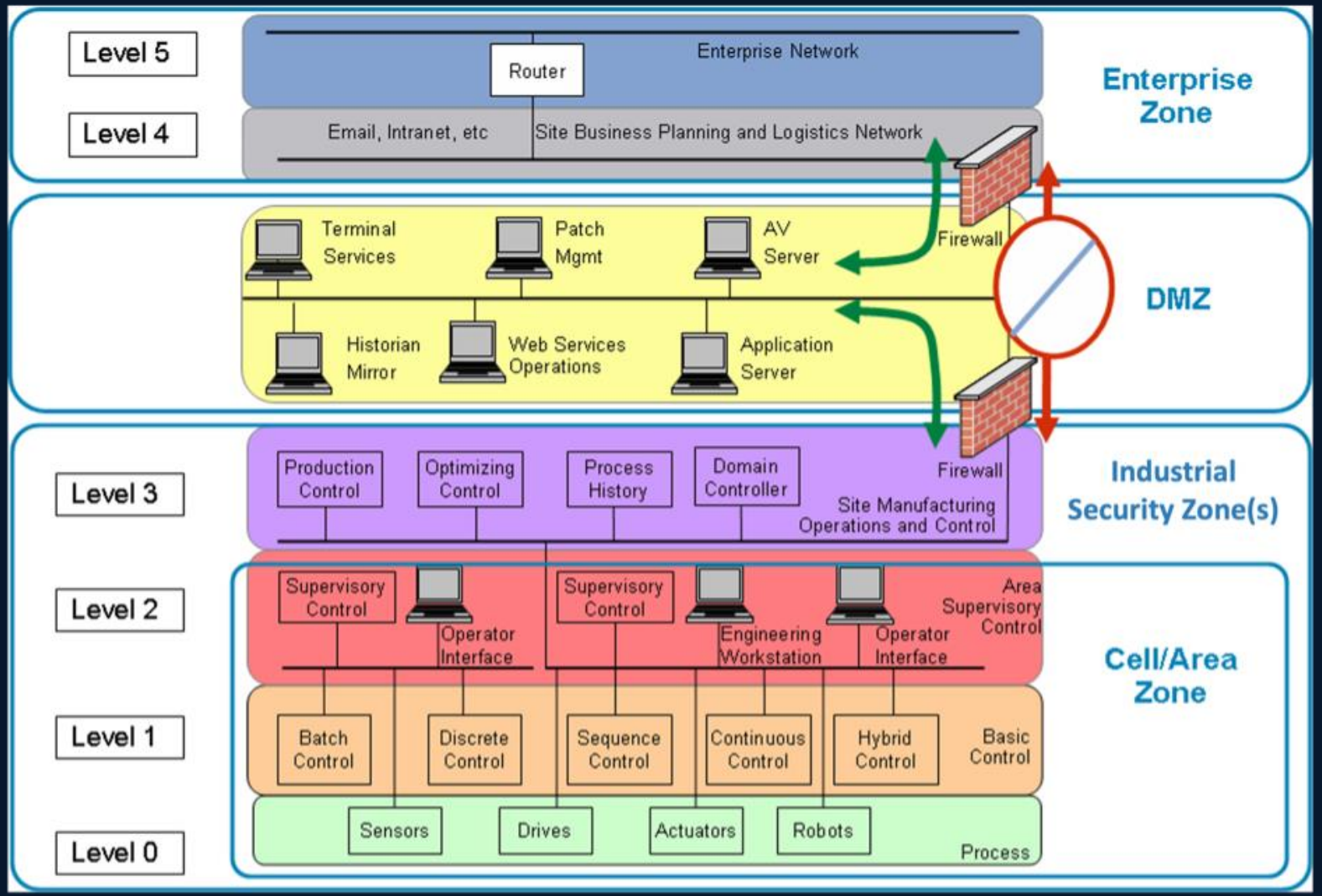
C9124
(AXE, AXI, AXD)

Defense in Depth

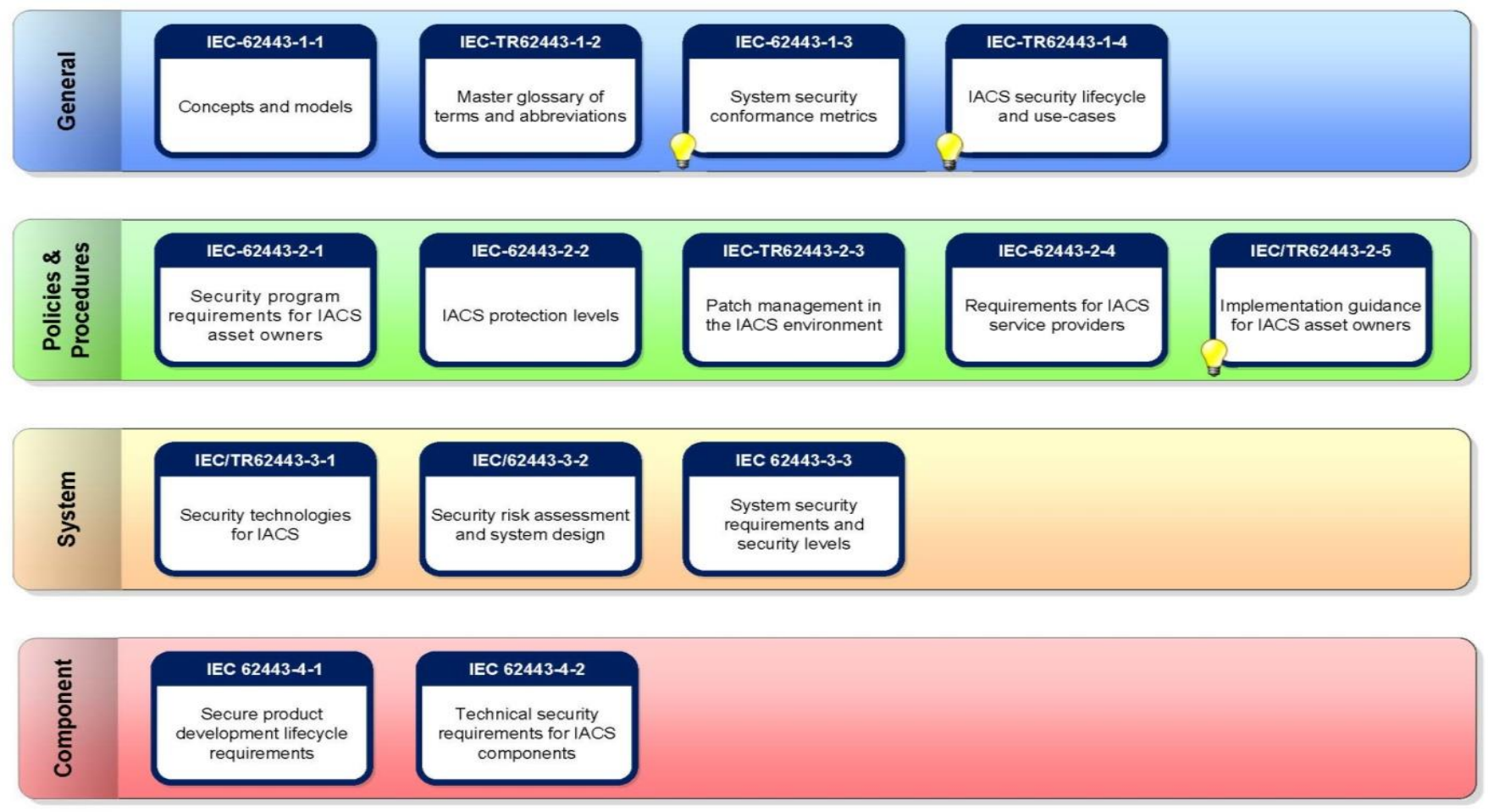


NIST Cybersecurity Framework

Purdue Model



IEC 62433

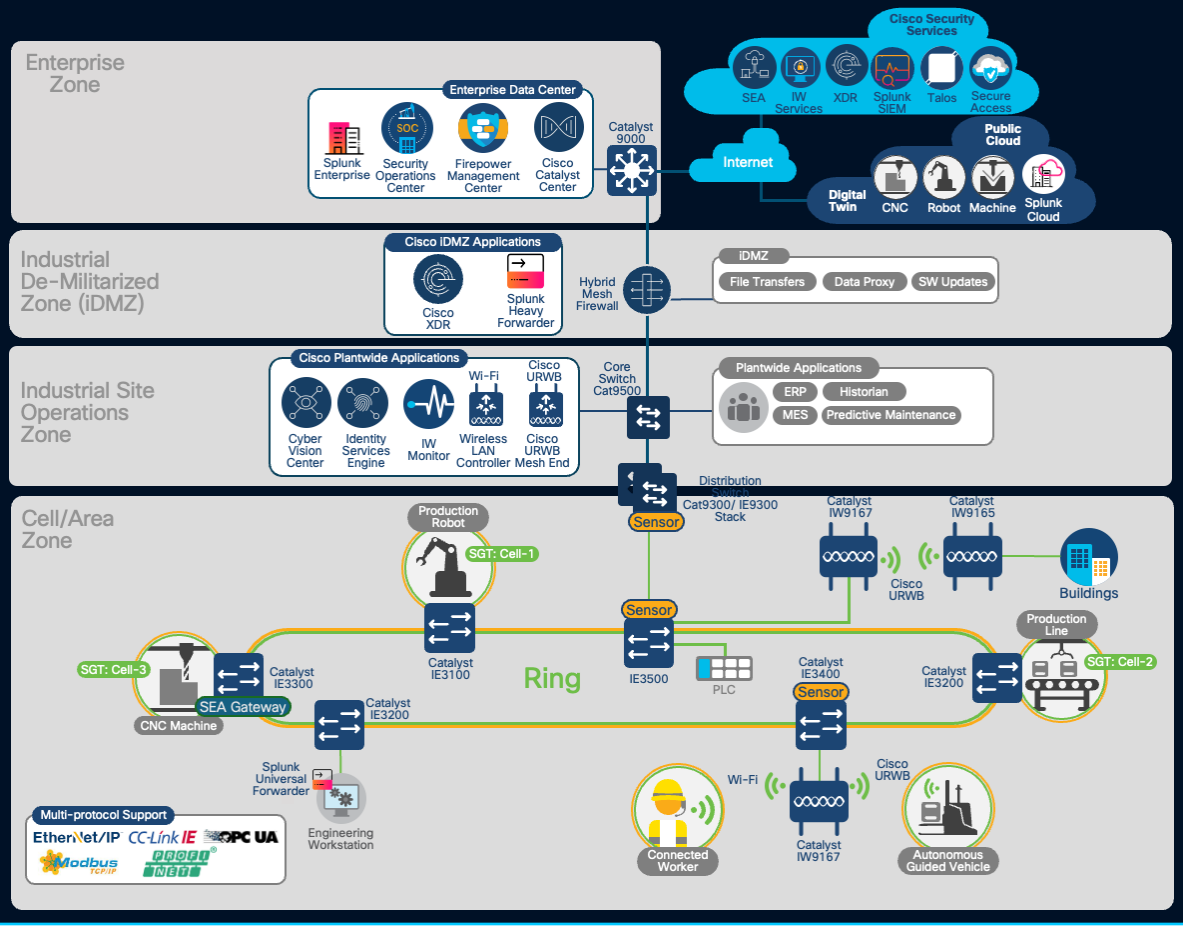


Cisco Validated Design for Manufacturing

Cisco Validated Design

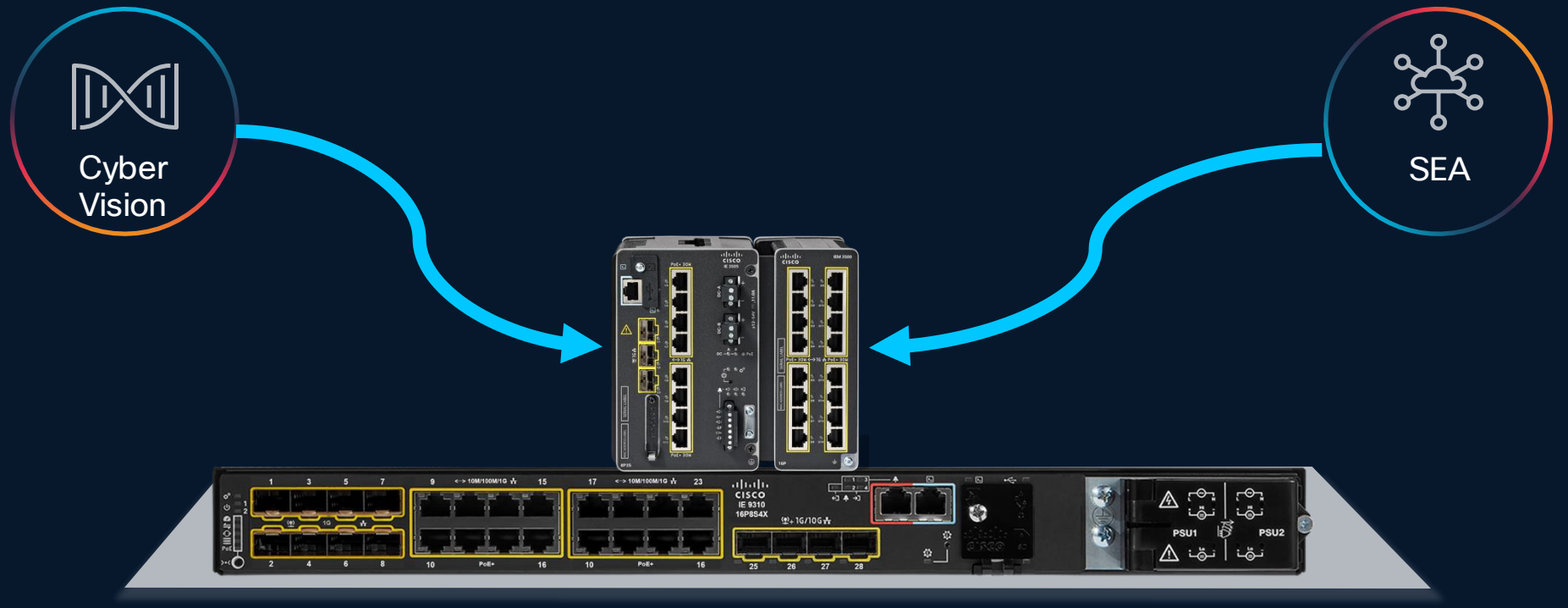
Technical blueprints and architectures, tested and proven, enabling standardization across the network

- Deploy secure network infrastructure
- OT asset visibility, communication patterns, and security risks
- Deploy security segmentation policy based on IEC-62443
- IT-defined & OT utilized secure remote access
- Threat Detection & Response by integrating into SOC operations
- Secure operations by applying consistent policies and SW versions with Catalyst Center



Proven to work with: Rockwell Automation SIEMENS Schneider Electric MITSUBISHI ELECTRIC

Cisco Cyber Vision & Secure Equipment Access



Cisco Cyber Vision

Visibility

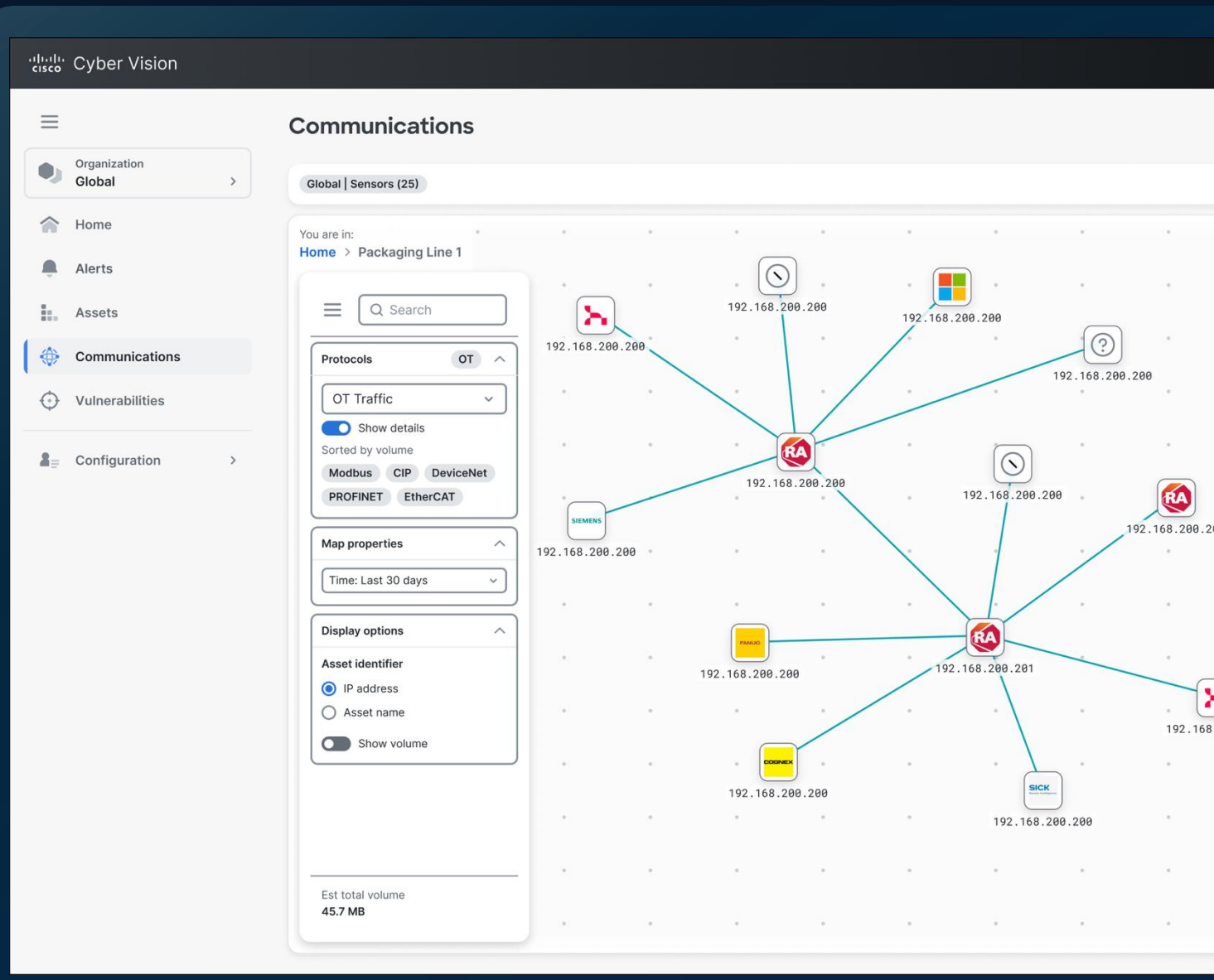
OT asset inventory
Communication patterns

Security Posture

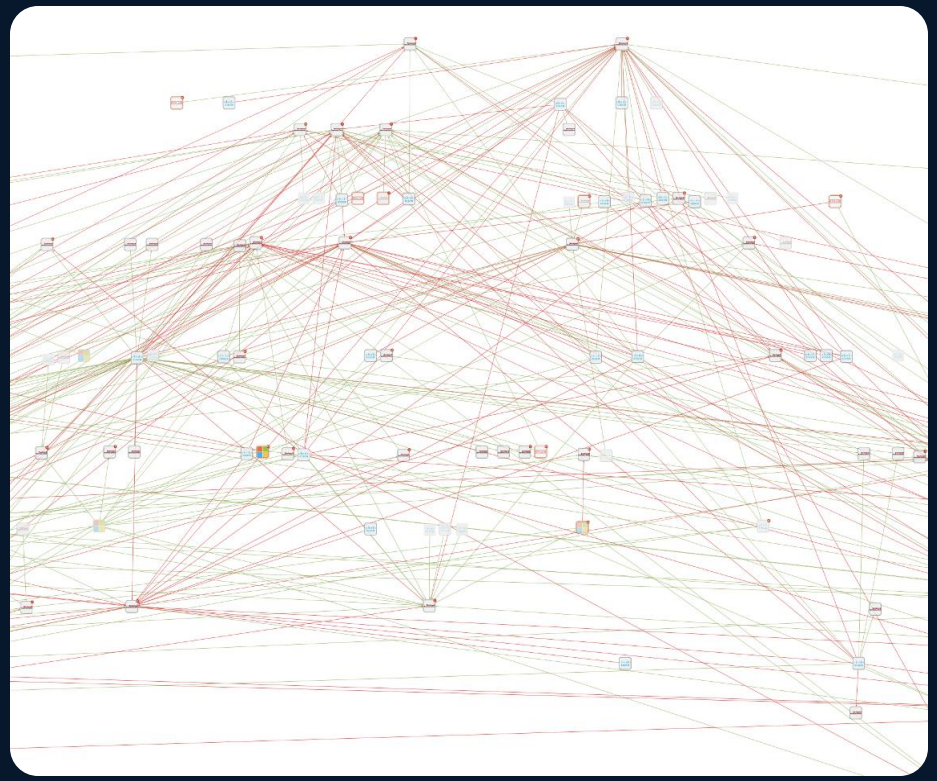
Device vulnerabilities
Risk scoring

Zone Segmentation

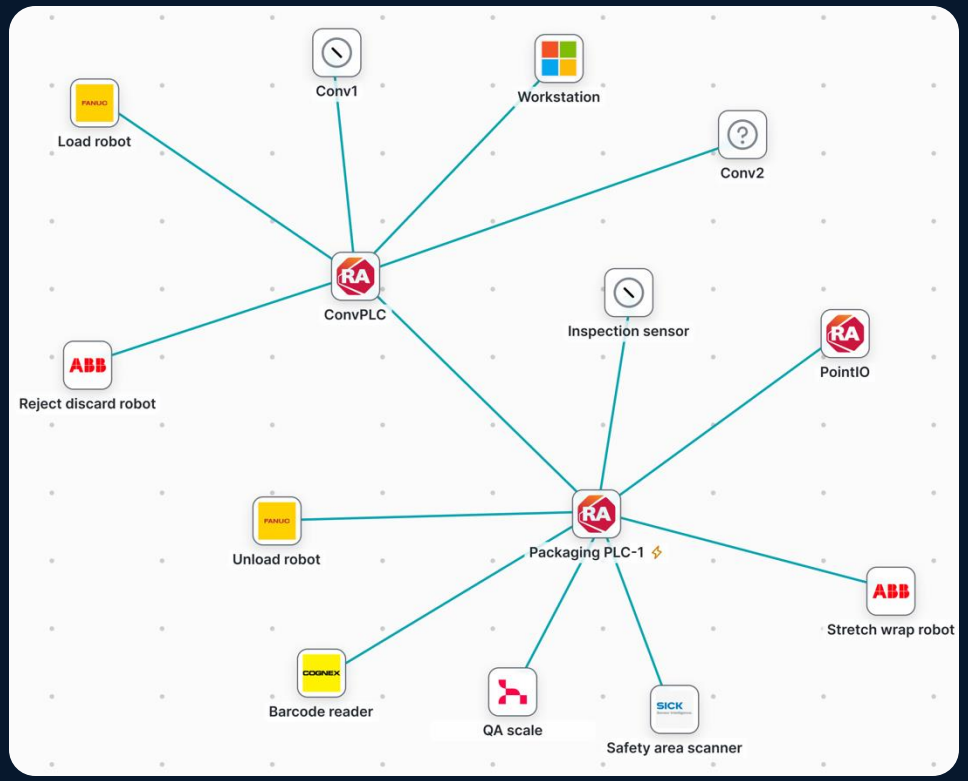
Automate segmentation below the IDMZ to protect operations



Grouping Assets to Reflect Production Processes



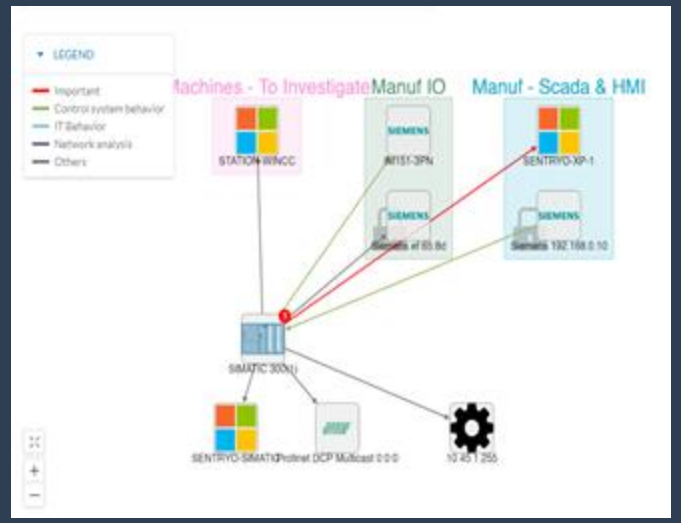
OT asset inventory highlights flat, unsegmented networks



Auto-grouping automatically creates security zones to drive network segmentation

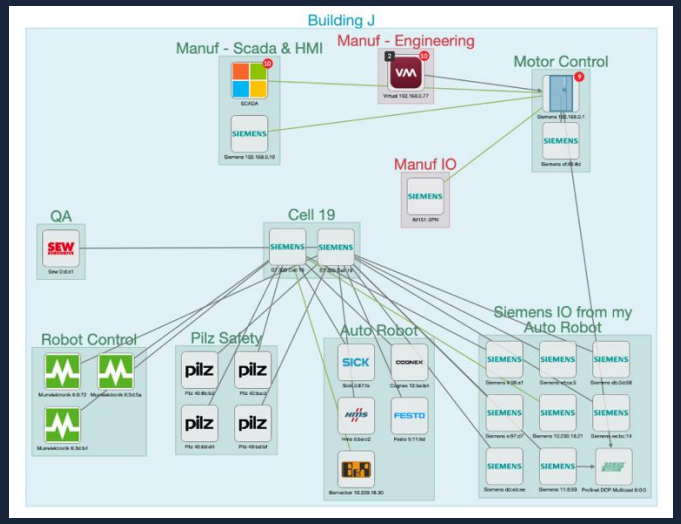
IEC 62443 Identify Zones and Conduits

Identify Application Relationships



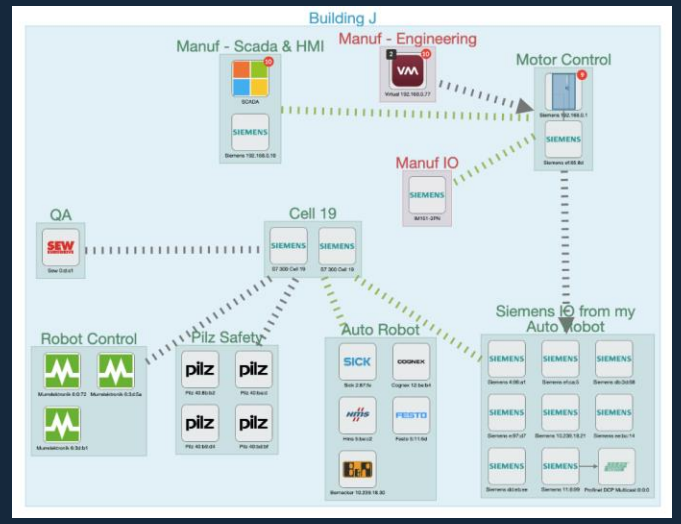
Cyber Vision maps traffic flows between endpoints and provides application-level details within the flows

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

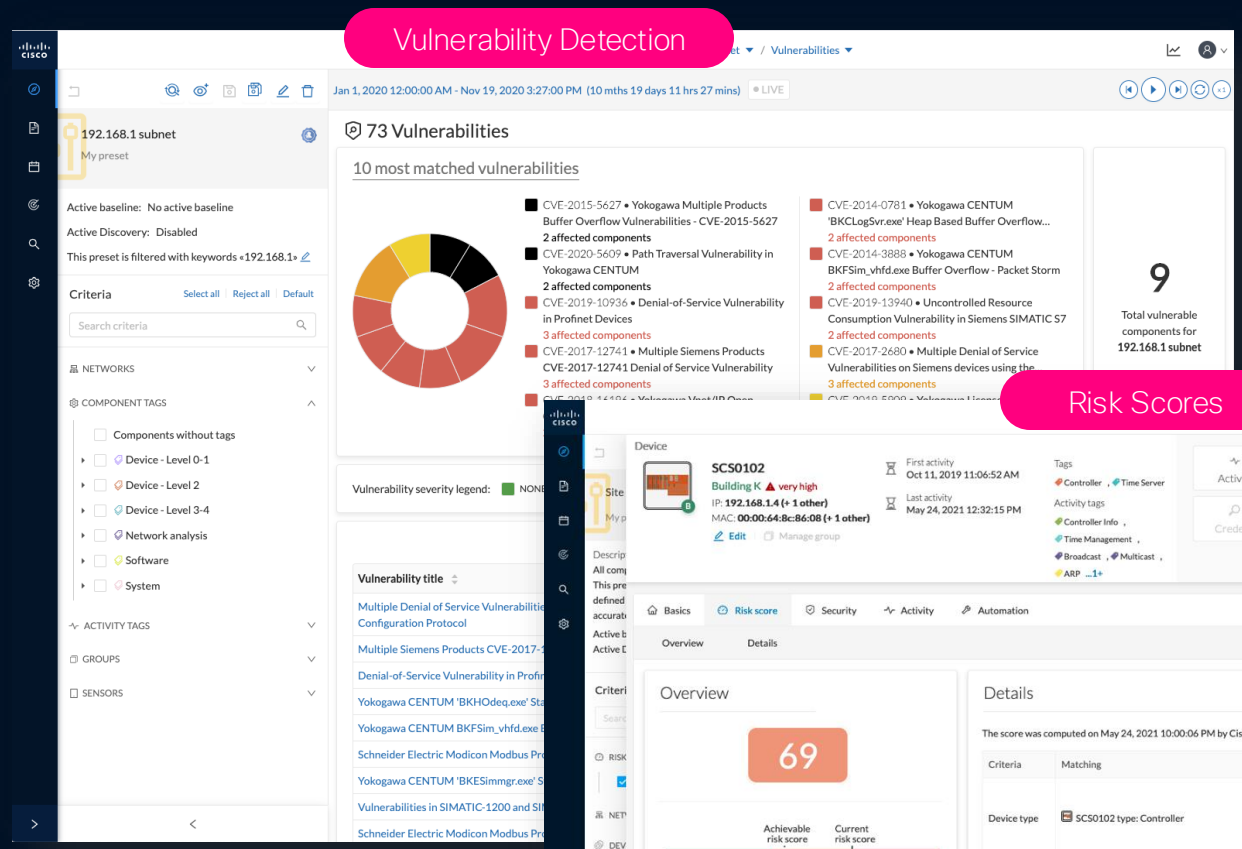
Security Posture

Vulnerability Detection

Identify known asset vulnerabilities so you can patch them before they are exploited

Risk Scoring

Asset risk scoring based on impact and likelihood to help you improve compliance



Detecting Abnormal Behaviors

Detect deviations from baselines

- -New and modified assets
- -New activities between assets
- -Variable changes
- -Program modifications

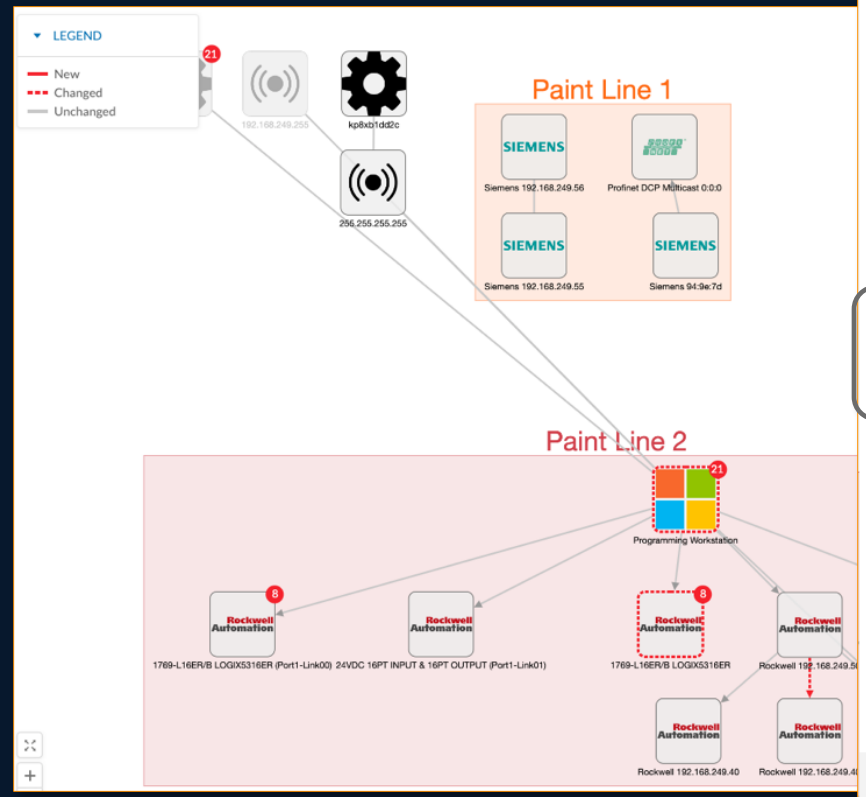
Multiple baselines for multiple states

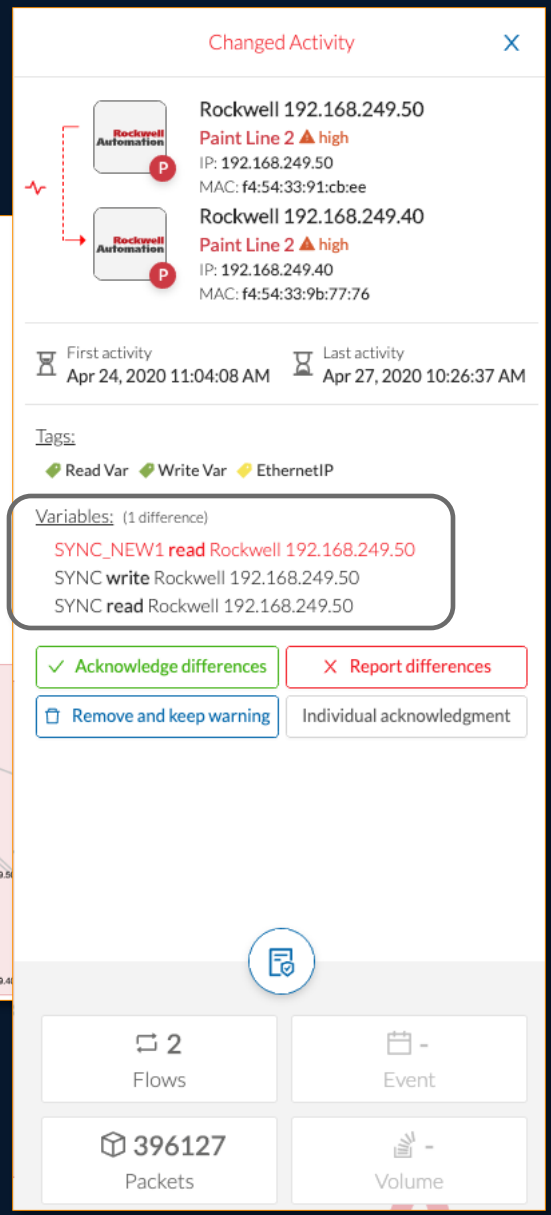
- -Reduces false positives

Response options

- -Acknowledge to modify the baseline
- -Report to provide context in investigations

Send events to firewall, SIEM, etc., to respond





Cisco Cyber Vision Portfolio

Cyber Vision Center

Hardware Appliance
UCS based servers with Hardware RAID

CV-CNTR-M6N
- 24 core CPU
- 128 GB RAM
- 3.2TB drives

Software Appliance
Virtual Machines

VMWare ESXi OVA

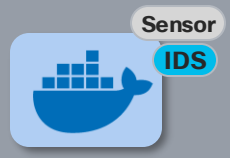
Hyper-V VHD

Minimum requirements
Intel Xeon, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Minimum requirements
Intel Xeon, 10 cores
32GB RAM and 1TB SSD
1 or 2 network interfaces

Cyber Vision Sensors

IC3000 Industrial Compute



Docker Sensor
x86 or ARM64 Compute

Hardware Sensor
(SPAN based to support brownfield)

Access Switch
IE-3300
IE-3400
IE-3500

Access Switch
IE-3400HD
IE-3500HD

Core/Agg
IE9300

Core/Agg
C9300/C9400

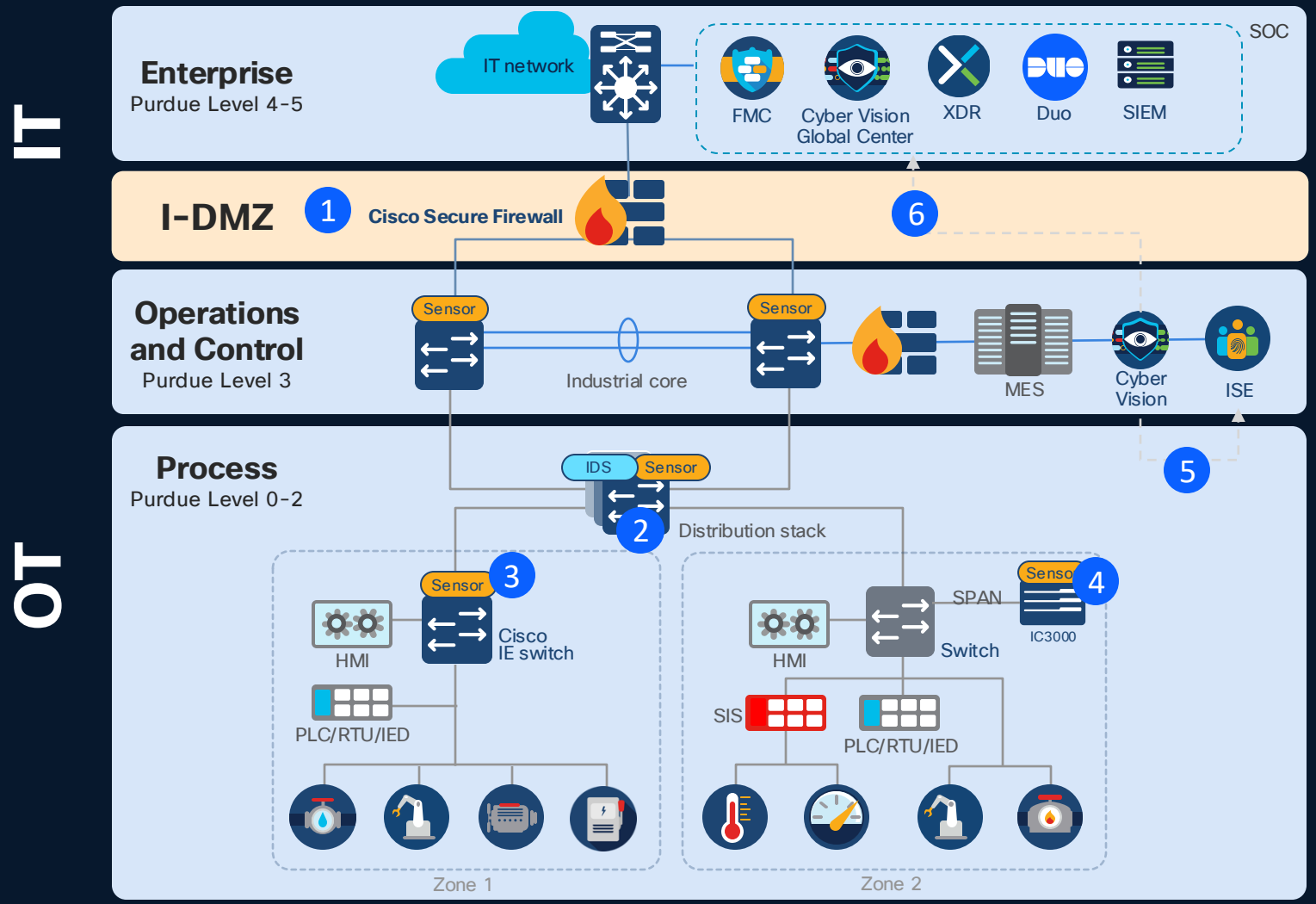
IR1101

IR1800

IR8300

Network Sensors
(Deep Packet Inspection built into network-elements eliminating the need for SPAN)

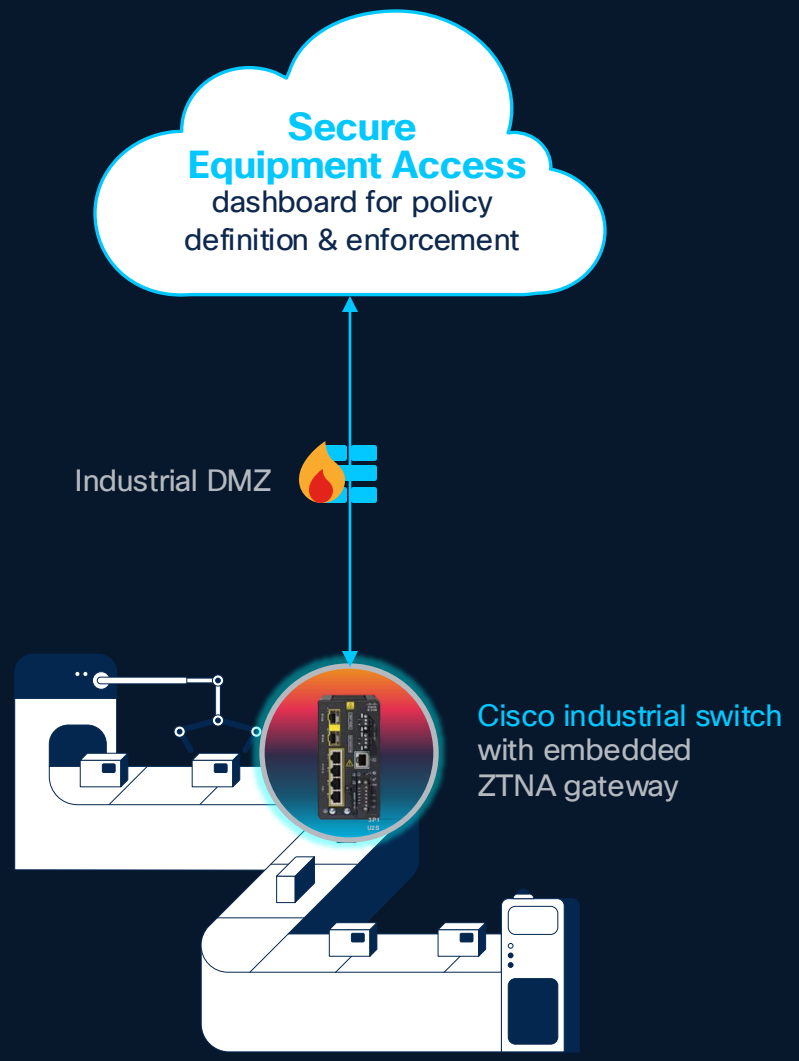
Cisco Cyber Vision in Manufacturing



1. Isolate IT and OT by installing an industrial DMZ with Cisco Secure FW
2. Create macro-segmentation zones in the Catalyst 9300 switches and deploy Cyber Vision sensors with Snort IDS.
3. Cyber Vision sensors deployed within segments across IE3500 switches
4. Cyber Vision hardware-sensors deployed via one-hop SPAN to gain visibility on non-Cisco switches
5. Build zones and conduits in Cyber Vision and share with ISE for micro segmentation
6. Cyber Vision shares details on OT devices and events with SOC to build informed security policies and investigate threats across domains

Zero Trust Network Access

- Never Trust Always Verify
- OT Asset Resource Isolation
- Clientless & Agent-based Access
- Remote User Posture Check
- Least Privilege Access
- Session Scheduling, Recording, Monitoring & Kill

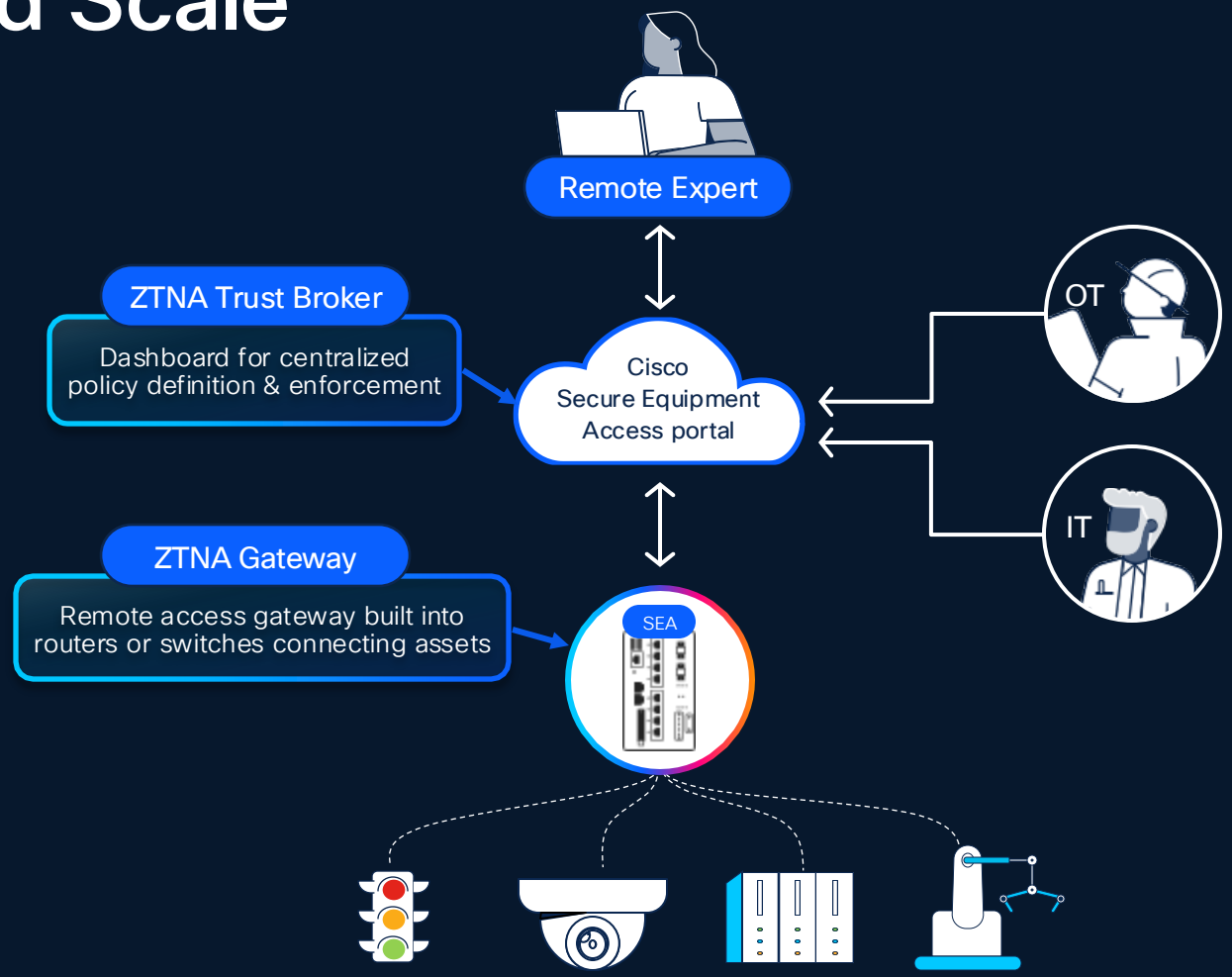


One-click zero trust remote access to any OT asset connected to Cisco industrial network

Easily Deploy, Manage, and Scale

A cloud service built into your industrial network

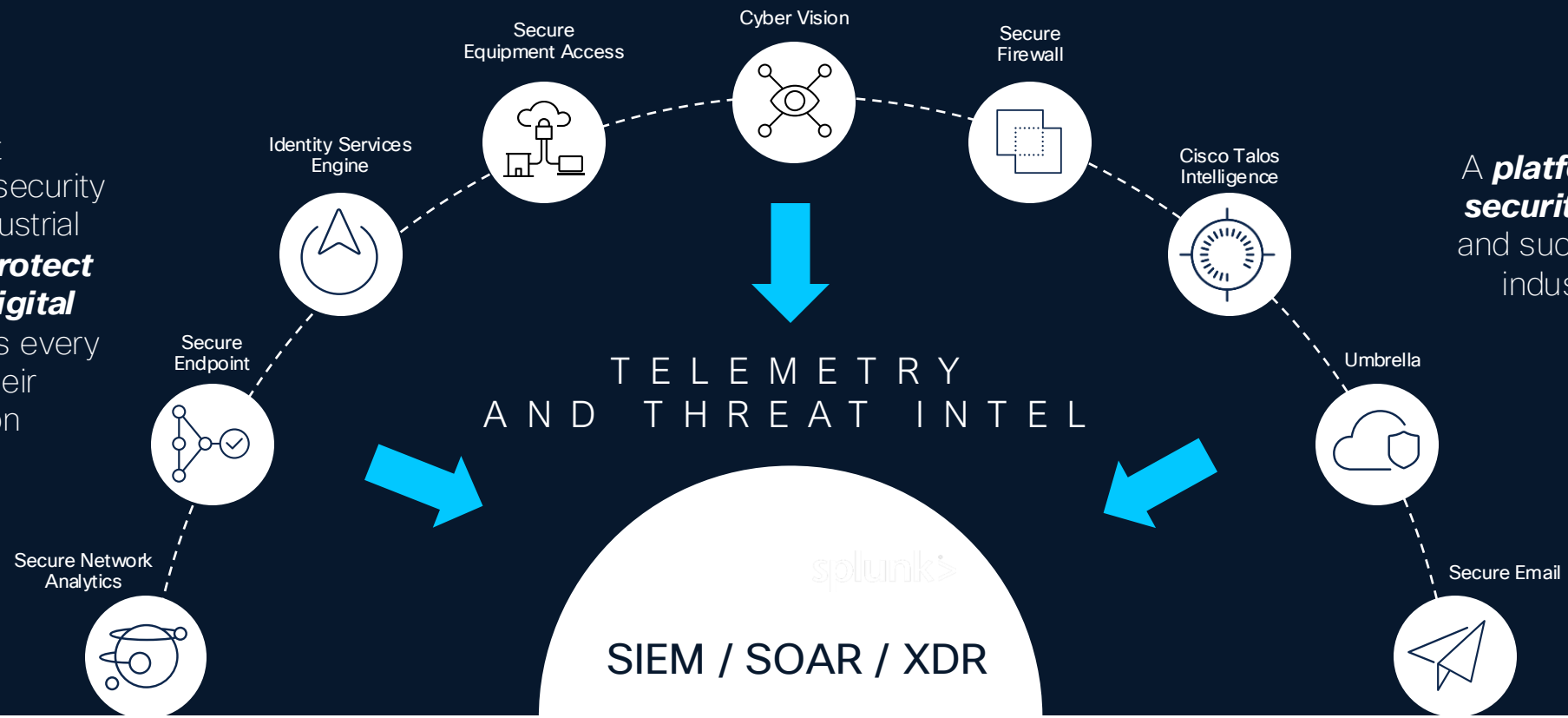
- Centralized policy definition for all assets and all sites
- Centralized enforcement increasing security and streamlining user experience
- Network-embedded gateways eliminating the need for dedicated hardware appliances



One-click zero trust remote access to any OT asset connected to Cisco industrial network

Cisco's Unified IT/OT Cybersecurity Platform

The most comprehensive security solution for industrial customers to ***protect their entire digital footprint*** across every aspect of their organization



A ***platform for OT, IT, and security*** teams ***to partner*** and successfully defend the industrial environment

AI powered cross-domain detection, investigation, and response

IT	OT	CLOUD

Key Takeaways

Future proof your network with Cisco AI ready industrial switching

Securing industrial operations starts with OT visibility

Leverage Cisco Validated Design for Manufacturing

Cyber Vision can help drive IT/OT collaboration

Take control over remote access to OT assets

Unify IT/OT visibility in the SOC to Identify, Detect, Protect, Respond and Recover

Thank you for your time.

Contact: BLMOUA@CISCO.COM