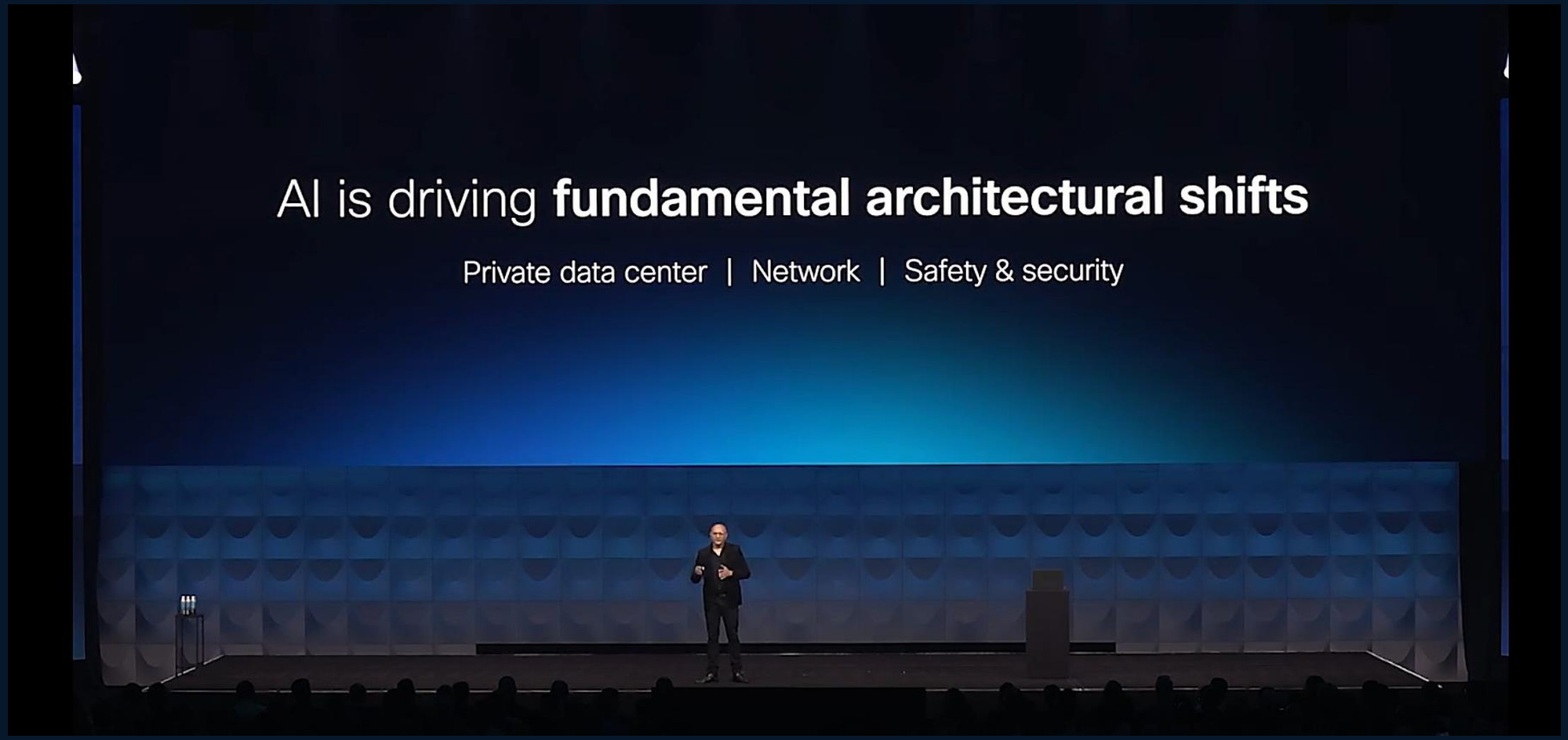
CISCO Engage | Tech Day Secure Network – Breakout Session

# Future-proof industrial networks for cybersecurity and AI

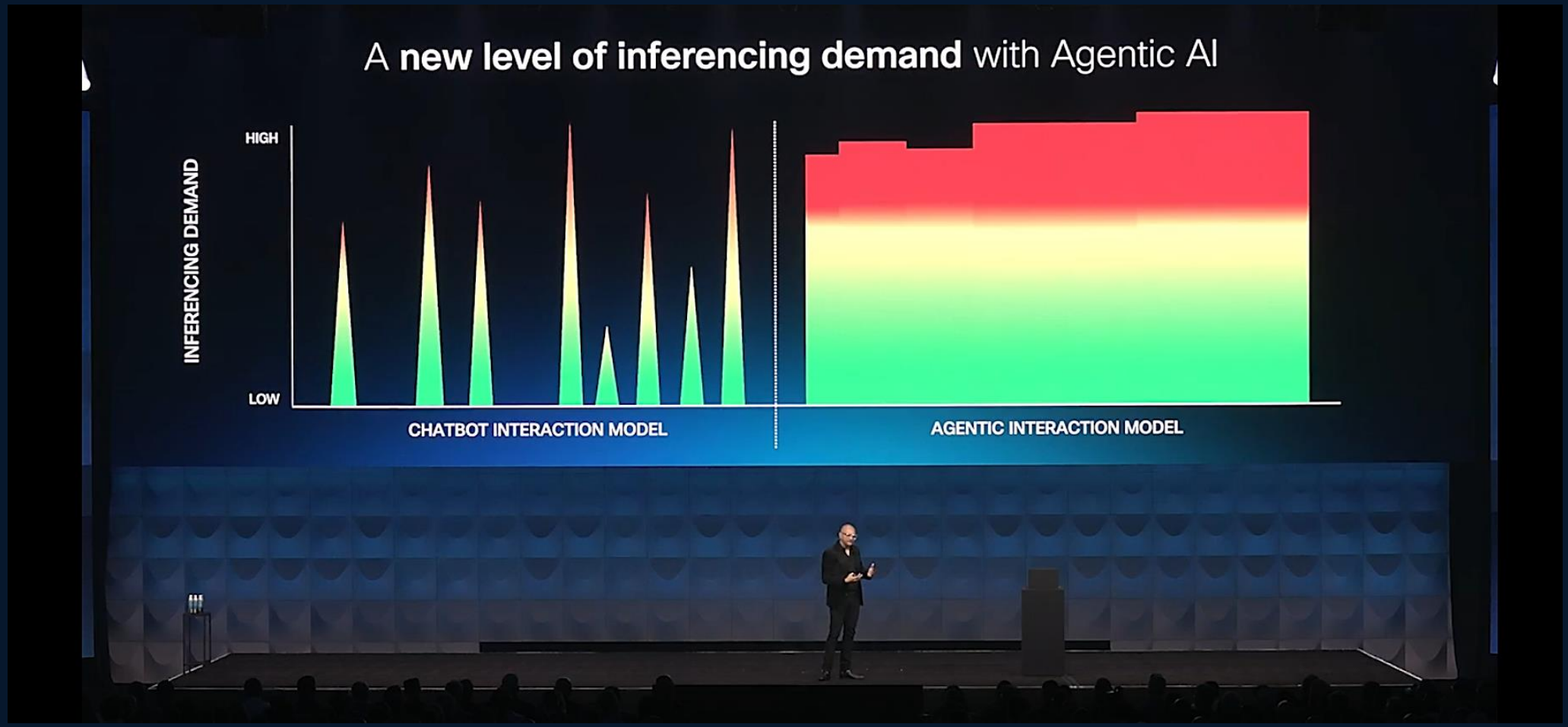
Building IT-OT resiliency solutions

Jack Reader
IOT, Solutions Engineer


October 9, 2025




Jeetu Patel, President & Chief Product Officer, Cisco Live, June 10, 2025



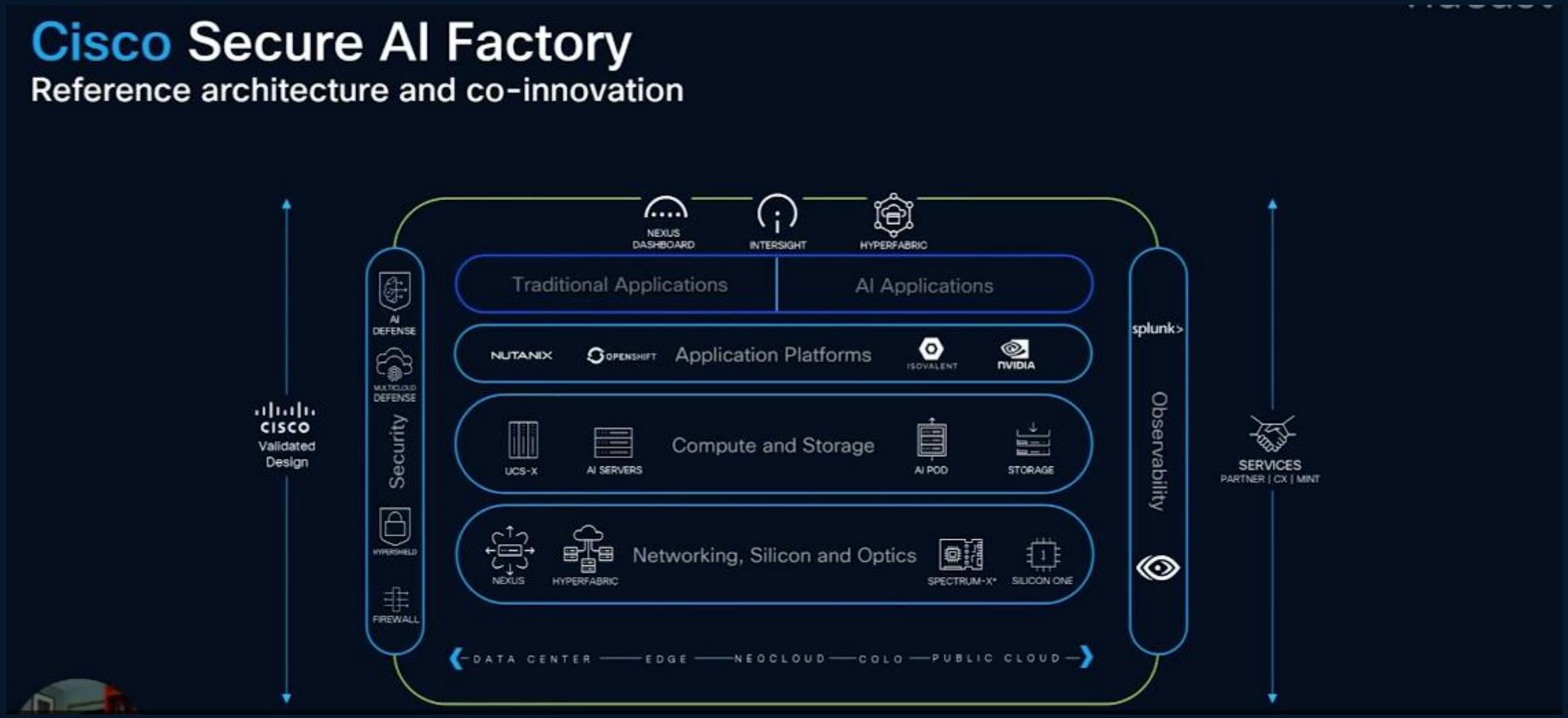
# Announcing AI Canvas

Reimagined user interface for human/agent interaction


DJ Sampath, SVP, Cisco AI Software and Platform Group, June 10, 2025

# Cisco Secure AI Factory

## Reference architecture and co-innovation



# Extending your IT to operational environments

Campus & Branch

- Warehouses
- Distribution Center
- Parking Lots
- Airport
- Port

- Factories
- Utility Substations
- Roadways

- Oil & Gas Refinery
- Mines

Reactive → Predictive

*Virtual*

*Perception → Reasoning → Action → Learning/Adaptation*

*Physical*

# OT modernization has become an **IT priority**

** Source: Harbor Research, IT / OT Business Case Trends*

Cybersecurity urgency and AI readiness are driving OT network modernization

Leaders are accelerating IT/OT collaboration for success

Early movers are seeing significant operational and financial benefits

# Vision systems needing high wattage 4PPoE

PTZ video surveillance for gunfire incidents

Cameras with heater/blower in extreme weather


Asset thermal monitoring to reduce maintenance costs

# AI Robotics – 3D object recognition


3D camera system

Sensors

Tool

Depth perception and collision-free operation requires robot arm to be outfitted with cameras and sensors that need to be connected to the edge inferencing system

# AI use cases across our customers today

## Vision Systems

Driving the need for PoE to power cameras and 10G uplinks for high bandwidth video traffic for AI inferencing

## IPC Virtualization

Network virtualization to connect thin clients on shop floor with VDI servers in manufacturing datacenter running AI workloads

## vPLC and vPAC

Minimize jitter between IO and control logic decoupled from physical hardware to run on servers capable of running AI models

## Edge-to-Cloud

Network assurance between AI inferencing at the edge and orchestration applications running in the cloud

If you tackle these use cases in silos,
you miss the fact the network is more critical than ever to realize success

# Cisco Live US 2025

## AI-Ready Data Centers

### Full-Stack AI Infrastructure

- Unified Nexus Dashboard
- Cisco Switches + NVIDIA Spectrum-X
- AI Defense for NVIDIA NeMo Framework

### Fusing Security into the Network: Hybrid Mesh Firewall

- Firewall 6100 Series
- Policy Control for Third-Party Firewalls
- Live Protect

### Service Provider Momentum

- New Cisco 8000 Routers

## Future-Proofed Workplaces

### Operational Simplicity Powered by AI

- Converged Meraki + Catalyst Platforms
- Unified Cloud Platform *(Meraki + Catalyst)*
- Multilayer Assurance (Owned + Unowned)
- Agentic Ops (Deep Network Model, AI Canvas)

### Scalable Devices Ready for AI

- Cisco C9350 and C9610 Smart Switches
- Cisco 8000 Secure Routers
- Industrial Switches
- Wi-Fi 7 Expansion + Campus Gateway
- Ultra-Reliable Wireless Backhaul
- Firewall 200 Series

### Fusing Security into the Network: UZTNA

- Security for Agentic AI

### AI Experiences

- *Cisco PTZ Camera*

## Digital Resilience

### Assurance and Observability

- Observability for AI
- Splunk + Thousand Eyes
- Splunk + Catalyst/Meraki

### Security Operations

- Cisco Firewall Logs ▸ Splunk (No Addl Cost)

### Data Platform

- Splunk PODs

# Cisco’s IIoT AI-Innovations

## AI Tooling

How we use AI to make the life of our customers easier

**AI for Networking**

## AI Infrastructure

How do we enable our customer AI projects

**Networking for AI**

**Operational simplicity**
powered by AI

**Scalable devices**
ready for AI

**Security**
fused into the network

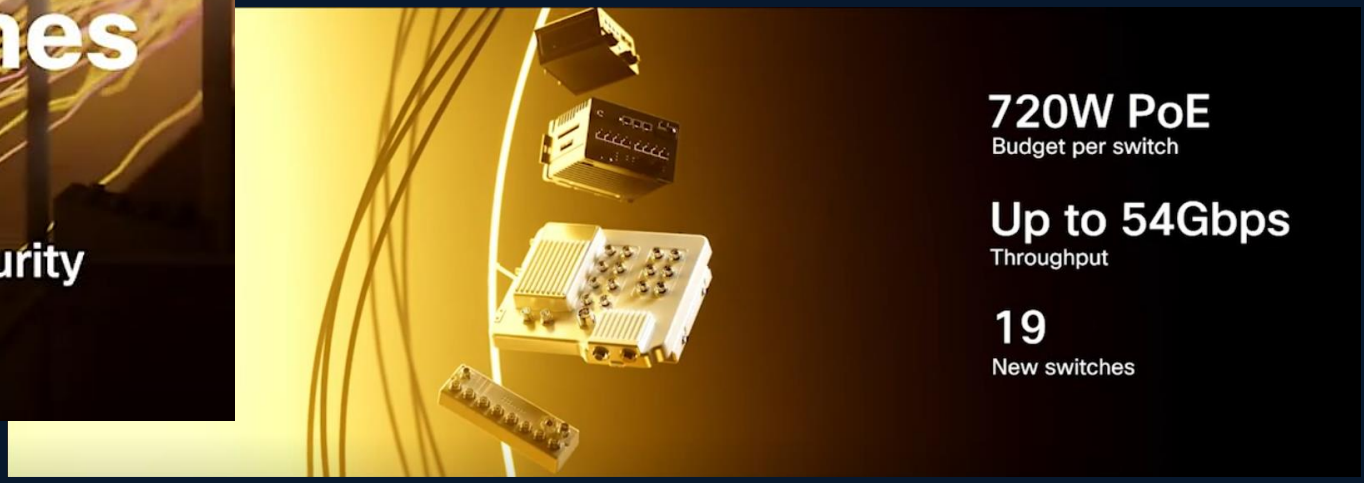
NEW

# Industrial Switches

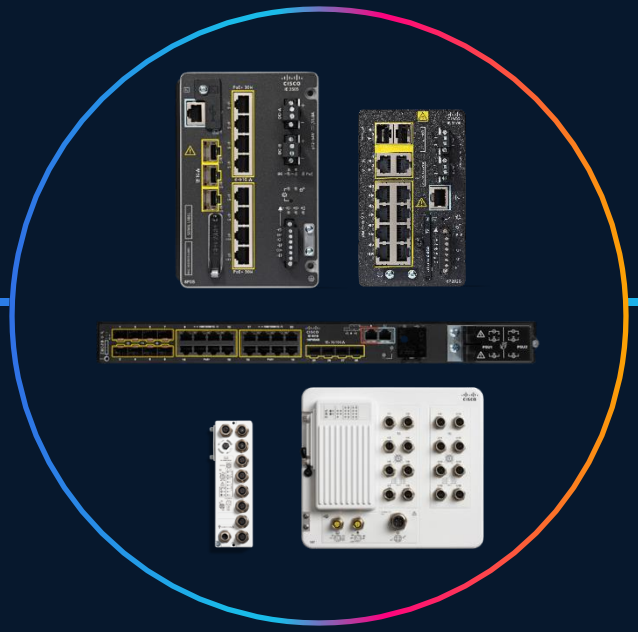
Resilient connectivity

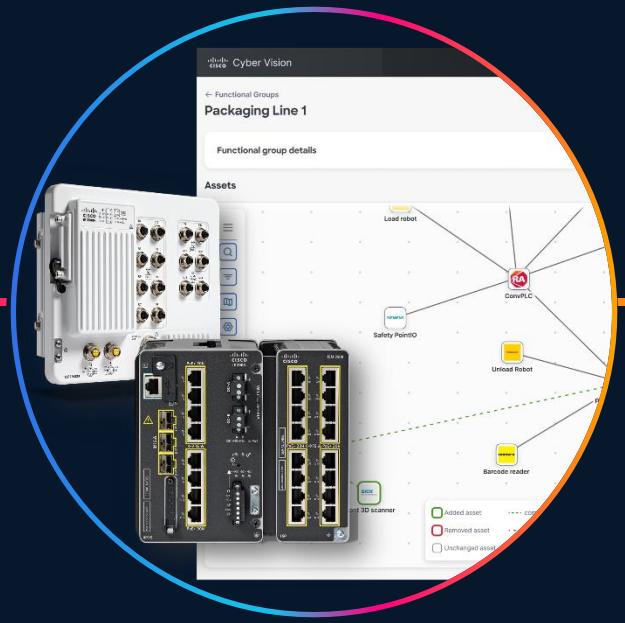
Cyber Vision and embedded security

Ruggedized designs



# Cisco announced a massive expansion of its market-leading industrial networking portfolio






Industrial switches for AI-driven operations + Redefining Wi-Fi to support AI-driven industrial mobility + AI-powered security to protect industrial networks

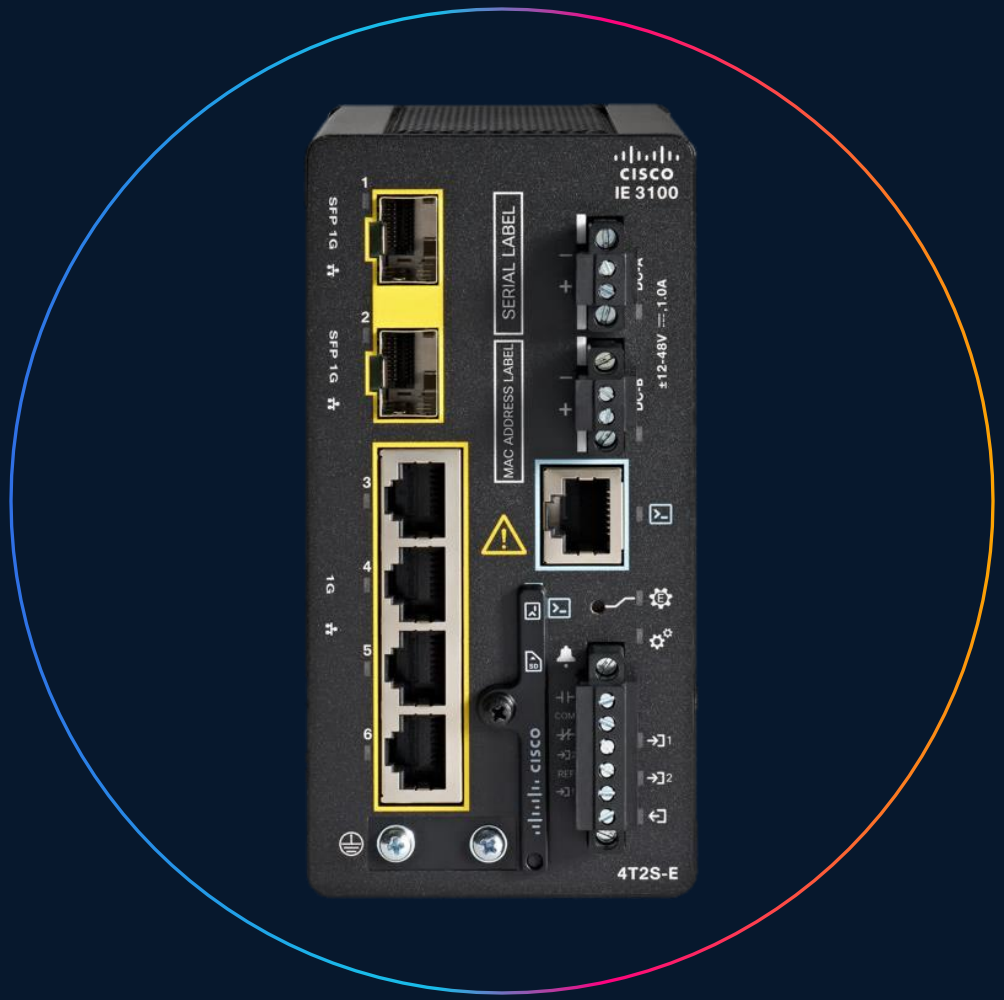
# Introducing IE3500 for Vision Systems


- Up to 480W PoE Budget to power 16 cameras with PoE+
- Up to 4x 2.5G and 12x 90W 4PPoE ports
- Fast PoE to restore power when switch boots after power failures
- Perpetual PoE to provide continuous power during switch warm reboots
- 3x 10G SFP uplinks to connect with AI inferencing systems

# Introducing IE3500 for Deterministic Latency


- TSN Frame Preemption for control and safety traffic using IEEE 802.3br and IEEE 802.1Qbu standards
- Simple to configure – Frame preemption Enabled hop-by-hop without the need for complex centralized scheduling
- Best-in-class PTP support for motion applications

# Introducing IE3100 with 4PPoE for video surveillance




- **Ultra compact** to fit in tight spaces with 1 or 2 90W 4PPoE ports
- **Fast PoE** to restore power when switch boots after power failures
- **Perpetual PoE** to provide continuous power during switch warm reboots
- **PoE Boost** to provide PoE power even when inputs voltage is under 48V

# Introducing Cisco IE3500 Rugged Series Switches

## Base

NEW

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

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

## Advance

NEW

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

NEW

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

## Common Expansion Modules

NEW

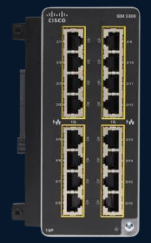
IEM-3500-6T2S
6x 1GE ports
2x 1GE SFP ports

IEM-3500-8T
8x 1GE ports

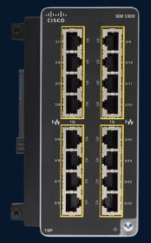
IEM-3500-8P
8x PoE/PoE+

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)

# Introducing Cisco IE3500H Heavy Duty Series Switches

## PoE

NEW

IE-3500H-14P2T

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

IE-3500H-12P2MU2X

## FE w/ GE Uplinks

NEW

IE-3500H-12FT4T

IE-3500H-20FT4T

## Full GE

NEW

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

# Introducing IE3100H for IO connectivity

- Compact size to fit into tight spaces such as robotic arms and custom-built machinery
- Enhanced resistance to dust, debris, vibrations, liquid spills, and wash-downs
- Best-in-class PTP support for motion applications
- Secure Equipment Access for zero-trust remote access for configurations, etc.

# New IE9300 Rugged Series Switch

IE-9310-26S2C

26x 1GE SFP ports

2x 1GE combo ports

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

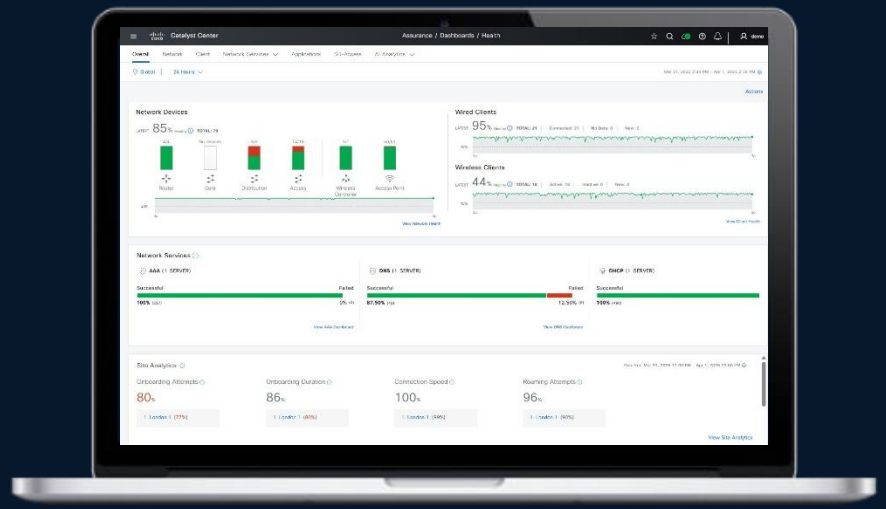
16x 1GE with PoE/PoE+ ports

8x 1GE SFP ports

Up to 480W PoE budget

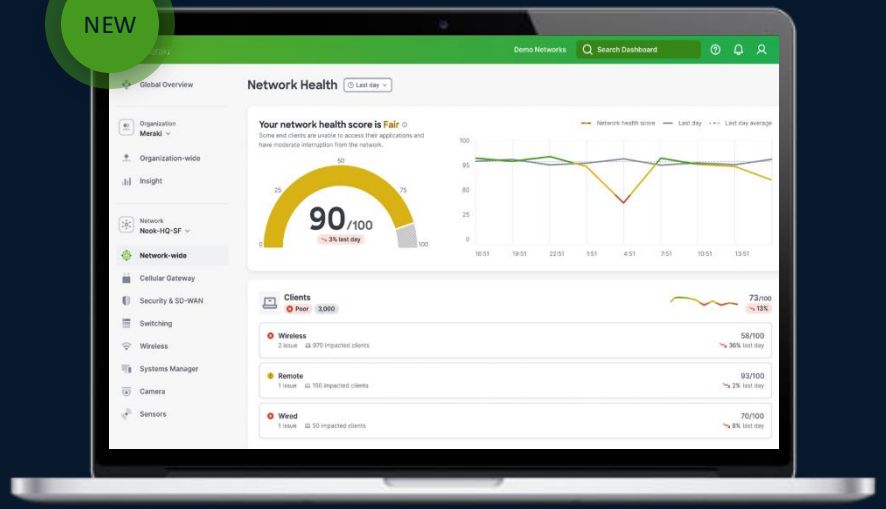
4x 10G SFP ports

# On-premises or Cloud management




Catalyst Center Management

NEW




Meraki Dashboard Management

Automate deployment, Simplify management with tools IT already knows and loves

# Industries need ultra reliable, low latency wireless

Automated Guided Vehicles (AGVs) and cobots


Tele-remote operations in mines and ports


Communications-based train control (CBTC) in rail

Connectivity where wired options unavailable or prohibitively expensive

# Addressing shifts in manufacturing

Factory floor layouts are constantly changing, disrupting line of sight and RF environments

Dropped connections create line stops, safety issues, and loss of productivity

**Wired, fixed** assembly lines are evolving into a more flexible, wireless factory floor

AGVs require **mobile, reliable, & lossless** wireless connectivity across the entire process

# Announcing unified Wi-Fi and URWB operations


Ultra-Reliable Wireless Backhaul built-in Enterprise Wi-Fi Access Points

One Management Platform, One wireless infrastructure to install

Best of Wi-Fi combined with new use cases enabled by URWB Technology

# Available across our industry leading portfolio of indoor, outdoor and industrial access points*

## Wi-Fi 7

CW9176I,
CW9176D1

CW9178I

Focus for 17.18.1 early Release

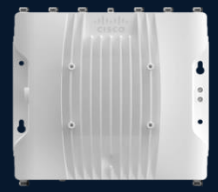
## Wi-Fi 6E

CW9136I

CW9166I, CW9166D1

IW9165E

IW9165D



IW9167E
IW9167E-HZ

IW9167I

## Wi-Fi 6

C9130
(AXE, AXI)

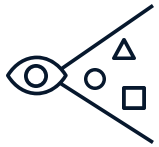
C9124
(AXE, AXI, AXD)

*Subject to change

Planned supported AP models post launch

# Cisco Cyber Vision

## Visibility & Security Platform for the Industrial IoT



### Visibility
OT asset inventory
Communication maps

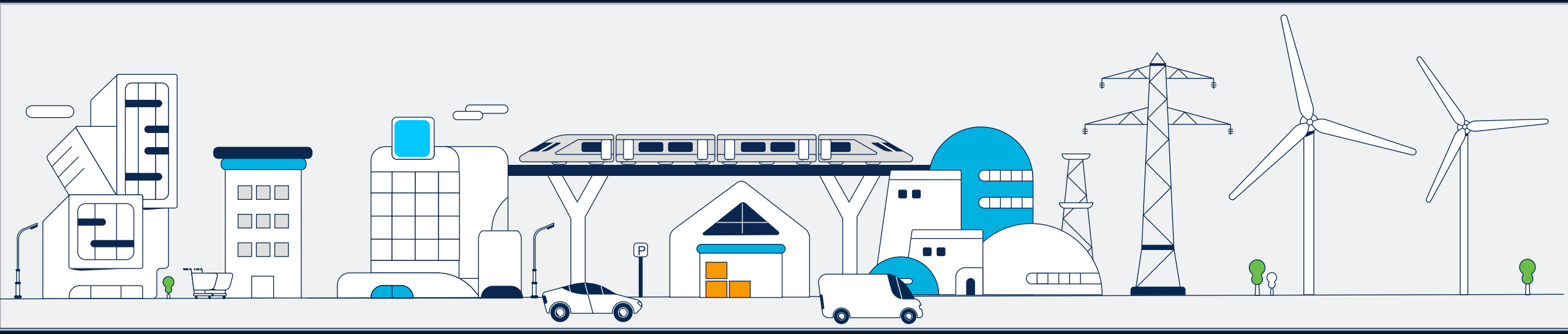
### Security Posture
Device vulnerabilities
Risk scoring to prioritize action

### Zone Segmentation
Automate segmentation below
the IDMZ to protect operations

### Secure Remote Access
Control risks from remote users
with zero-trust network access

OT security and secure remote access you can deploy at scale

# Securing industrial operations starts with OT visibility




Inventory OT assets and their communications

Spot vulnerabilities to patch or mitigate

Create access policies to segment networks

Detect bypass or leaks in the IDMZ

Drive compliance and governance

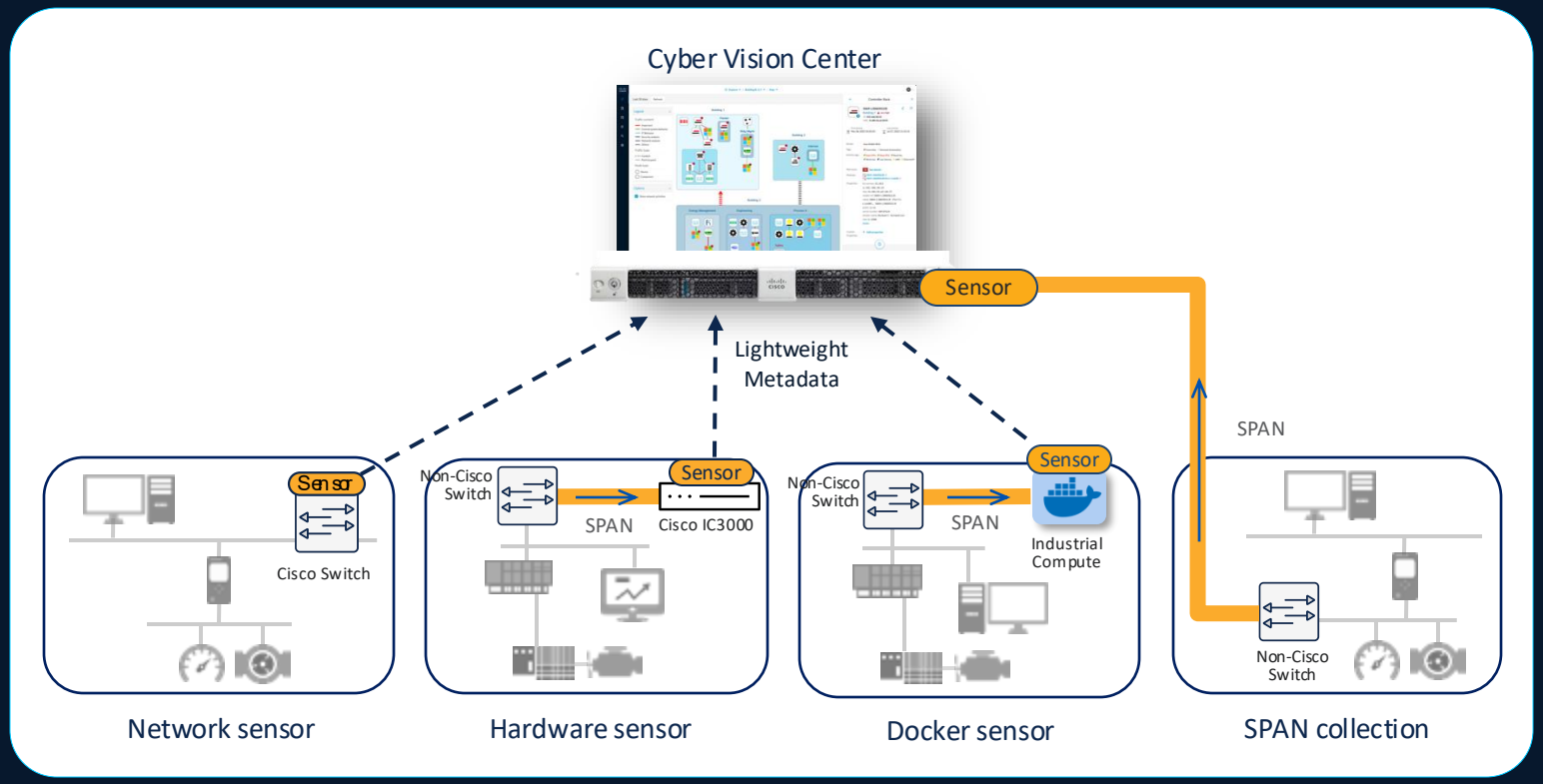
OT context and insights are foundational to securing industrial networks



cisco

# Cisco Cyber Vision

## Implementing OT visibility at the lowest TCO




- Network embedded sensor
  No need for addition hardware
- No need for SPAN collection networks
- Active discovery passes NAT boundaries
- Comprehensive visibility, even at lowest Purdue levels

Scales across brownfield and greenfield environments

# The journey to secure industrial networks

Understand the OT security posture with OT visibility

Limit blast radius with network segmentation

Control risks from remote access to OT assets

Monitor OT networks in the SOC

# Enforcing OT network segmentation using the network

## Industrial Switches

Enforcing port access control and implementing microsegmentation

## Industrial Routers

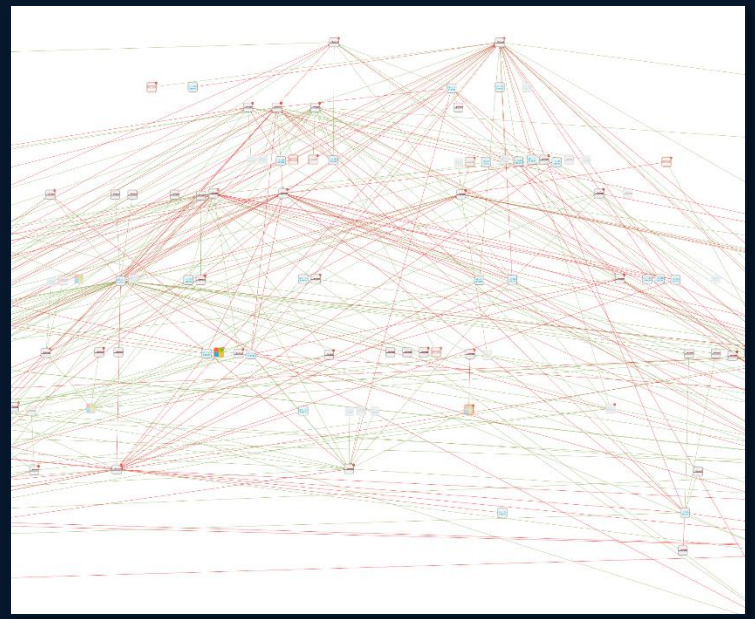
Isolating field assets and enforcing comprehensive NGFW policies

## Hybrid Mesh Firewalls

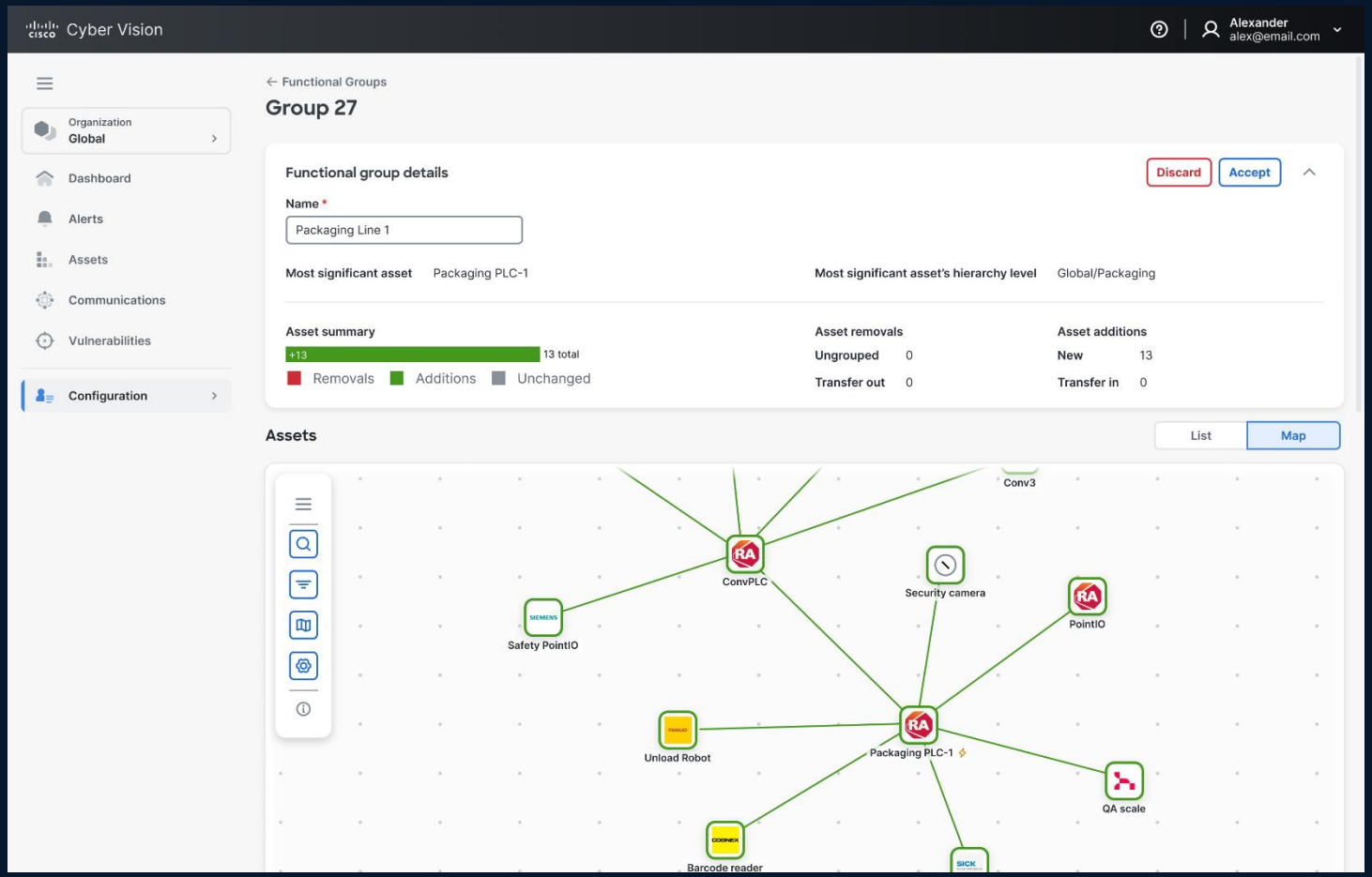
Building robust industrial DMZ and implementing macrosegmentation

Using the network to shrink the zones of trust and protect operations at scale

# Introducing AI-driven Network Segmentation for OT



OT asset inventory projects highlight flat, unsegmented networks

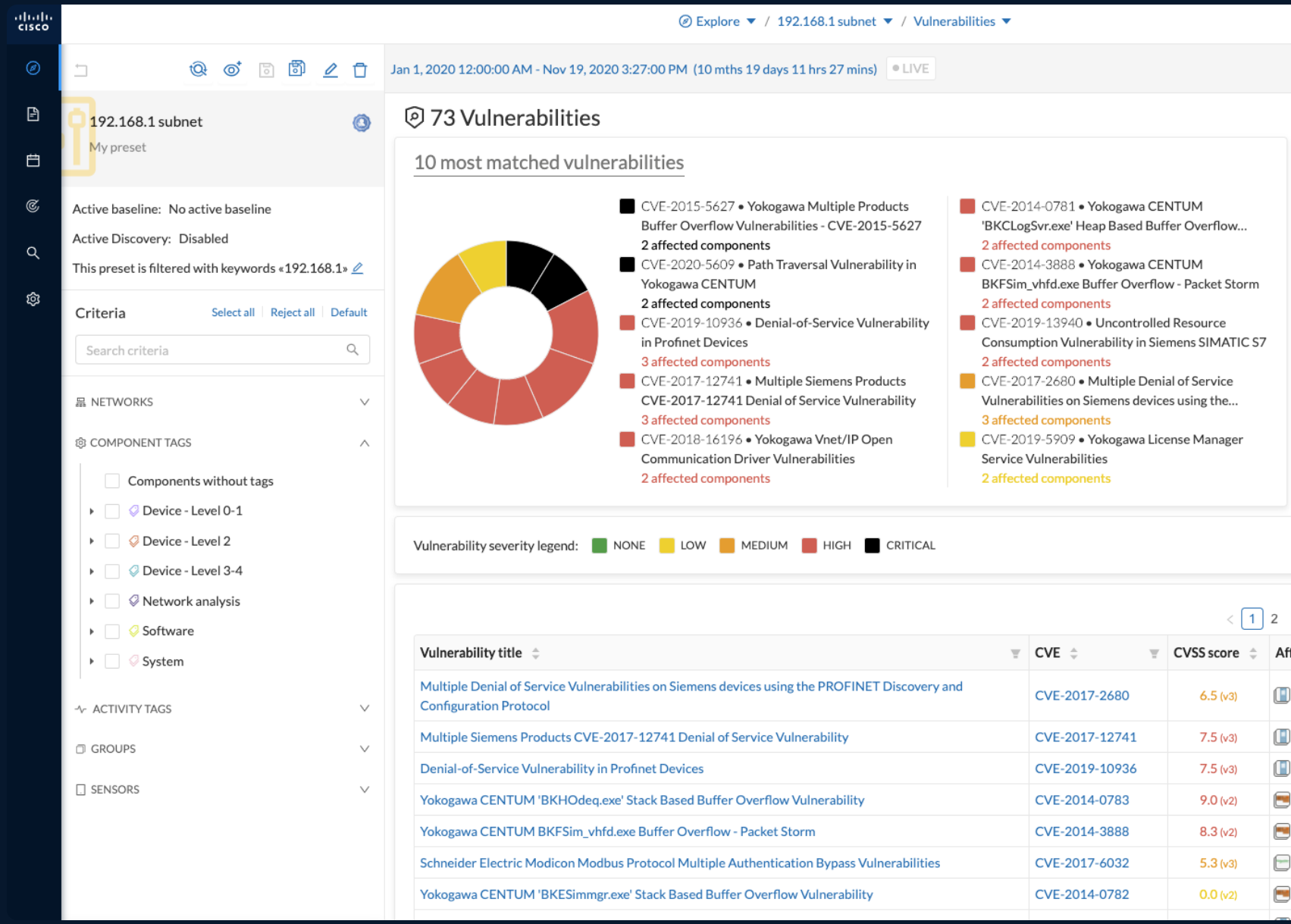



Cisco Cyber Vision ML-driven auto-grouping automatically creates security zones to drive network segmentation using Firewalls or NAC

Cyber Vision

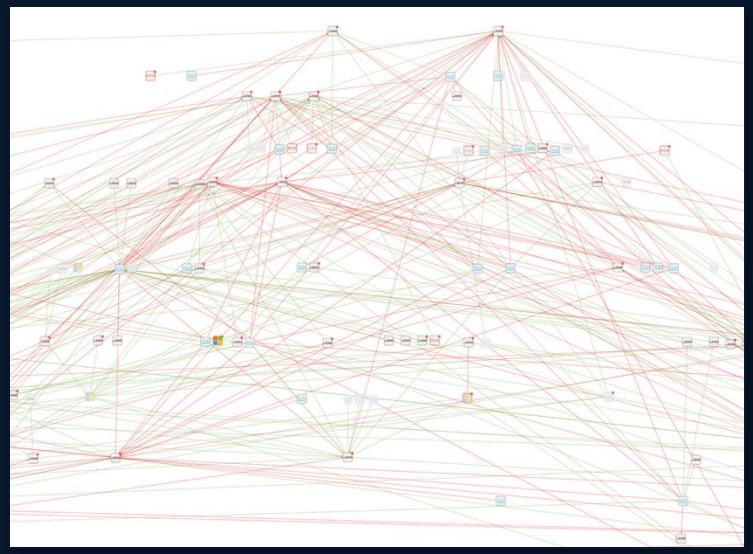
# Identify & Track Vulnerabilities

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



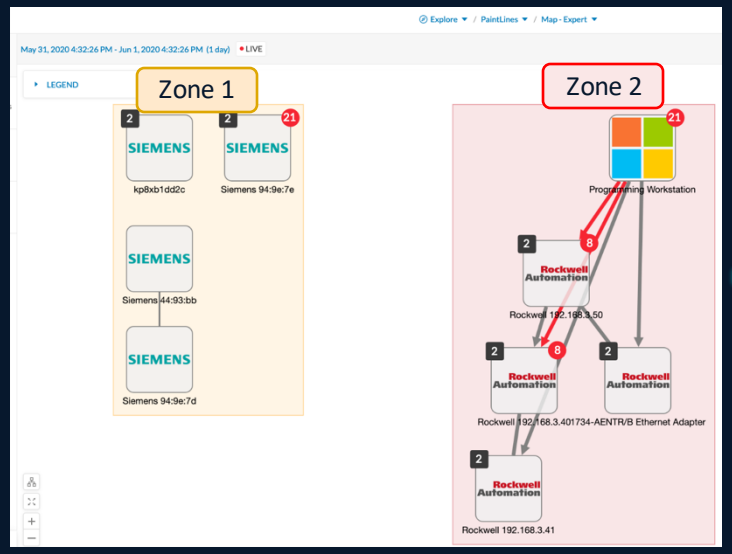
# Using visibility to drive OT segmentation at scale

## Cyber Vision discovers OT assets…



OT asset inventory projects highlight flat, unsegmented networks

## …and groups them into logical zones…




Cyber Vision helps OT teams document security zones to drive segmentation

## …to drive policy enforcement

Cisco Identity Services Engine

Cisco Secure Firewall Management Center

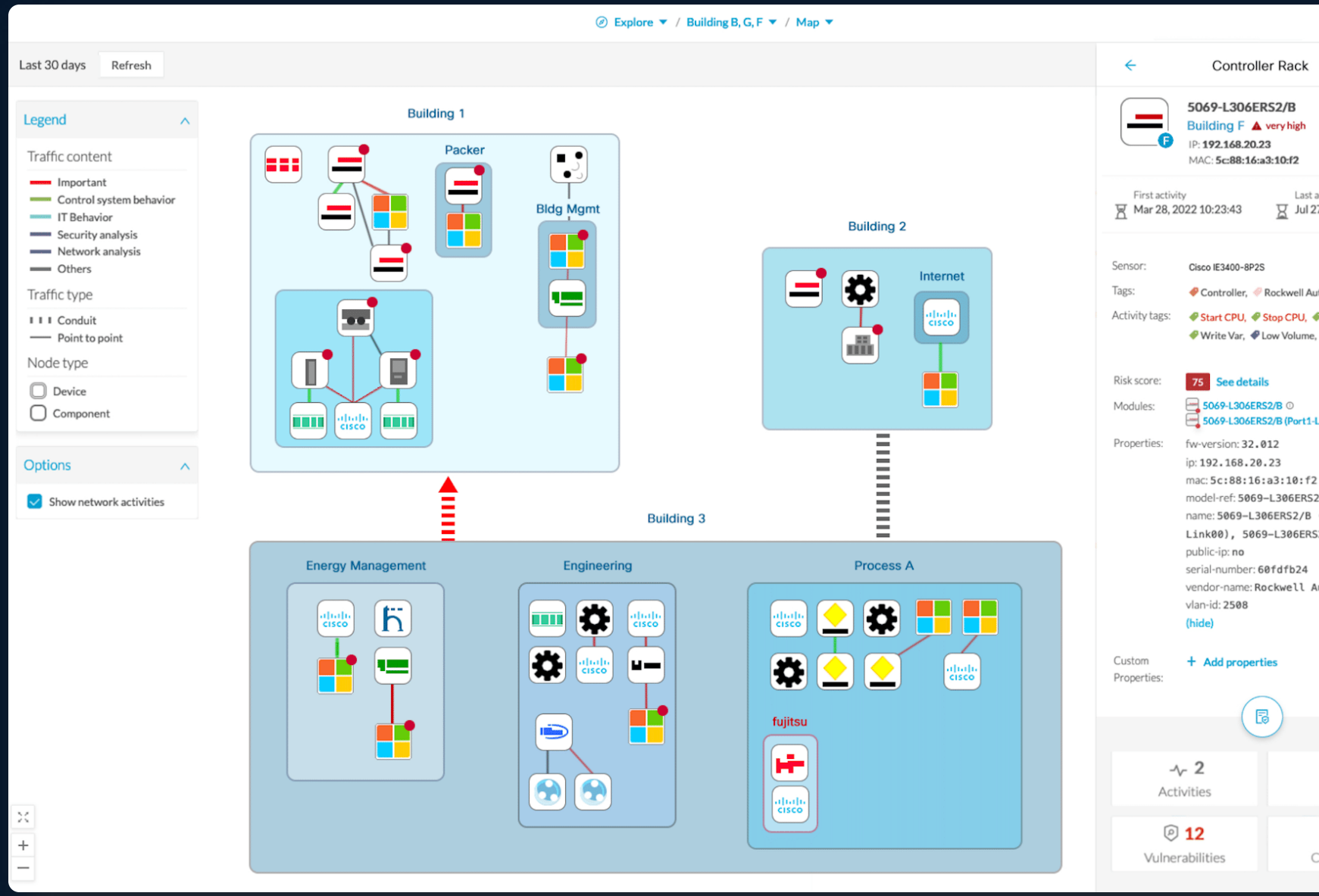
Adaptive segmentation enforced by IT, controlled by OT

Segmenting OT networks in weeks, not in years, without causing downtime

Cyber Vision

# IEC-62443 segmentation made simple

- Group OT assets into zones
- Visualize conduits
- Identify traffic violations
- Share context with other platforms to enforce segmentation
- Changes to groups automatically update access policies

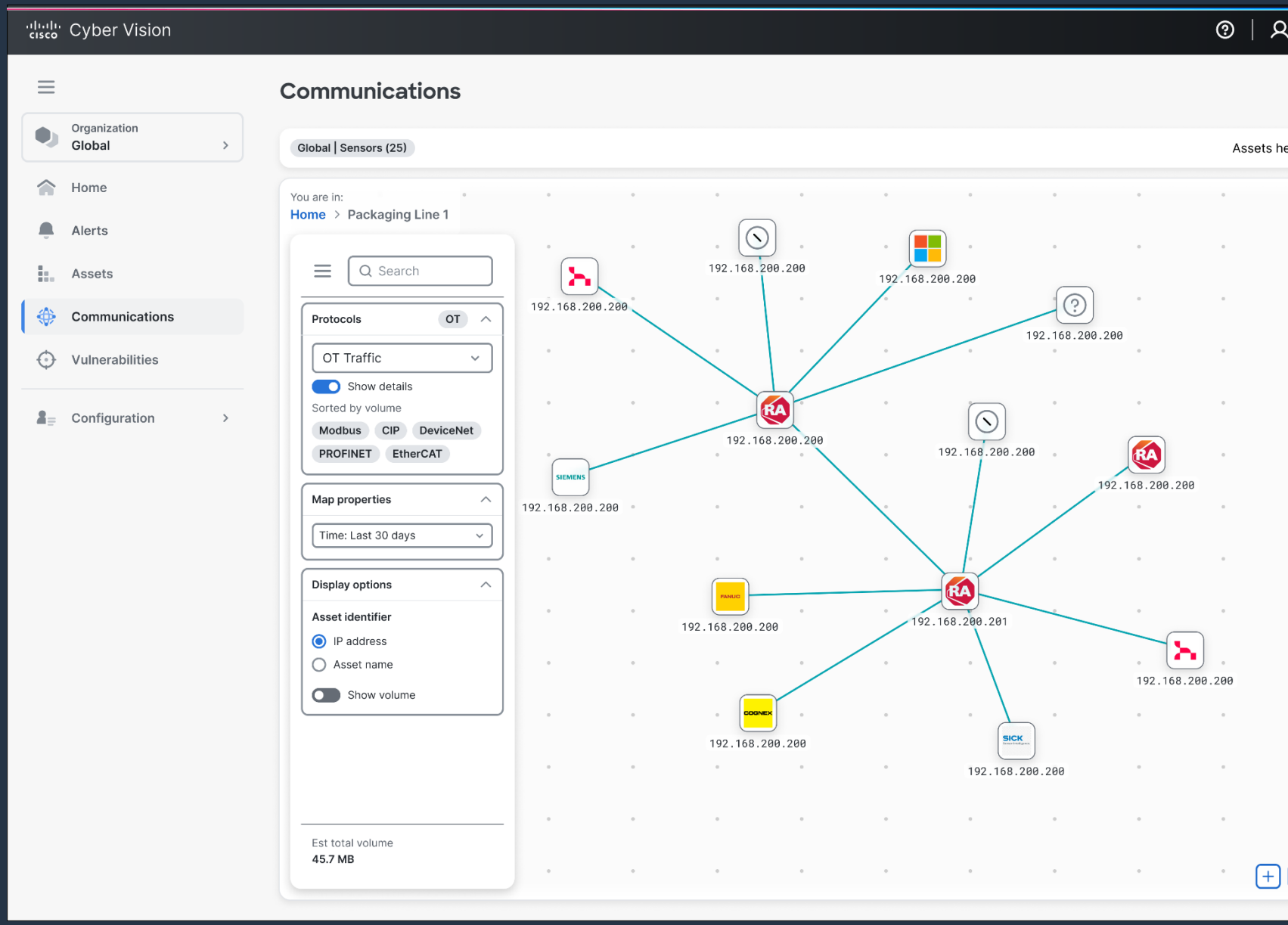


# Cyber Vision

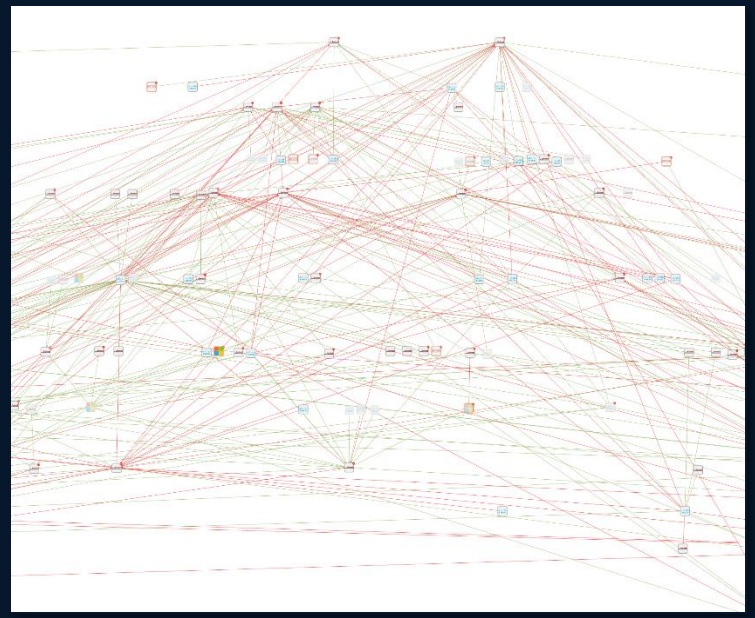
## Visibility
OT asset inventory
Communication patterns

## Security Posture
Device vulnerabilities
Risk scoring

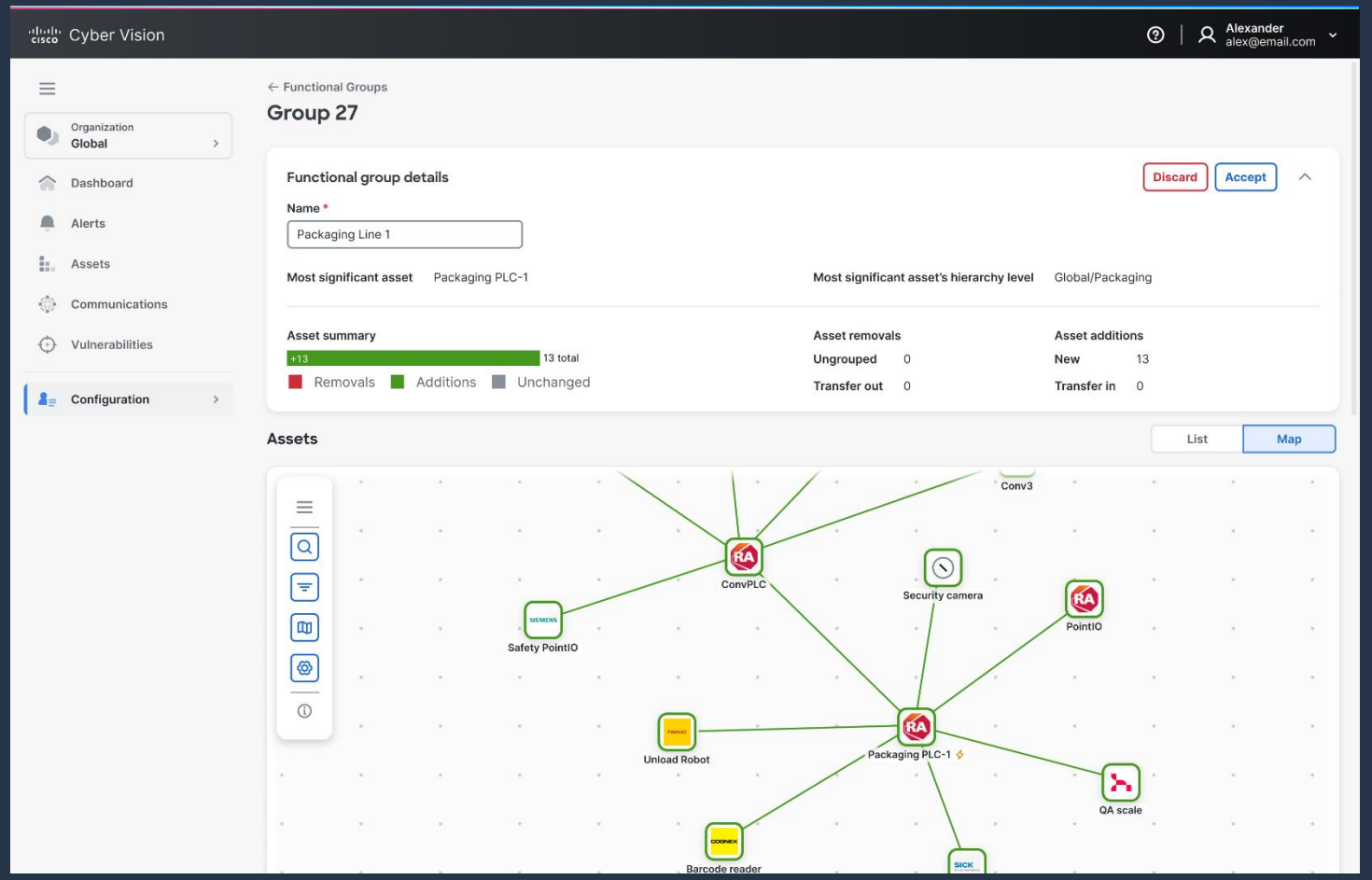
## Operational Insights
Track process/device modifications
Record control system events



# Introducing AI-driven asset auto-grouping

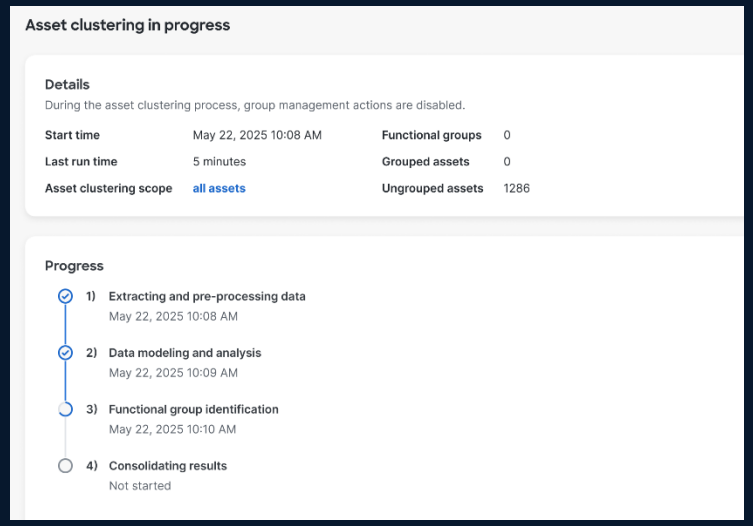


OT asset inventory projects highlight flat, unsegmented networks

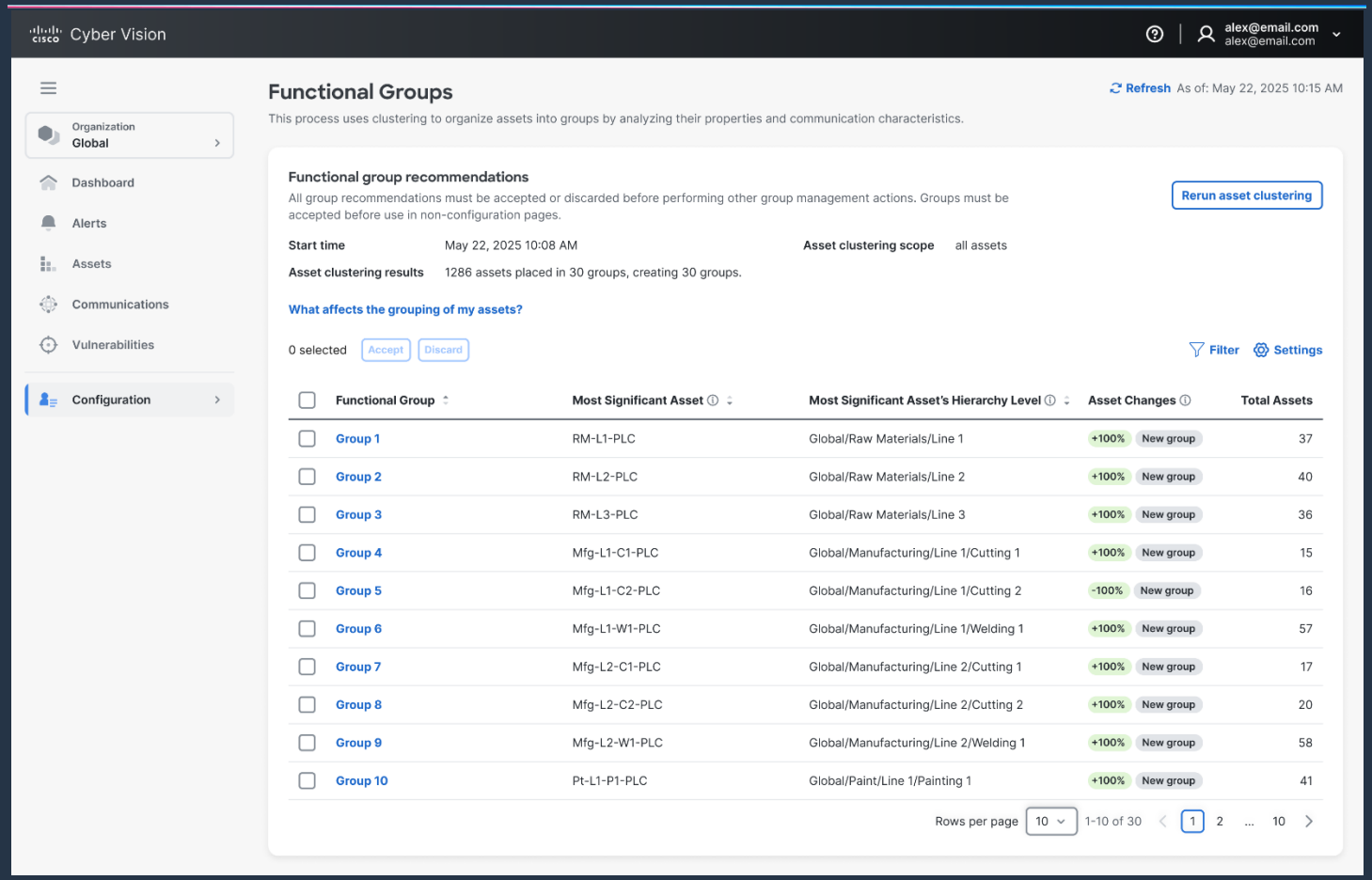



Cisco Cyber Vision AI-driven auto-grouping automatically creates security zones to drive network segmentation using Firewalls or NAC

# Introducing AI-driven asset auto-grouping



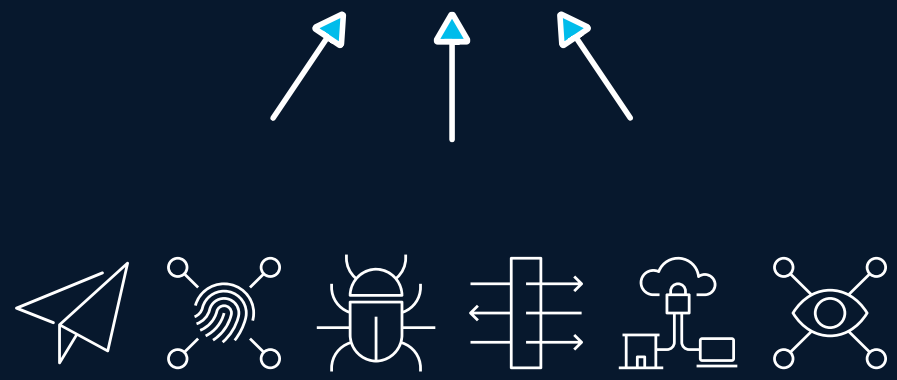

AI-driven asset-clustering analyzes the communications patterns of the assets in the network




Upon completion, groups are presented to an admin for review

# Unifying IT and OT visibility into the SOC to detect threats faster

splunk> a cisco company



Visibility across the entire attack chain

- Enrich IT security event information provided to the SOC with **OT context** from Cyber Vision
- **Visibility across the entire attack chain** – detect threats before they even reach the OT network
- Unifying visibility is key whether you have a dedicated OT SOC or a unique SOC for IT and OT
- Splunk **risk-based alerting** reduces alert volumes and enhances productivity with high-fidelity threat detection



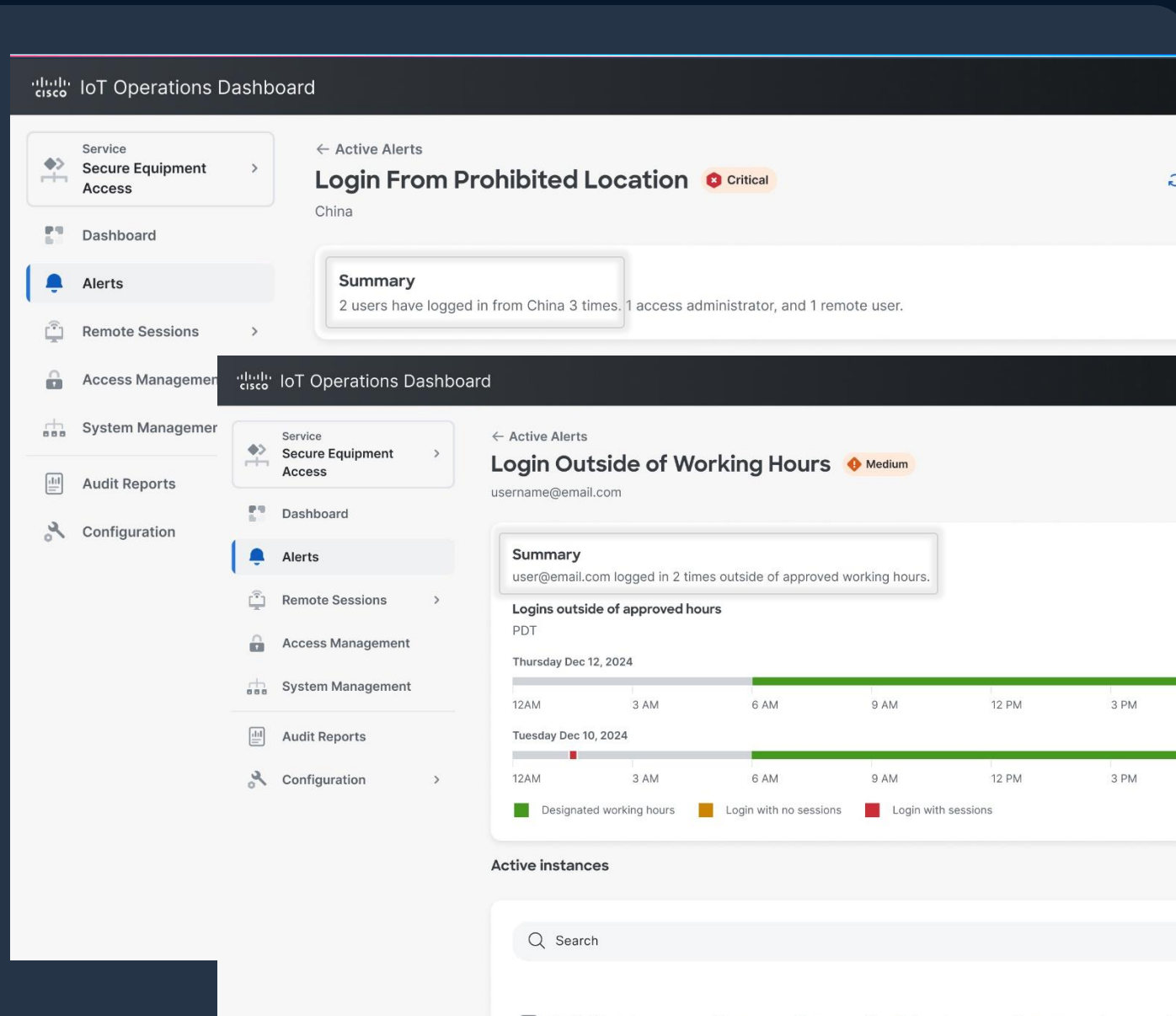
cisco

# Remote user identity threat detection

With the rise in remote access activities, remote user identity is becoming a significant attack vector in OT networks

We are delivering new capabilities in SEA to detect threats related to remote user identity

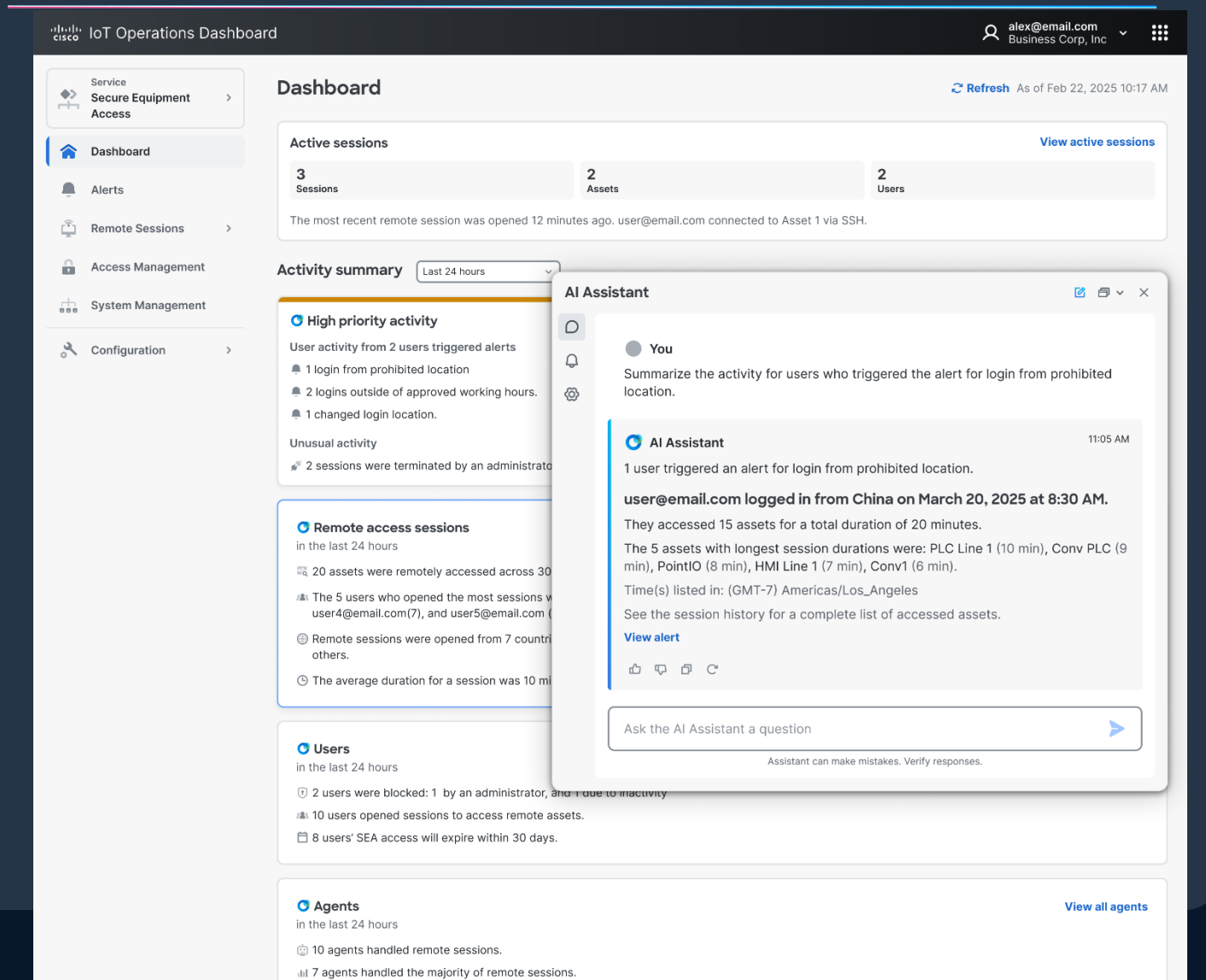
- Login from unapproved geolocation
- Login outside working hours
- Auto deactivation of unused accounts



# Cisco AI Assistant for Secure Equipment Access

Get a complete picture of remote access activities for forensic, audit, and compliance purposes without having to parse extensive audit trails

New GenAI driven insights into **who** accessed **which** assets and **when**, powered by Cisco AI Assistant



# Call to action

Securing industrial operations starts with OT visibility

Beware of hidden costs! Only network-embedded OT visibility can scale

Leverage visibility to drive IT/OT collaboration and segmentation below the IDMZ

Take control over remote access to OT assets… with a solution made for OT

Unify IT/OT visibility in the SOC for a comprehensive view on the attack chain

Learn more at
cisco.com/go/iotsecurity

# Thank you