

Modernizing Industrial Networks for Cybersecurity and AI

Luke Biroldi – Account Executive



Trends in industrial networking

Growing 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

Extending your IT to operational environments



Campus & Branch

 Warehouses

 Distribution Center

 Parking Lots

 Airport

 Port

 Factories

 Utility Substations

 Roadways

 Defense

 Oil & Gas Refinery

 Mines

Consistent Network Architecture
IOS-XE, Catalyst Center, SD-WAN Manager

Airports

Improve passenger experience

- Provide pervasive Wi-Fi connectivity
 - Reduce delays in baggage handling
-

Boost safety and security of the critical infrastructure

- Ensure safety with surveillance cameras
 - Provide access control at gates
 - Protect against cyber threats
-

Increase operational efficiency

- Reduce turn-around times for planes
- Ensure seamless communications throughout the airport



Jet Bridges



Runways



Cargo and Baggage
Handling



Airport Transportation
Systems

Parking lots and outdoors

Improve customer/user experience and safety

- Place digital signage for navigation
- Use surveillance cameras and lighting for safety
- Deploy secure Wi-Fi for customer use

Manage parking lot space efficiently

- Monitor available spaces with sensors and cameras

Secure entry/exit controls, ticketing, and payment kiosks

- Securely connect control and POS systems to the network

Improve staff productivity

- Provide robust connectivity to staff and equipment in harsh and outdoor non-climate-controlled conditions
- Shorten deployment cycles with make changes with ease using tools they already know and trust



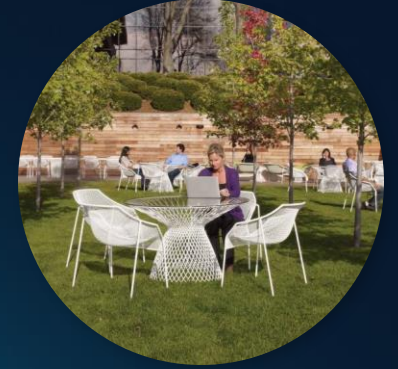
Garages



Outdoor Malls



Stadium and event
Centers



Outdoor Campuses

Warehouses and distribution centers

Optimize logistics operations

- Reduce costs and provide better customer experience
- Increase real-time process visibility
- Improve shelf utilization and inventory management

Improve staff safety, connectivity, and productivity

- Automate fulfillment operations
- Provide reliable connectivity for fixed and mobile devices with ruggedized network equipment

Comply with regulatory and sustainability requirements

- Reduce power requirements
- Monitor environmental conditions for safe storage

Ensure uninterrupted operations and prevent theft

- Maintain accurate inventory counts with greater visibility
- Connect security systems like surveillance cameras, badge readers, etc.
- Prevent, detect, and remediate cybersecurity breaches



Sorters



Forklifts, AGVs and embedded scales



Handheld scanners and tablets



Conveyor belts

AI and software are revolutionizing industries



Machine vision



More cameras need more
PoE options (4PPoE)
More bandwidth (10G)
New form factor required



Autonomous vehicles and
Tele remote operations



Pervasive WiFi and
industrial wireless
infrastructure



Software Defined
Automation



Unified fabric from plant
floor to data center ->
Use virtualization to
co-locate HW and SW
Need for frame
preemption



AI robotics
and cobots



Disaggregate
robots HW/SW
Leverage AI to
program robot
Move CPU/GPU
workload to DC for
elasticity and scale
Need for low latency



Industrial data
collection



Need for standardization
and automation of
manufacturing
infrastructure
Data collection at scale

Cisco sees the network as the key to unlock software-driven industrial automation and industrial AI

Virtualized control/AI
in the data center



VIRTUAL ROBOT
CONTROLLER



VIRTUAL
PLC/RTU



VIRTUAL
COMPUTE

Nervous system
is the network

Network

Physical components
in the field



ROBOTS, VEHICLES



FIELD ASSETS



SENSORS

**This requires a
new architecture
for industrial
networks**



Cisco's Industrial IoT network architecture

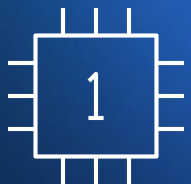
Operational simplicity
powered by AI



Security
fused into the network



Scalable devices
ready for AI



Operational simplicity powered by AI



Our unified platform – Managing IT/OT portfolio

PLATFORM

Management

Assurance

API / Integrations

Intelligence - AgenticOps

HARDWARE



Smart
Switches



Secure
Routers

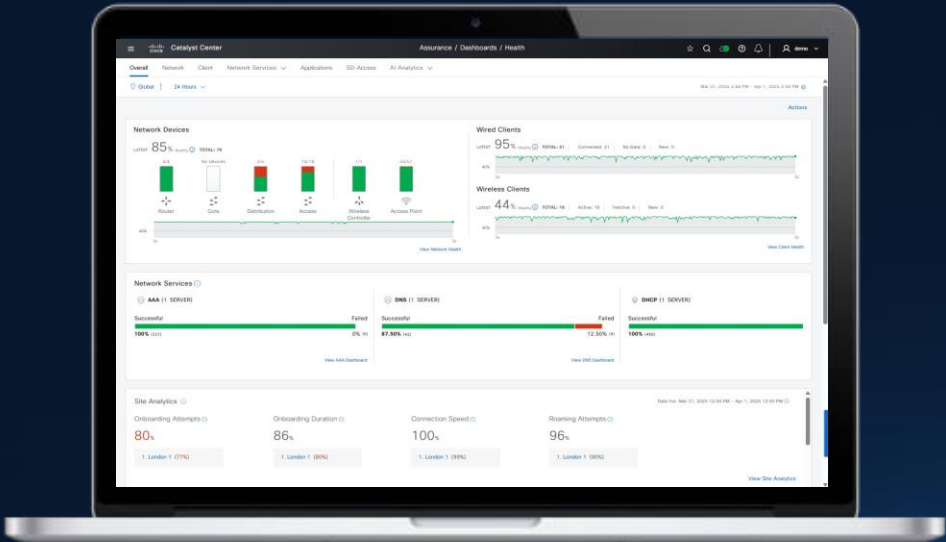


Wireless



Industrial
IoT

Unified management and security across IT and OT with Catalyst Center



Industrial Switching

Industrial Wireless

Industrial Routing



Reduce downtime



Increase efficiency



Stay compliant

What can Catalyst Center do for OT networks?



Manage networks with automation and performance assurance such as zero-touch provisioning, rapid issue detection and resolution, etc.



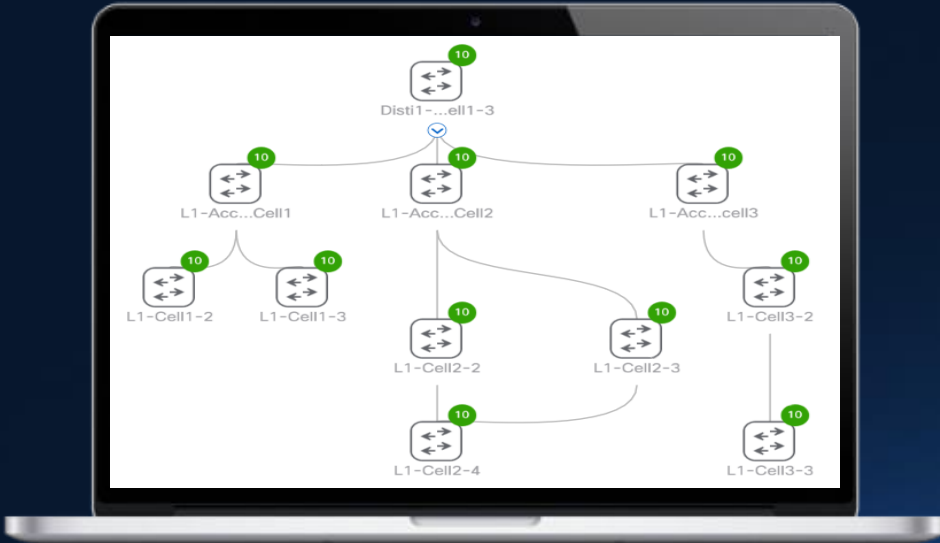
Secure operations by applying consistent macro- and micro-segmentation policies and deploy key security firmware updates efficiently.



Boost innovation by AI-driven problem identification and resolution assistance, keep the network performing optimally, and enable even further automation through APIs



Extend to non-Cisco devices by monitoring and managing many 3rd party network devices



Our unified platform – Assuring IT/OT portfolio

PLATFORM

Management

Assurance

API / Integrations

Intelligence – AgenticOps

HARDWARE



Smart
Switches



Secure
Routers



Wireless



Industrial
IoT

AVAILABLE | NOW

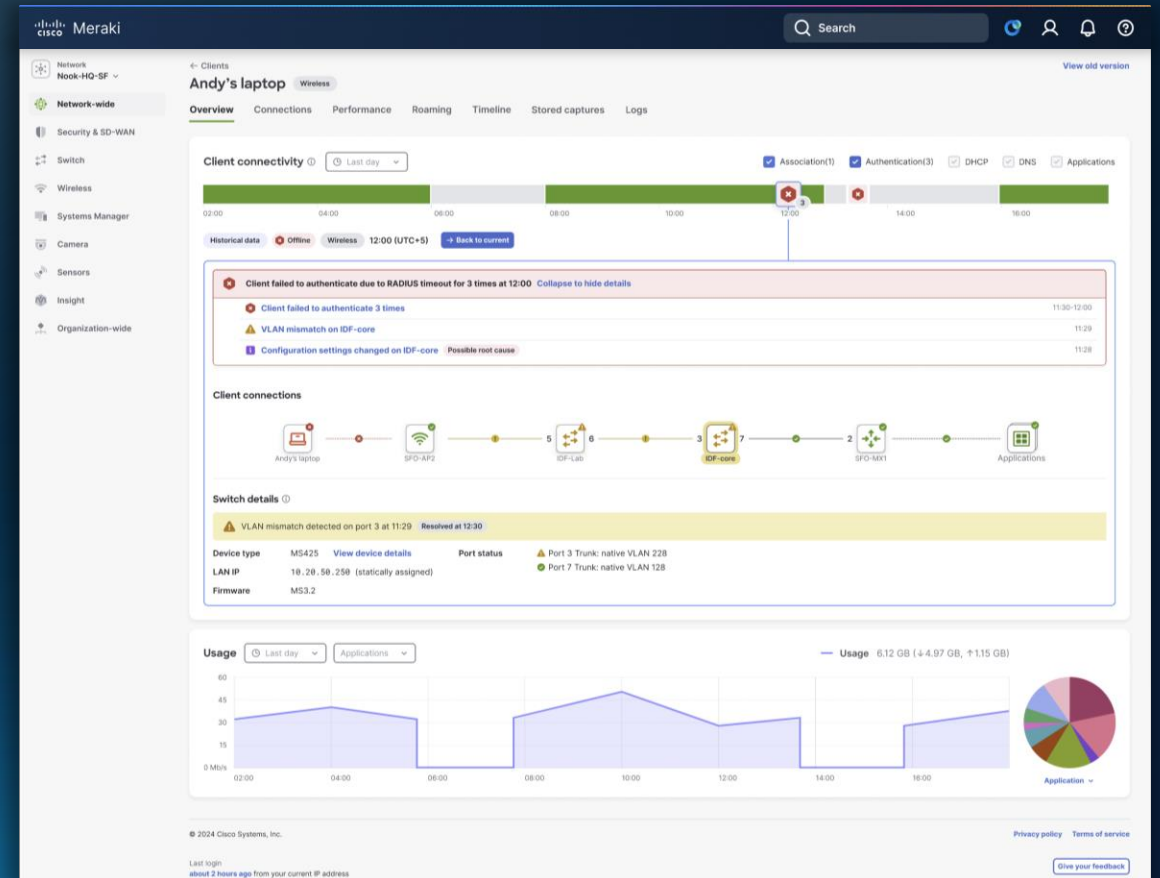
Assurance across every digital experience

Deep visibility into both owned and unowned networks

AI-powered insights surface experience-impacting issues instantly

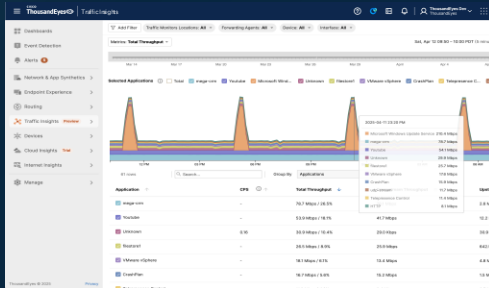
Closed-loop workflows trigger automated remediation

AI Assistant accelerates root cause analysis end-to-end



Deep visibility from campus to mobile to industrial

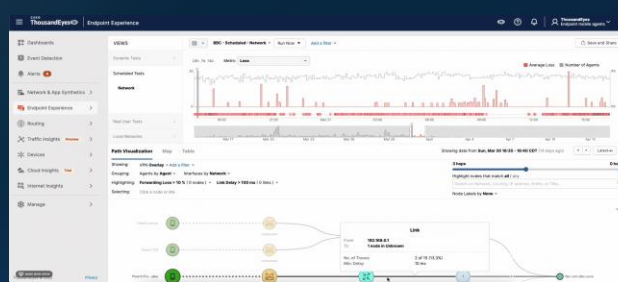
ThousandEyes Traffic Insights



Smarter visibility and planning
for enterprise networks

GA | JUNE

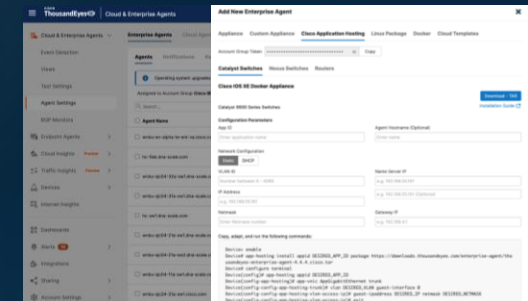
ThousandEyes Mobile endpoints



Extends Assurance to
mobile endpoints

BETA | NOW

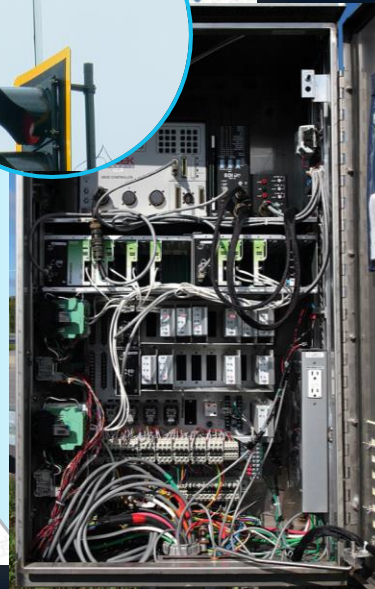
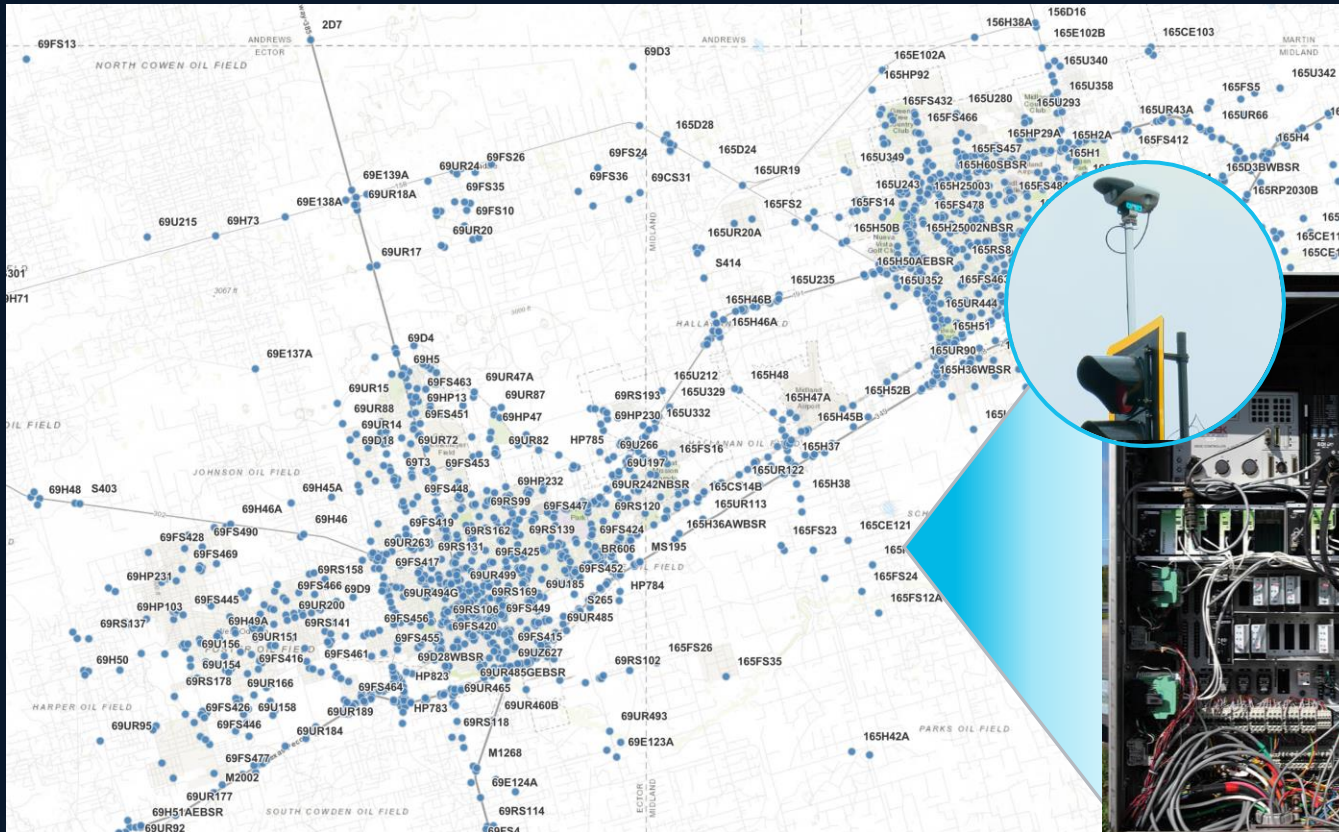
ThousandEyes Industrial Devices



Assurance for the industry's
largest Industrial IoT portfolio

GA | JULY

Example: Edge-to-cloud network assurance in roadways



Traffic control orchestration in the cloud

Inferencing at the Edge



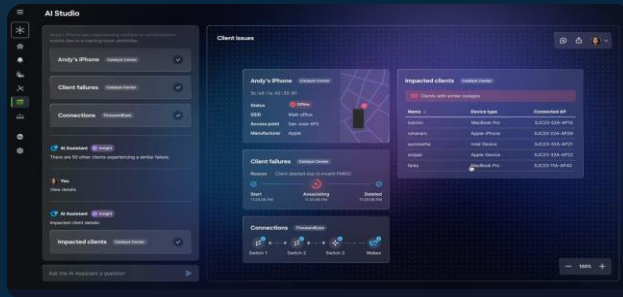
Driving the need for cybersecurity at the edge, and observability across customer owned and 3rd party networks between edge and cloud

The background is a dark blue field filled with a complex network of glowing lines and nodes. The lines are in shades of blue, purple, and orange, creating a sense of dynamic movement and connectivity. Nodes are represented by small circles and squares, some of which are highlighted with larger, more prominent outlines. The overall aesthetic is futuristic and technological, suggesting a digital or network environment.

IT/OT operations further simplified with AgenticOps

AgenticOp lineup

ALPHA | OCTOBER



AI Canvas

Cross-domain collaborative troubleshooting

BETA | JUNE



cisco
AI Assistant

AI Assistant

Accelerate network operations

POWERED BY DEEP NETWORK MODEL

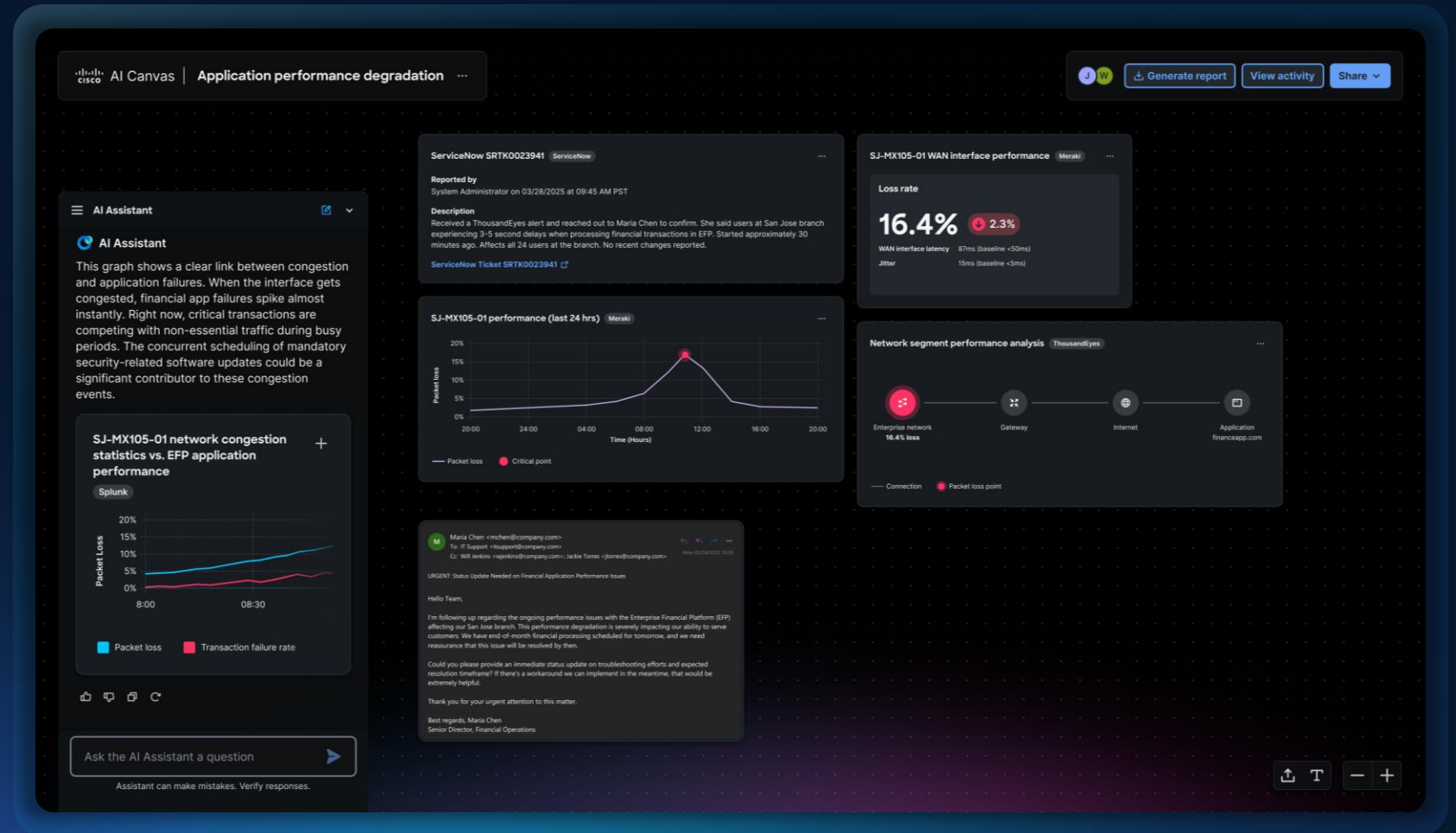
ALPHA | OCTOBER

AI Canvas

Troubleshooting and execution across multiple domains

Collaboration across multiple users (NetOps, SecOps and execs)

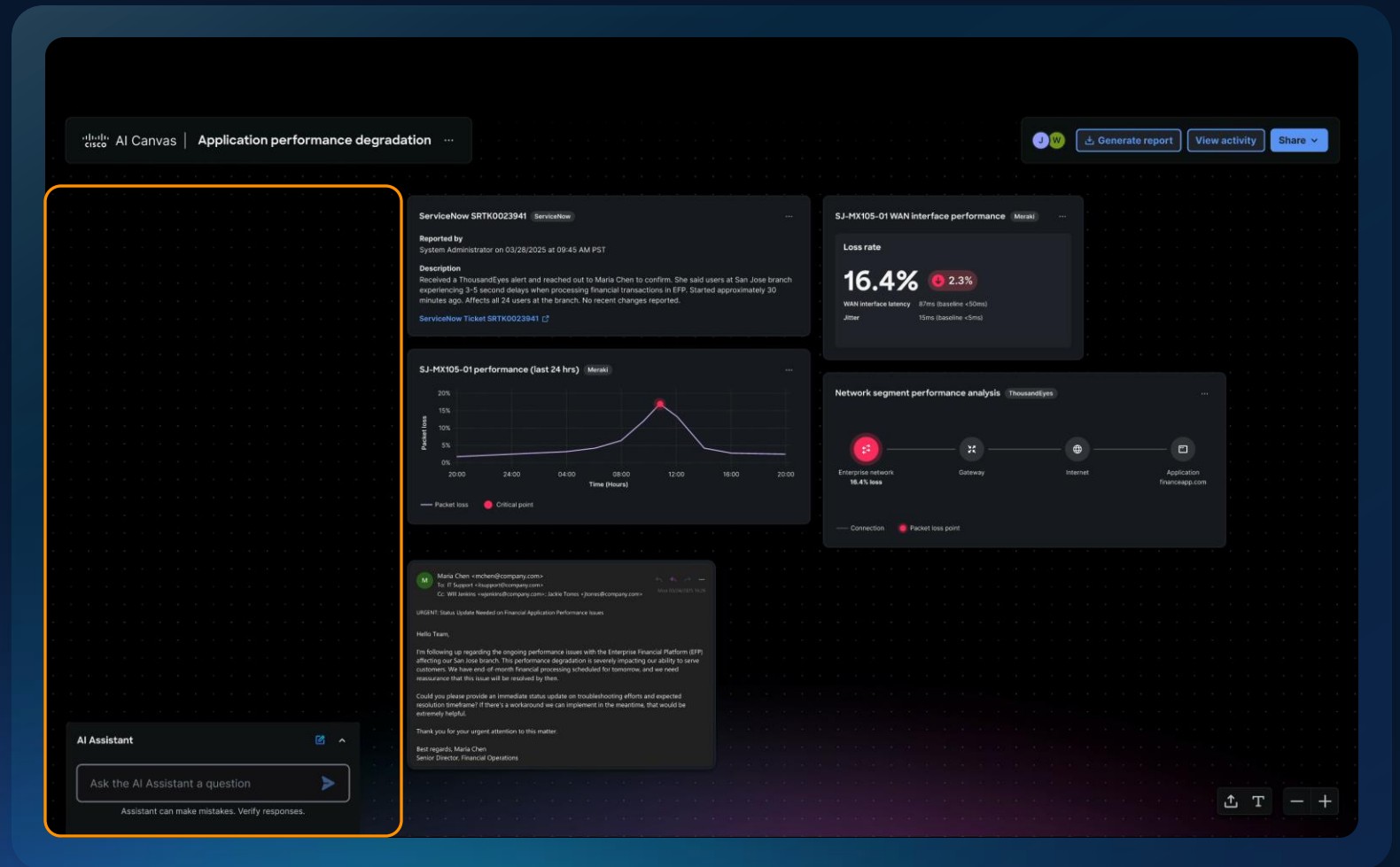
Built on the foundation of the Deep Network Model



AI Assistant embedded in AI Canvas

Interface to ask and explore in natural language

Guides you through diagnostics, decisions, and action inside the Canvas



AI Canvas

AgenticOps is powered by Deep Network Model

The most advanced networking LLM

Purpose-Built for Networking

20% more precise reasoning for troubleshooting, configuration, and automation.

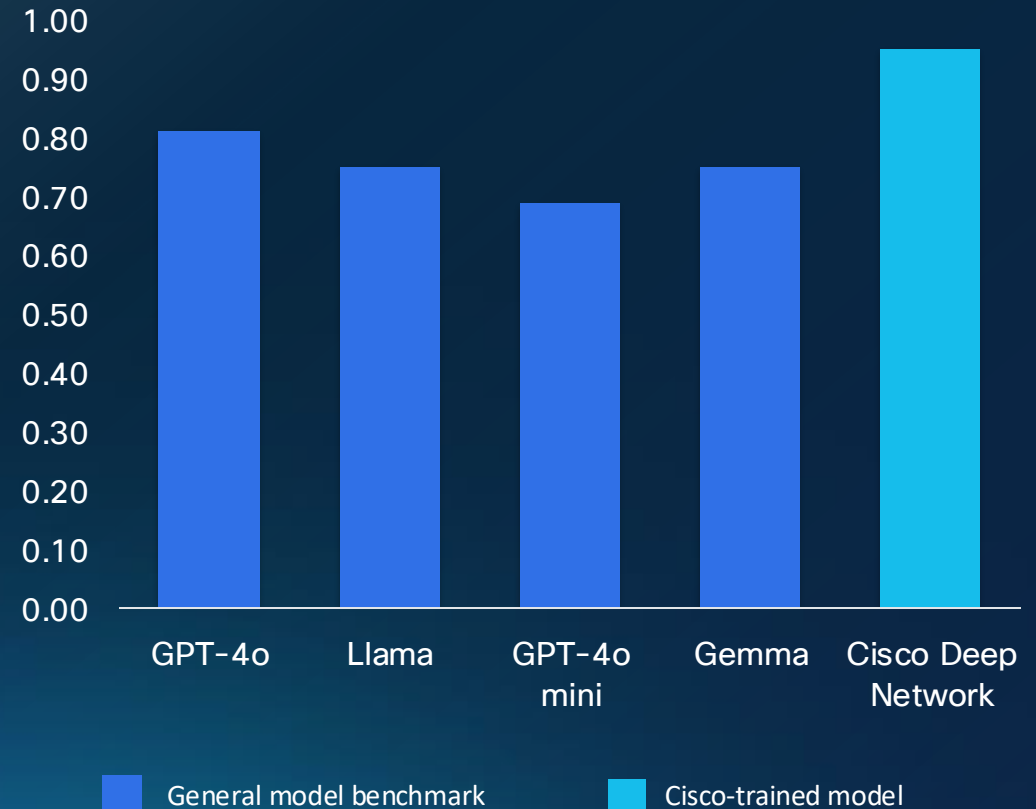
Trusted Training

Fine-tuned on 40+ years of CiscoU and CCIE-level expertise.

Continuous Learning

Evolves with live telemetry and real-world Cisco TAC and CX insights.

Outperforms general models by ~20%

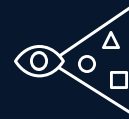


Accuracy on CCIE-style MCQs (590-question benchmark, May 2025)

Security fused into the network

Building cyber-resilient, AI-ready industrial networks

Cisco Industrial Threat Defense



Unified visibility across OT and IT

Insights to drive industrial security best practices and better detect threats traversing IT and OT domains



Adaptive network segmentation

Protect industrial operations by streamlining network segmentation to prevent attacks from spreading



Secure remote access

Get full control over remote access to industrial assets with a self-service ZTNA solution purpose-built for OT

Industrial security built into Cisco networking equipment to easily deploy at scale

Device vulnerabilities

Risk scoring

Automate segmentation below the IDMZ to protect operations



Grouping assets to reflect industrial processes is challenging



Thousands of assets



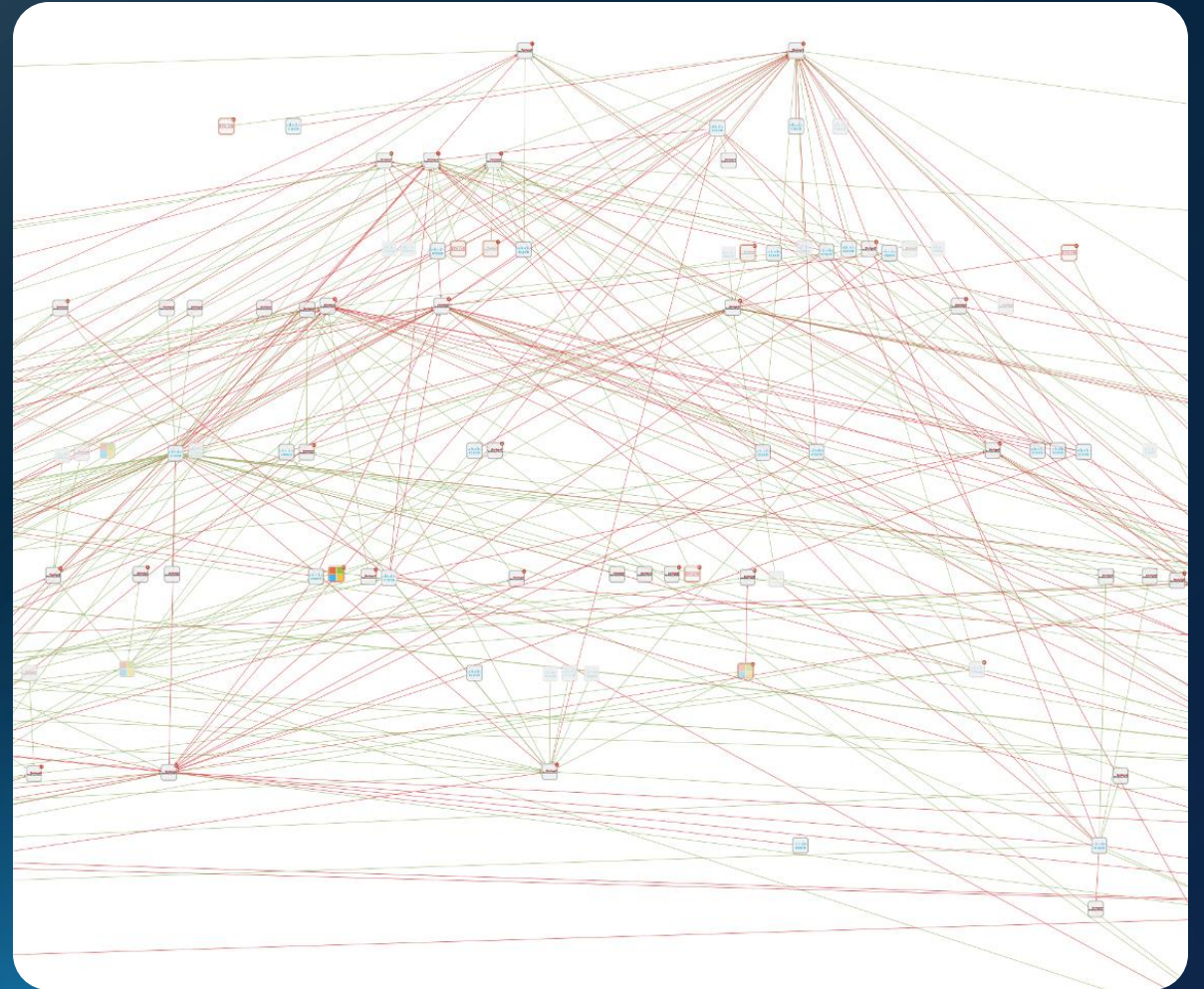
Millions of flows



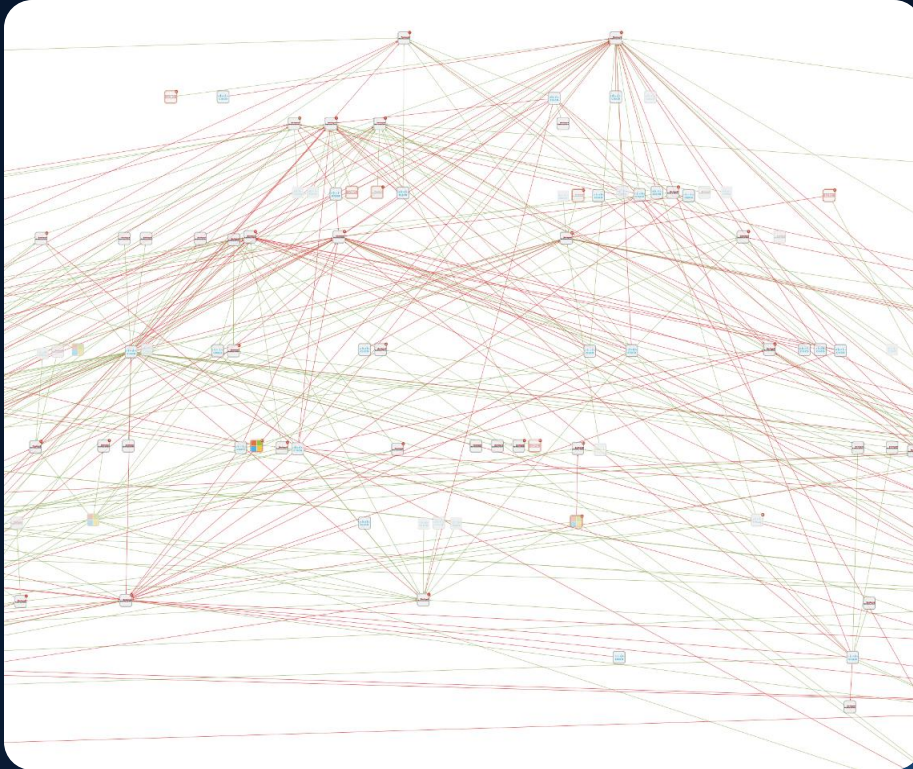
Broadcast, multicast traffic spreading across flat networks



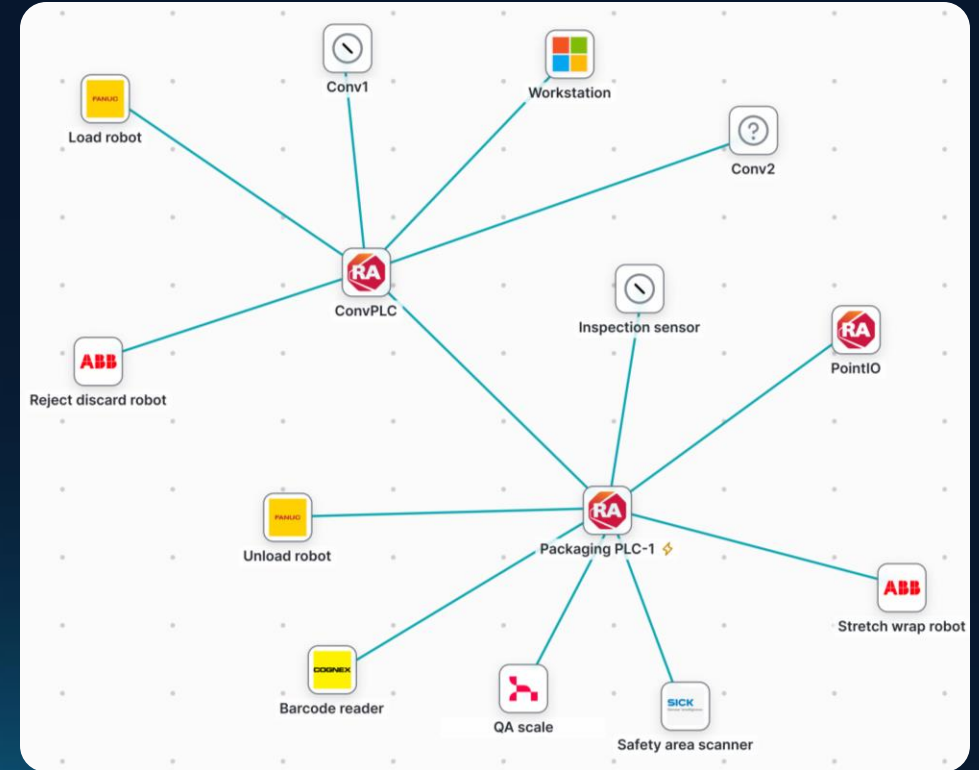
Hard for a human to group assets



Introducing AI-based clustering for segmentation



OT asset inventory projects highlight flat, unsegmented networks



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

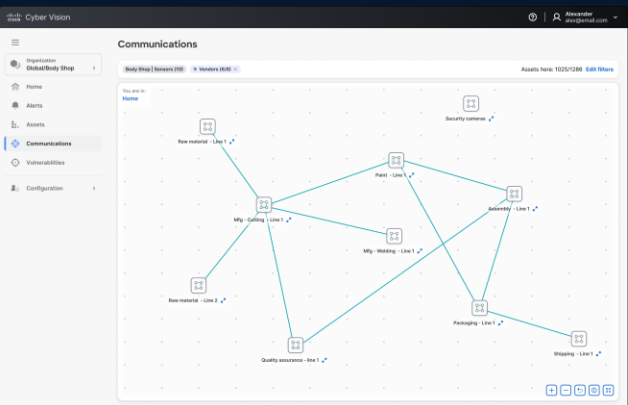
Visibility driven segmentation with Identity Services Engine



Grouping assets
in Cyber Vision

Drives TrustSec
Auth policy in ISE

Segmentation enforced by
switches and routers

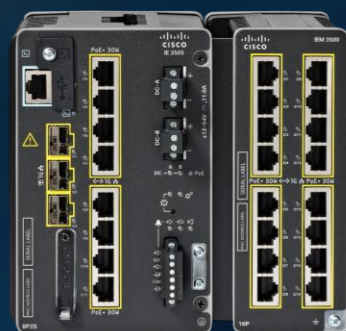


PxGrid

Groups	
Groups	✗ ✓ ✗ ✓ ✓ ✓
	✓ ✓ ✗ ✓ ✗ ✗
	✗ ✓ ✓ ✗ ✗ ✗



RADIUS



Zero downtime with OT controlled adaptive access policies

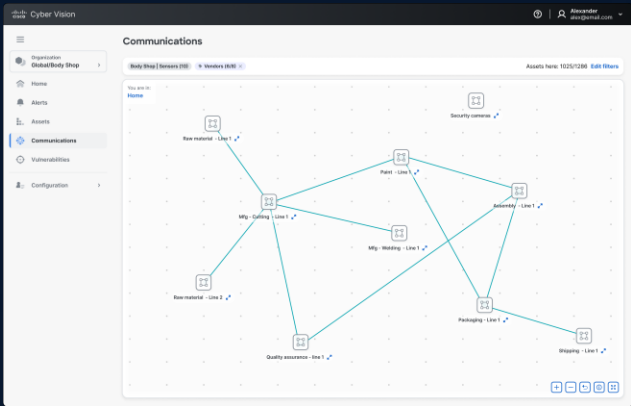
Visibility driven perimeter defense with Secure Firewall



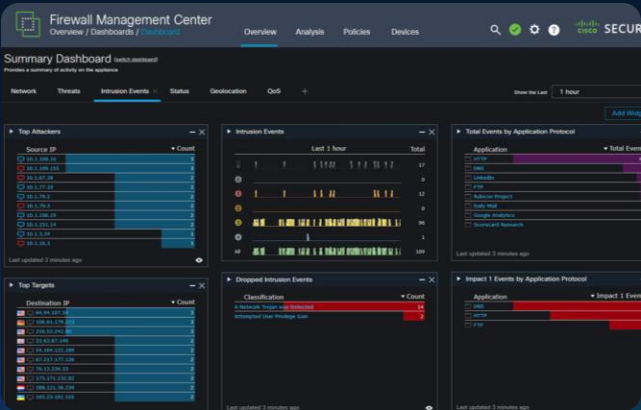
Grouping assets
in Cyber Vision

Drives TrustSec
Auth policy in ISE

Segmentation enforced by
switches and routers



PxGrid



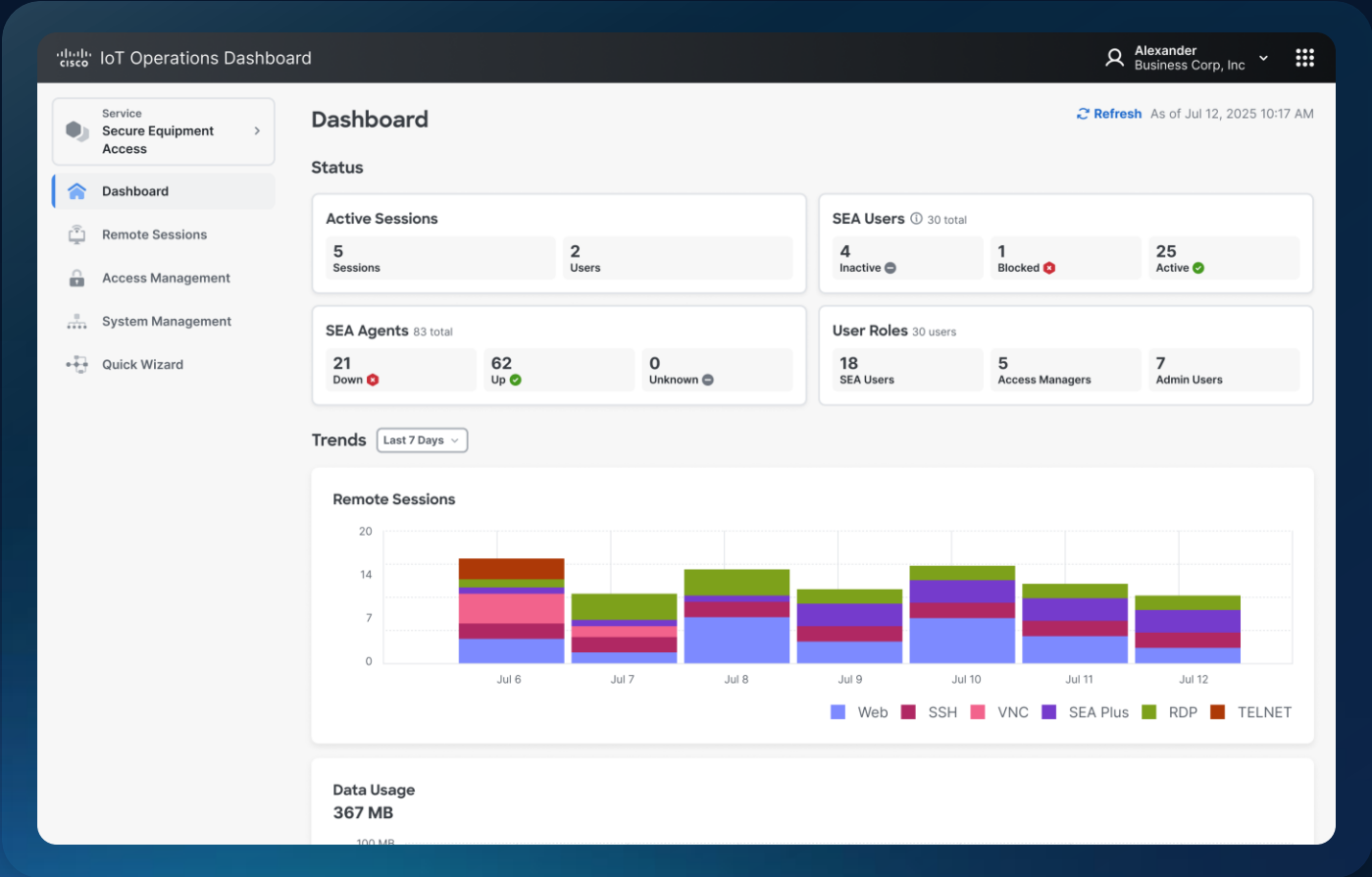
RADIUS



Zero downtime with OT controlled adaptive firewall rules

Secure Equipment Access

Network embedded **Zero Trust Remote Access** to your OT assets



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

Service Secure Equipment Access

Dashboard

Alerts

Remote Sessions

Access Management

System Management

Audit Reports

Configuration

Active Alerts

Login From Prohibited Location Critical

China

Summary

2 users have logged in from China 3 times. 1 access administrator, and 1 remote user.

Active instances

Search Days inactive Filters 2 results

Service Secure Equipment Access

Dashboard

Alerts

Remote Sessions

Access Management

System Management

Audit Reports

Configuration

Active Alerts

Login Outside of Working Hours Medium

username@email.com

Summary

user@email.com logged in 2 times outside of approved working hours.

Logins outside of approved hours

PDT

Thursday Dec 12, 2024

Tuesday Dec 10, 2024

Designated working hours Login with no sessions Login with sessions

Active instances

Search

Settings

Login Time	Discrepancy	Alert Rules	Occurrences	Severity	Last Time Detected
Dec 12, 2024 10:31 PM	3 hr 1 min	1	1	Medium	Dec 12, 2024 10:31 PM
Dec 10, 2024 2:15 AM	4 hr 30 min	1	1	Medium	Dec 10, 2024 2:15 AM

The background of the slide is a dark blue field filled with dynamic, flowing light streaks. These streaks are primarily in shades of bright blue and cyan, with some warmer orange and pinkish tones visible in the upper right quadrant. The lines are curved and layered, creating a sense of depth and movement, reminiscent of light trails or data flow.

Scalable devices ready for AI

Helping industries digitize by bringing IT to the OT world

Choose the best tool for each use case with increasing leverage



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

19 versatile
form factors

54 Gbps
throughput

720W per
switch

Cyber Vision
embedded
security

Introducing

All New Industrial Ethernet Portfolio



AVAILABLE JULY 2025

Cisco IE3100/H | Cisco IE3500/H | Cisco IE9300

Announcing 19 new switches joining Cisco's leading portfolio

DIN-rail Portfolio



8x

+



2x

NEW!

Cisco IE3100 - Compact 4PPoE



2x

Cisco IE3200



4x

Cisco IE3300



2x

Cisco IE3400

NEW!



6x

Cisco IE3500

IP67 Portfolio

NEW!



2x

Cisco IE3100H - Compact



6x

Cisco IE3400H

NEW!



8x

Cisco IE3500H

Rackmount Portfolio



4x

Cisco IE9300 - All Copper



3x

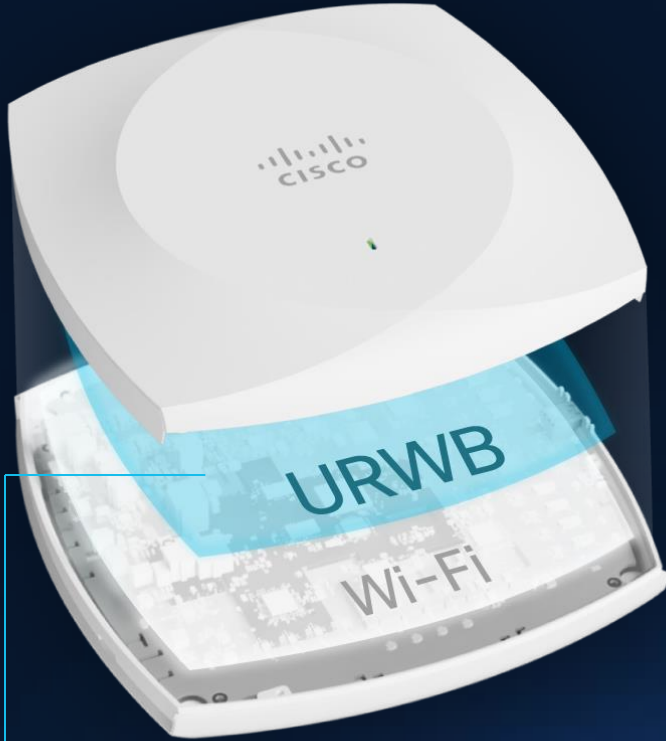
Cisco IE9300 - All Fiber

NEW!



Cisco IE9300 - Mixed Ports

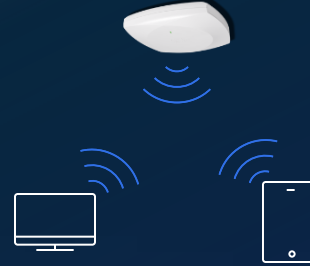
Unified Wi-Fi and URWB infrastructure



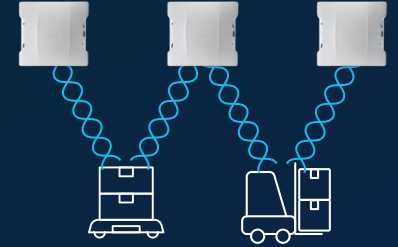
Ultra-Reliable Wireless
Backhaul built-in Enterprise
Wi-Fi Access Points

Before

Wi-Fi
Access
Network



Industrial
Wireless
Network



Now



Unified Wireless Infrastructure

One management platform, One wireless infrastructure to install
Best of Wi-Fi combined with use new cases enabled by URWB technology

Leadership in Industrial Networking



Cisco's IIoT Leadership

20+ years of industrial networking experience
making Industrial Ethernet equipment

Market leadership across all product categories

- Industrial Edge Networking Marketing Leader 2024 by Omdia
- OT Security Solutions Market Leader 2024 by Forrester
- Industrial Ethernet Switching Market Leader 2024 by ARC
- Industrial and Outdoor Wireless LAN infrastructure Market Leader by ARC
- IIoT Company of the Year 2025 by IoT Breakthrough awards

Expansive vertical customer depth

Manufacturing

52,000+

companies in
139 countries

Utilities

19,000+

customers in
163 countries

Transportation

32,000+

organizations in
169 countries

Introducing a Generational Industrial Experience

- Announcing 19 new switches joining Cisco's leading portfolio
- Unifying Wi-Fi and Cisco's URWB infrastructure for one management platform and one wireless infrastructure to install



“In Q2, we saw growth of more than 50%, signaling an acceleration as customers prepare for the deployment of AI-powered robotics and industrial security.”

Chuck Robbins, CEO, Cisco

Thank you



