CISCO Connect

Modernizing Industrial Networks for Cybersecurity & AI

Mark Knellinger- Business Solutions Architect

April 7, 2026

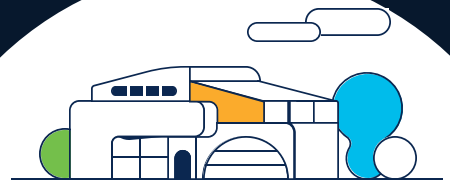
Networks Are Extending Beyond Carpeted Spaces

Enterprise Operations

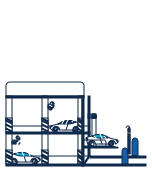
Extending the IT network beyond traditional climate-controlled spaces to non-carpeted areas.

Industrial Operations

Connecting operational technologies to help industries digitize and get ready for what's next.



Enterprise Solutions



Parking

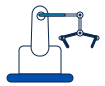
Roadways

Transportation

Renewables

EV chargers

Utilities

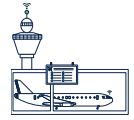


Manufacturing

Oil & Gas

Mining

Warehouses



Airports

Seaports

Connecting outdoor and industrial environments

cisco

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

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 Sees the Network as the Key to Unlock Software-Driven Industrial Automation and Industrial AI

Brains
in the data center or the cloud

VIRTUAL ROBOT CONTROLLER

VIRTUAL PLC/RTU

VIRTUAL COMPUTE

Nervous system
is the network

Network

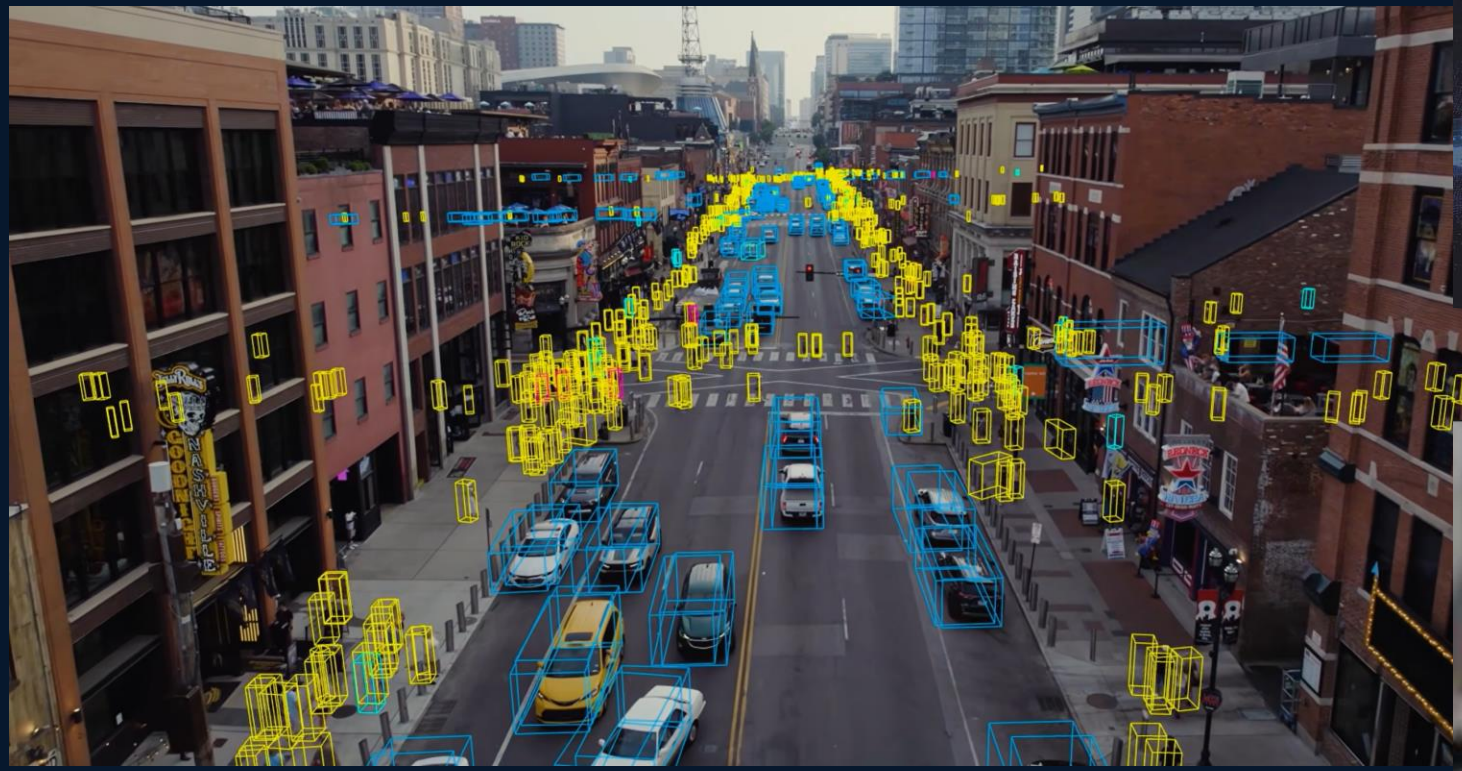
Physical components
in the field

ROBOTS, VEHICLES

FIELD ASSETS

SENSORS

LiDAR in Nashville

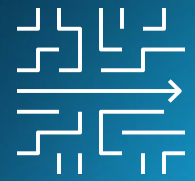


[Broadway LIDAR 2025 - YouTube]

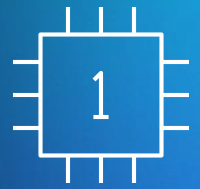
This requires a new architecture for industrial networks

Cisco's Industrial IoT Portfolio

Operational Simplicity
powered by AI



Scalable Devices
ready for AI



Security
fused into the network

cisco

Our Unified Platform – Managing IT/OT Portfolio

PLATFORM

Management

Assurance

API / Integrations

Intelligence - AgenticOps

HARDWARE

Smart Switches

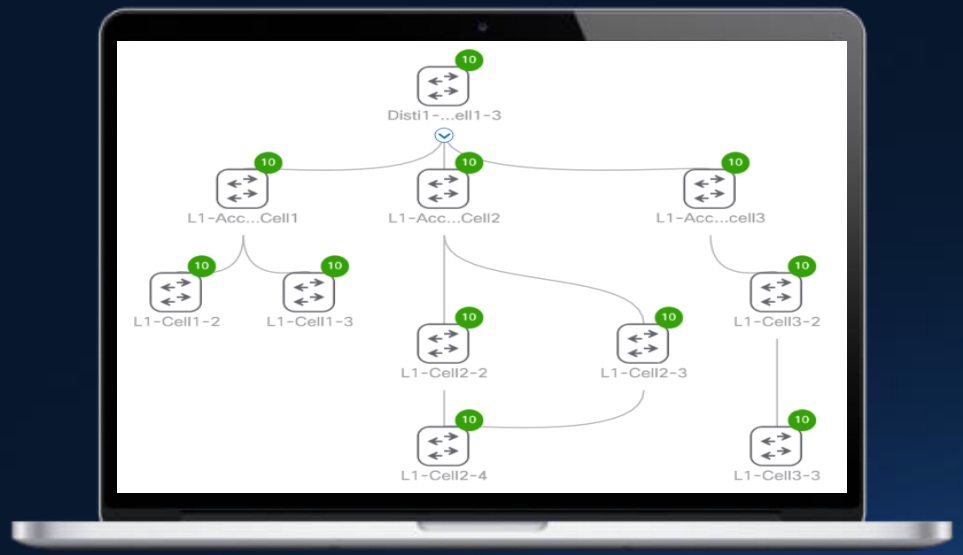
Secure Routers

Wireless

Industrial IoT

cisco

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

Extend IT to Operational Environments

Industrial Edge Leader
Omdia 2024

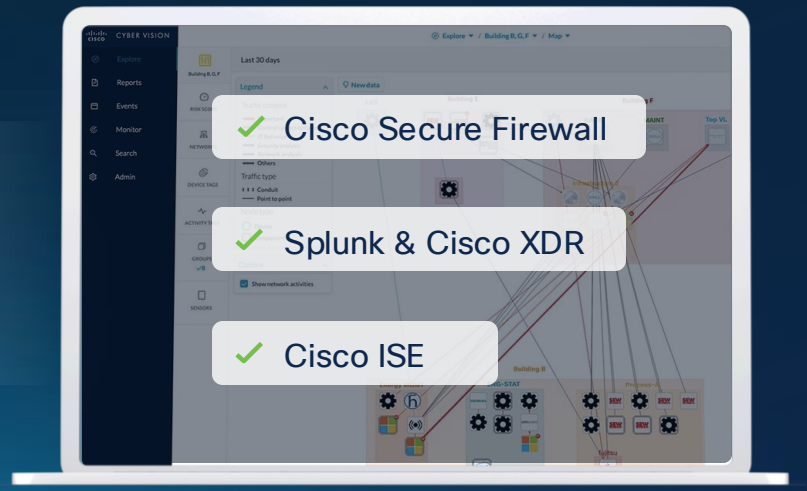
Industrial Ethernet
Switching Leader
ARC 2024

OT Security Leader
Forrester Wave 2024

Industry leading industrial networking portfolio

+

Cisco industrial security

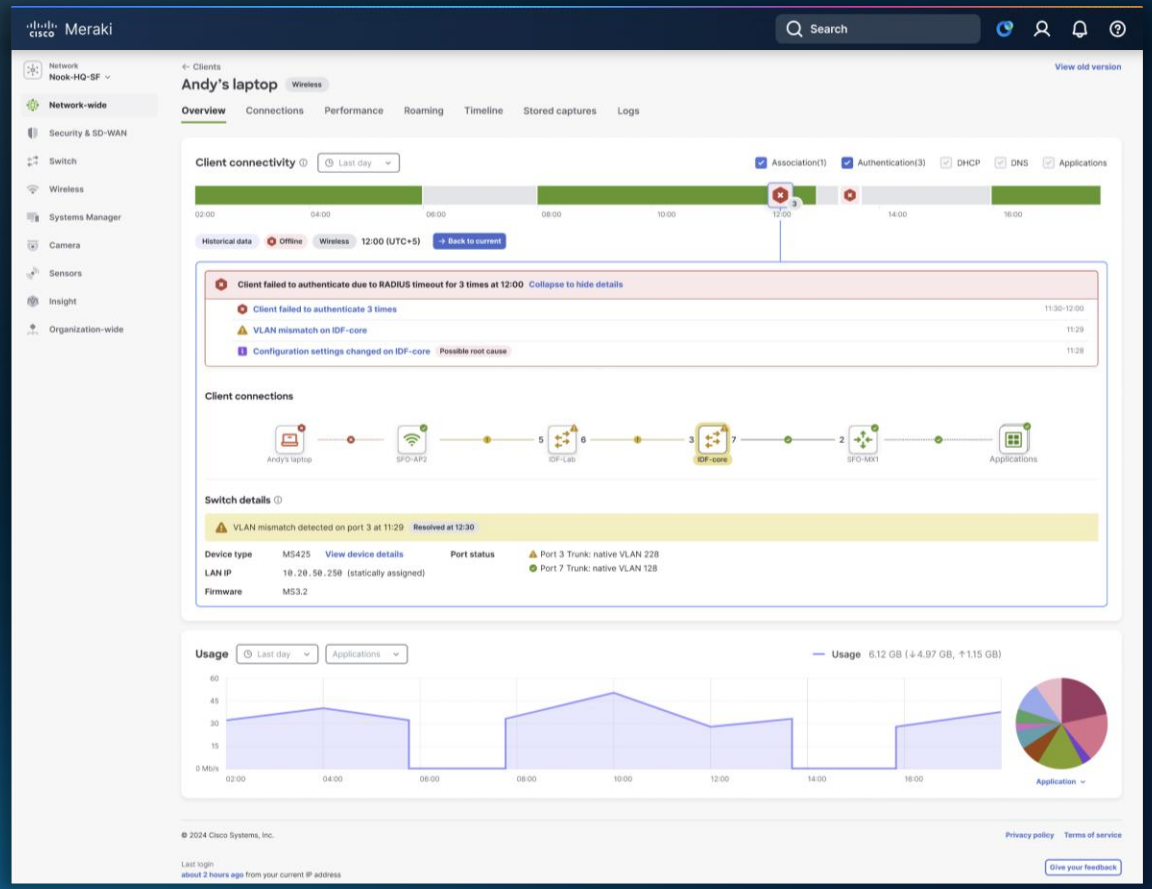


Cyber Vision Center

AVAILABLE | NOW

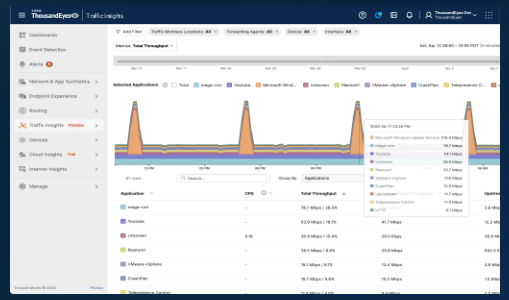
Assurance Across Every Digital Experience

- 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

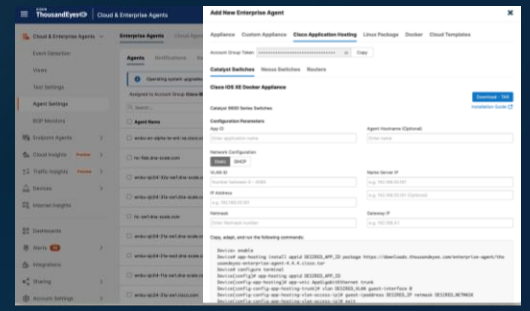
GA | JUNE

ThousandEyes Mobile endpoints

Extends Assurance to mobile endpoints

BETA | NOW

ThousandEyes Industrial Devices



Assurance for the industry's largest Industrial IoT portfolio

GA | JULY

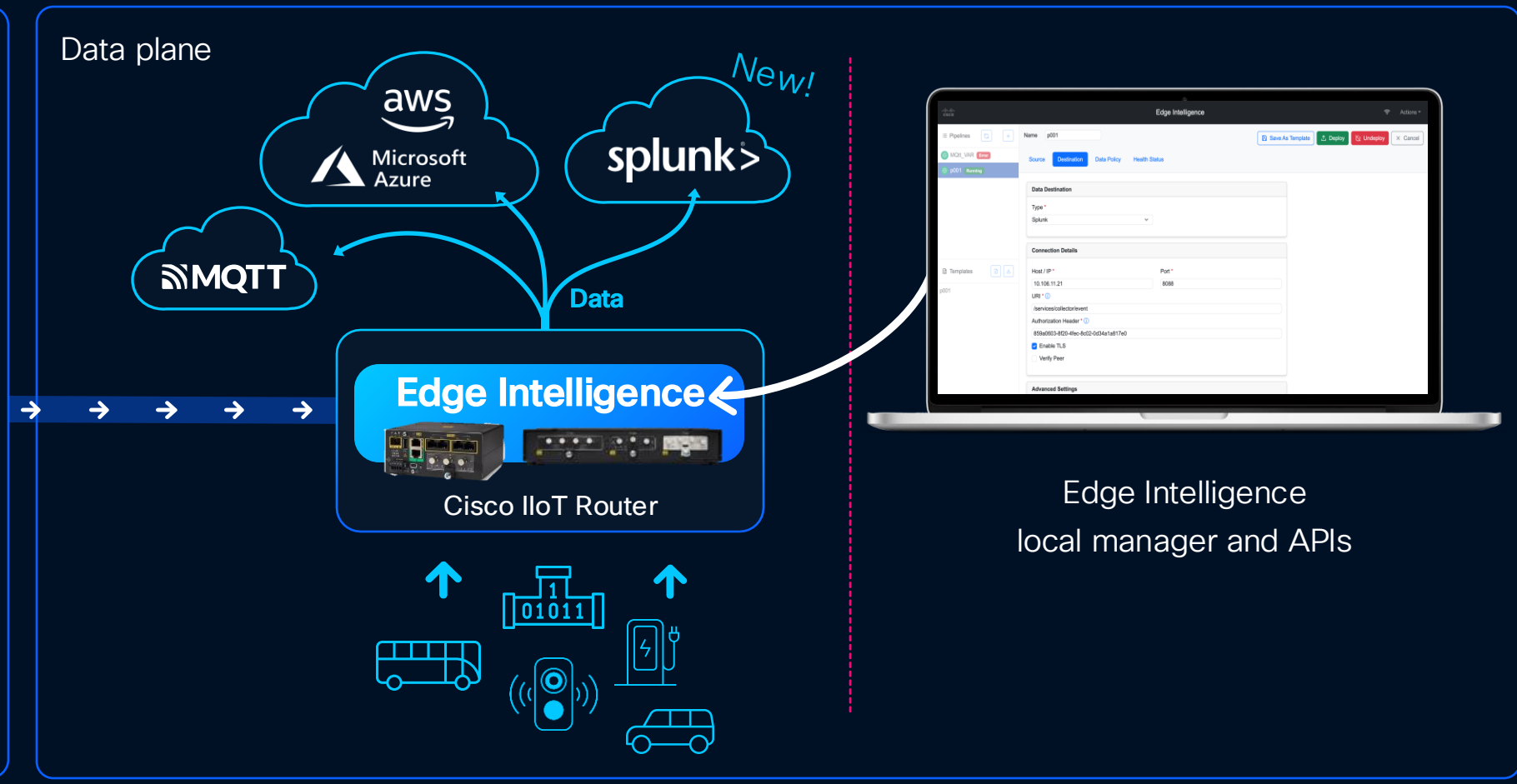
Ensuring Clean Normalized Data for AI

Extract
Seamlessly extract data from disparate sources

Transform
Convert raw data to intelligence

Govern
Control when and where data goes

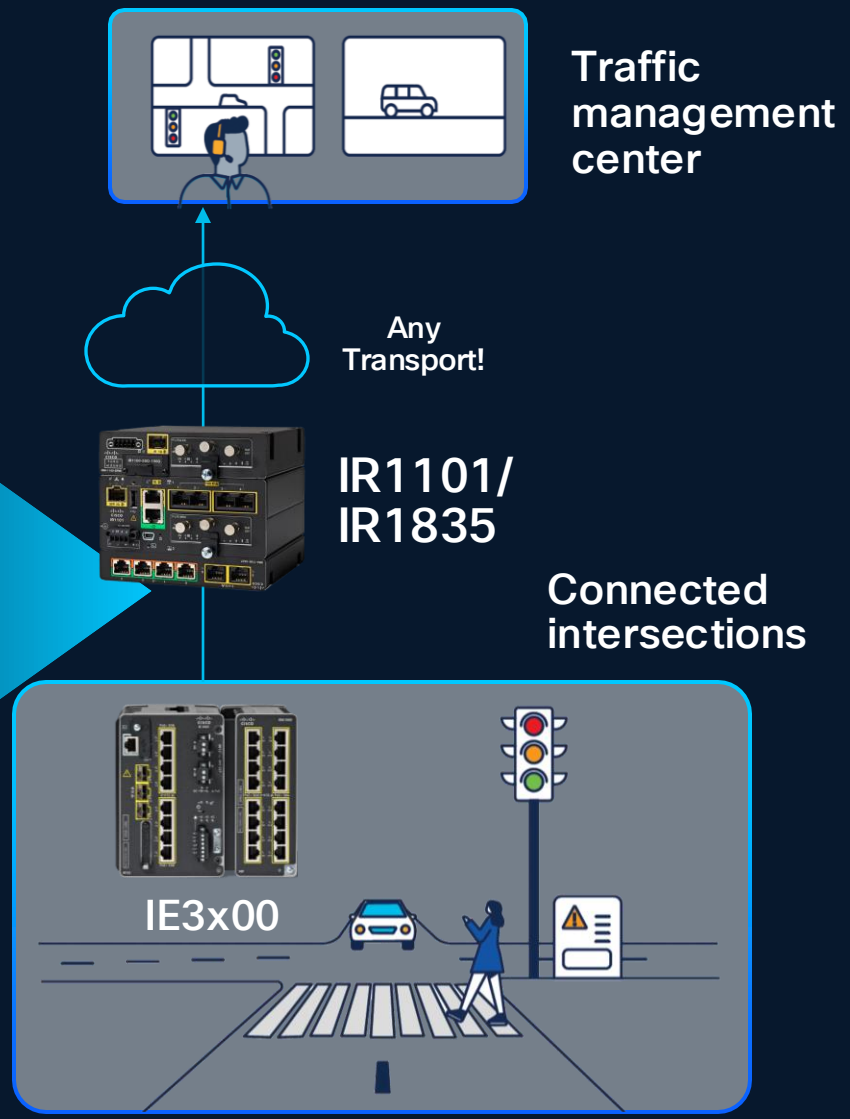
Deliver
Create data access policies at the edge and auto-deploy them for secure delivery



Easily configure and deploy data governance policies with Edge Intelligence

Reduce Complexity at the Roadside

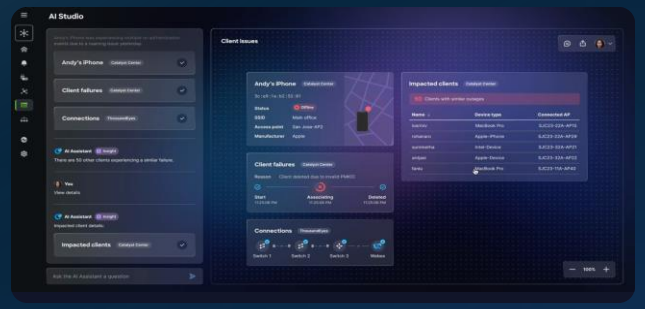
- Catalyst SD Edge
- Layer 7 Zone-Based Firewall, inc. IPS
- Cyber Vision Sensor
- Edge Intelligence
- Secure Equipment Access



IT/OT Operations Further Simplified with AgenticOps

AgenticOp Lineup

ALPHA I OCTOBER



AI Canvas

Cross-domain collaborative troubleshooting

BETA I JUNE

cisco AI Assistant

AI Assistant

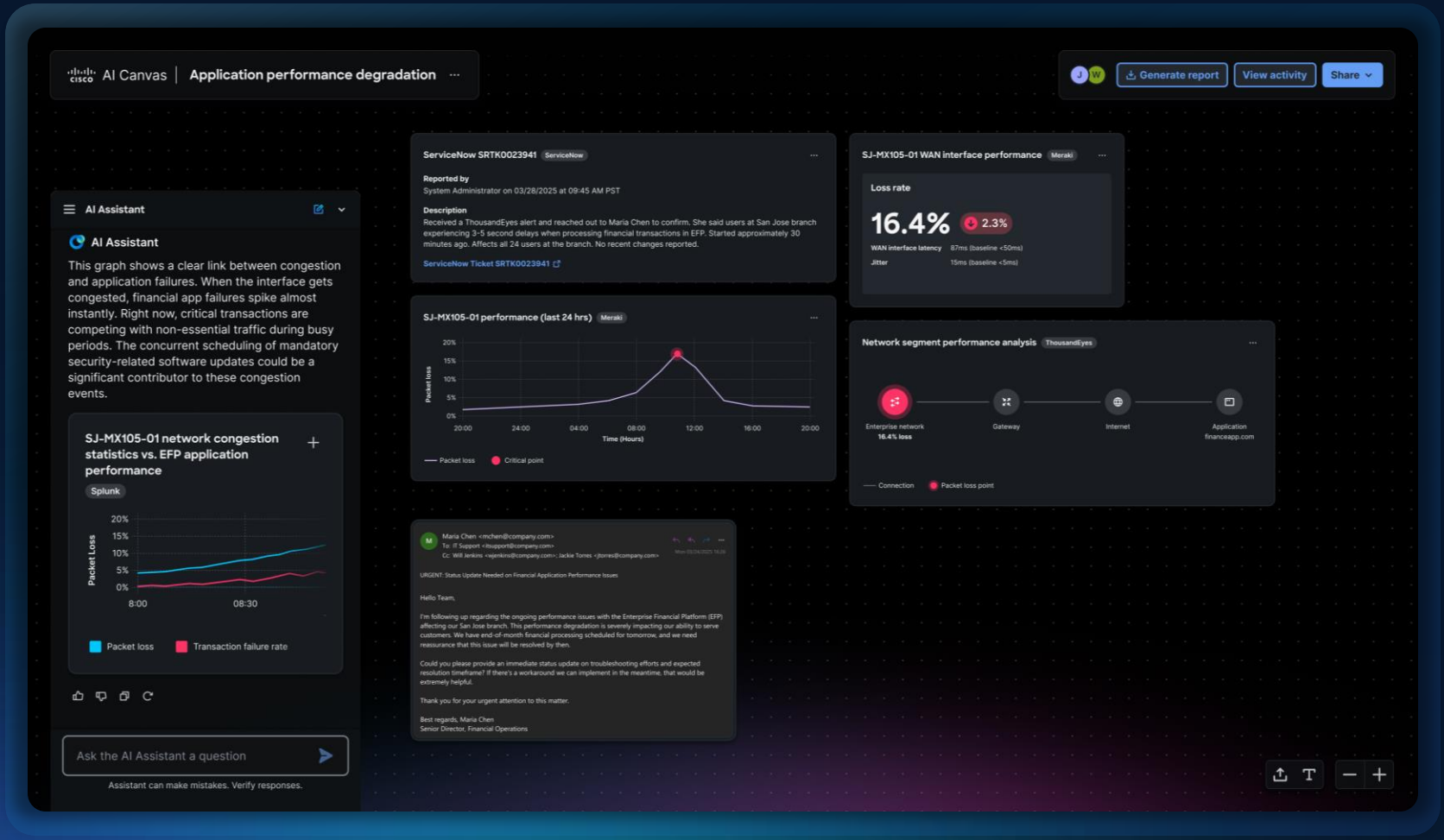
Accelerate network operations

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



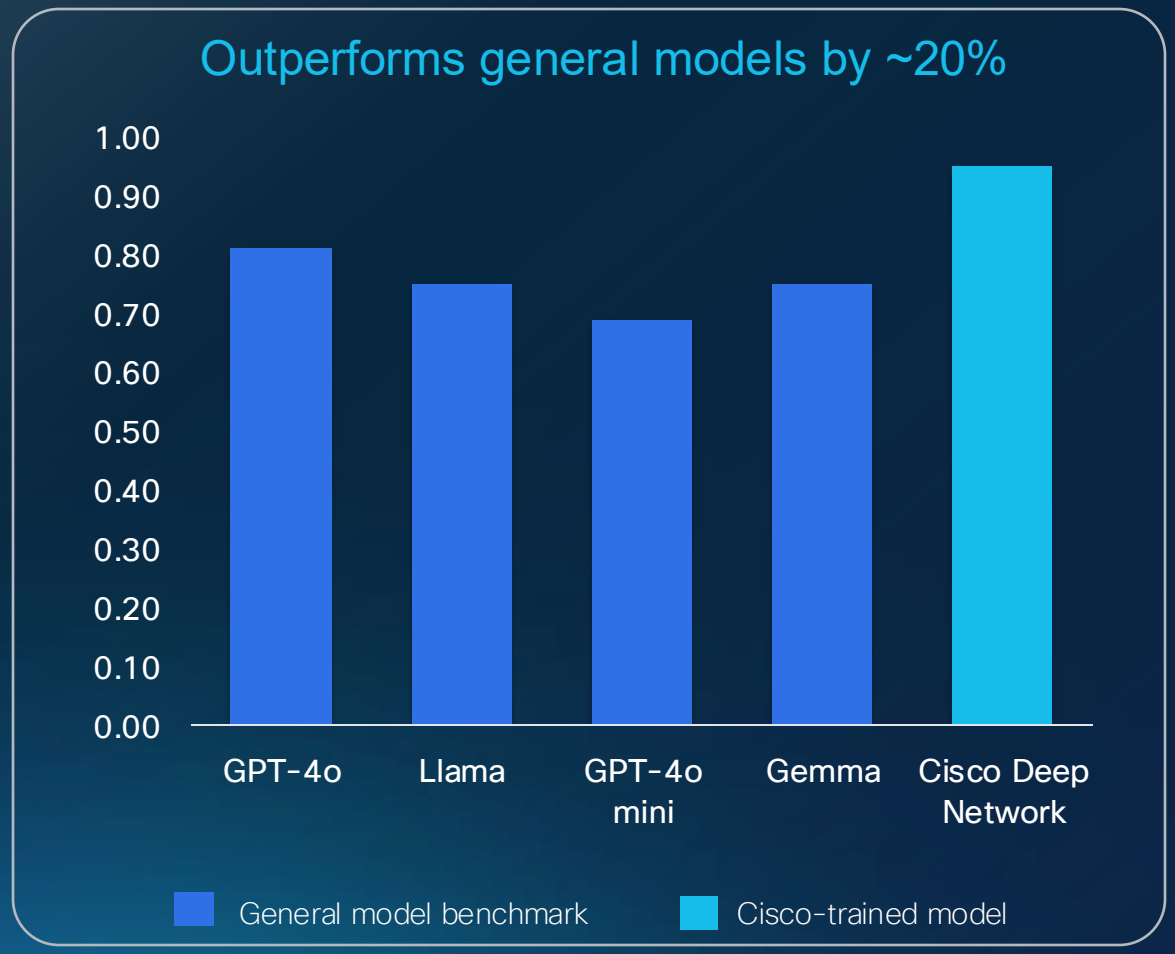
AgenticOps Is Powered by Deep Network Model

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.

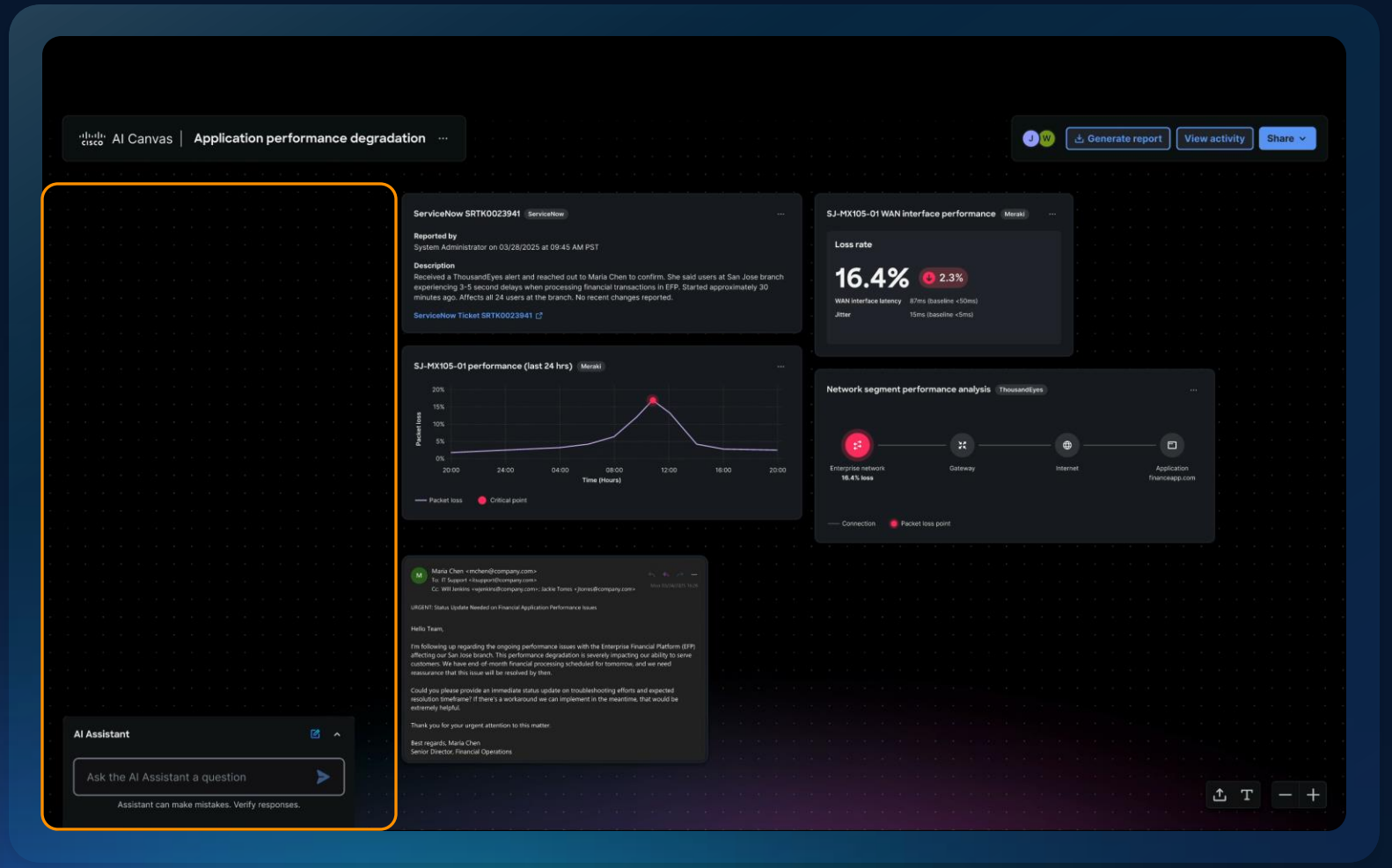


Accuracy on CCIE-style MCQs (590-question benchmark, May 2025)

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

Cisco Network as a Fabric to Secure OT at Scale

OT Visibility
embedded in
network equipment

Secure Remote Access
gateway embedded in network
equipment

Segmentation Policies
enforced by network
equipment

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

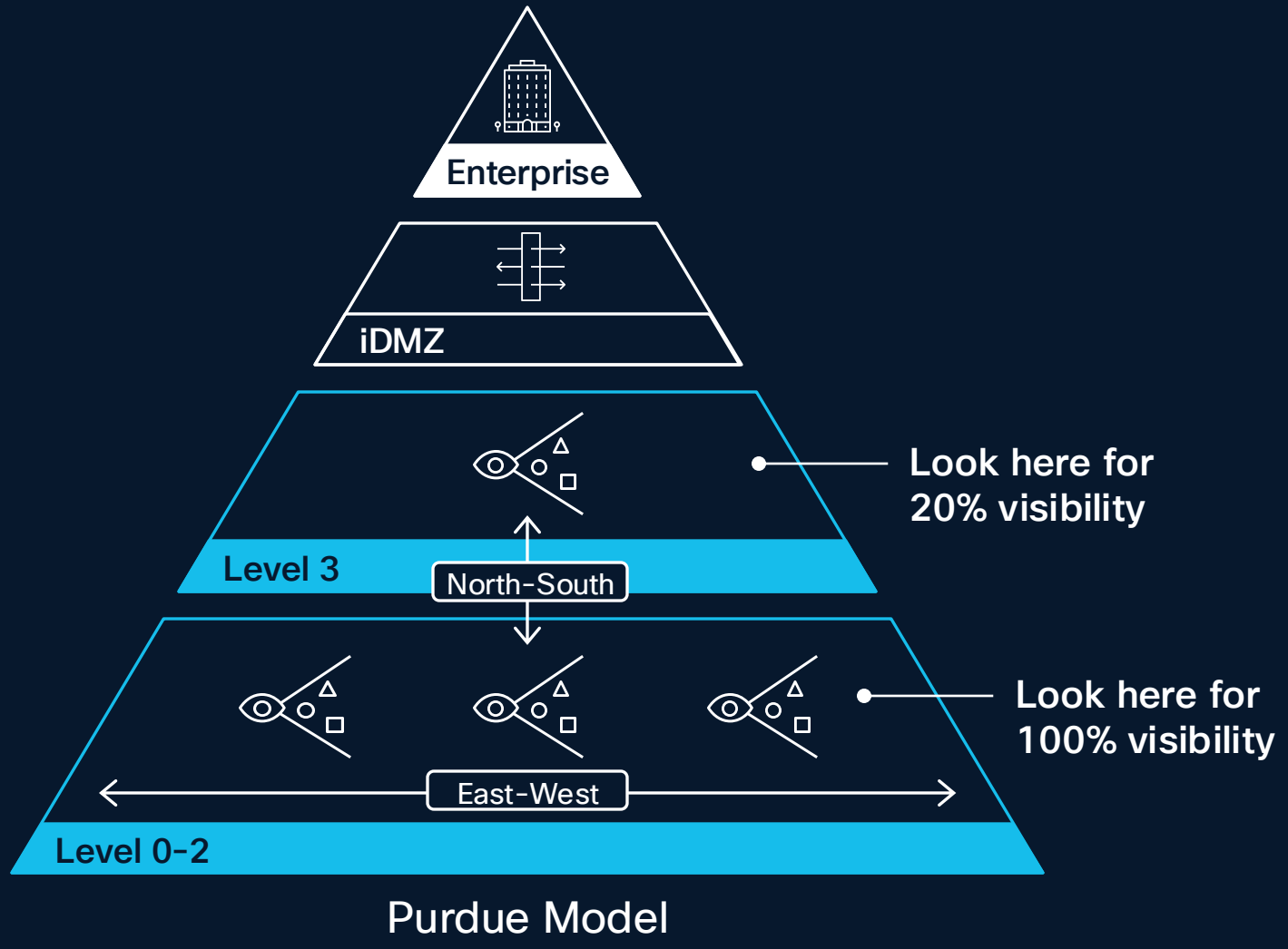
Protect industrial operations by streamlining network segmentation to prevent attacks from spreading

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

Security Starts With Visibility, but Where You Look Matters

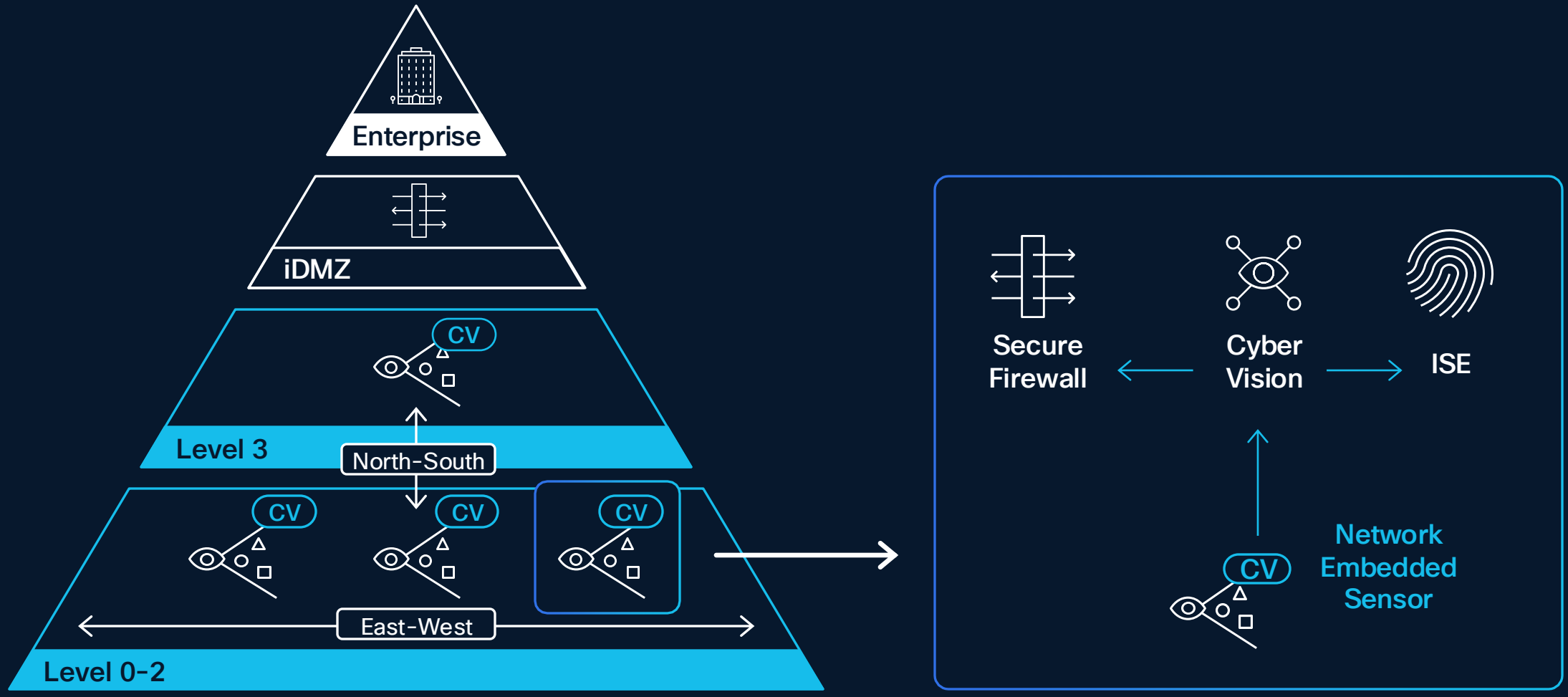


Purdue Model

Visibility to Level 0-2 using SPAN or hardware appliances is expensive and complex

You run the risk of downtime if you try to segment Level 0-2 without 100% visibility

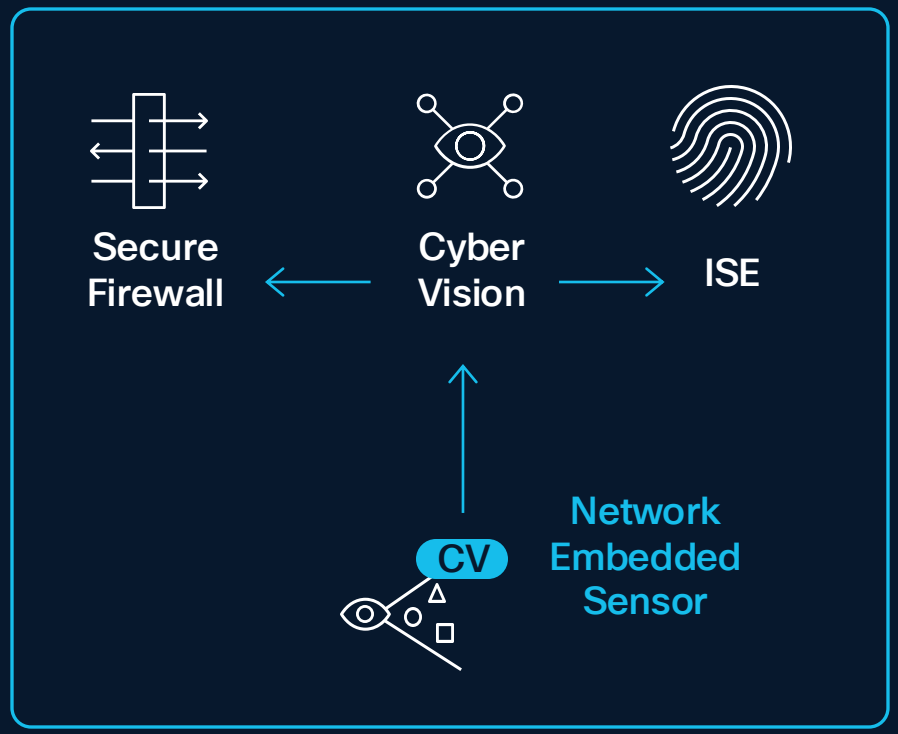
Visibility Driven Adaptive Segmentation



Purdue Model

Visibility Driven Adaptive Segmentation

- Security policies abstracted to mirror industrial processes
- Network or firewall enforced micro or macro segmentation
- Enforcement policy dynamically updates based on Cyber Vision mapping



Cyber Vision

Visibility

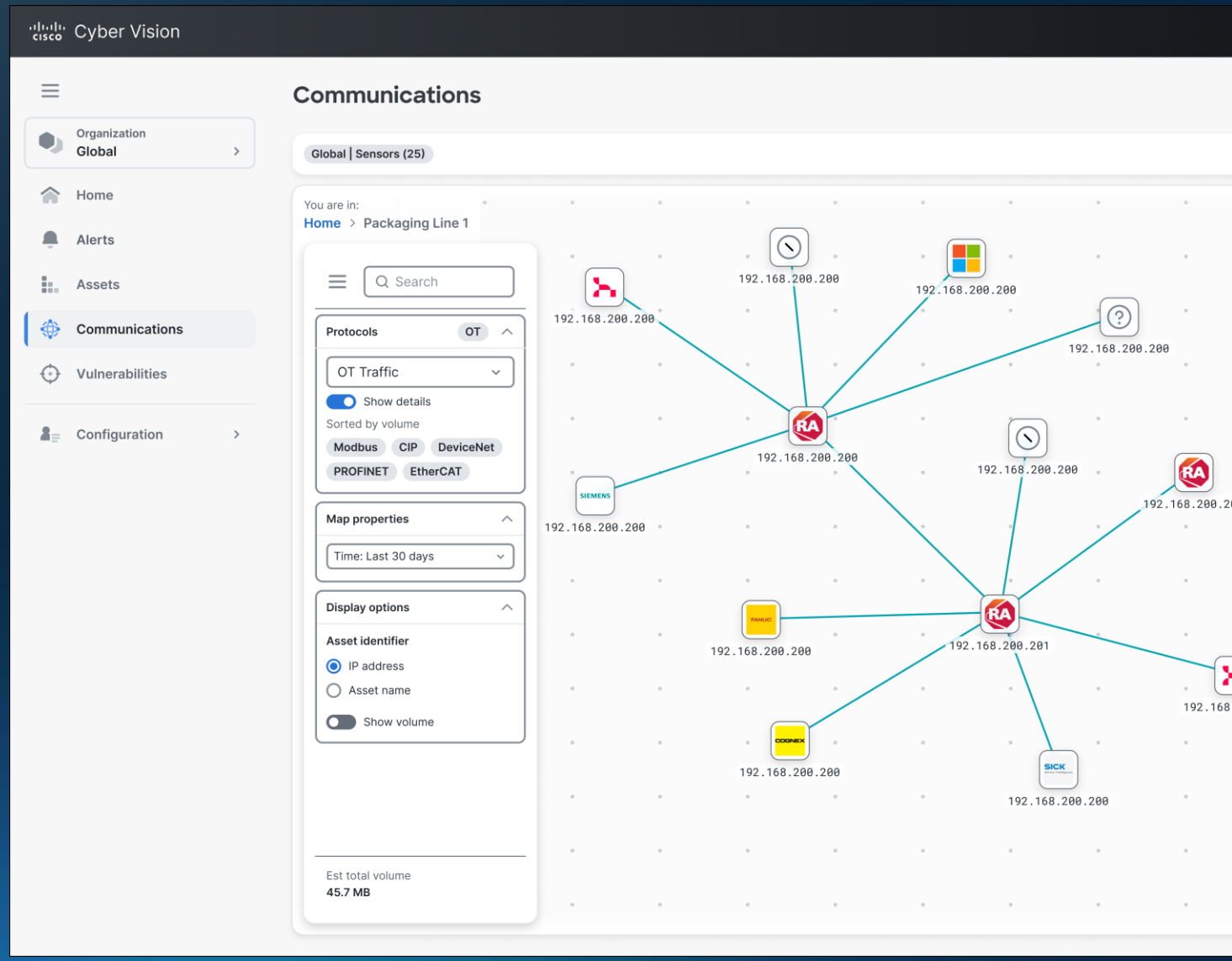
OT asset inventory
Communication patterns

Security Posture

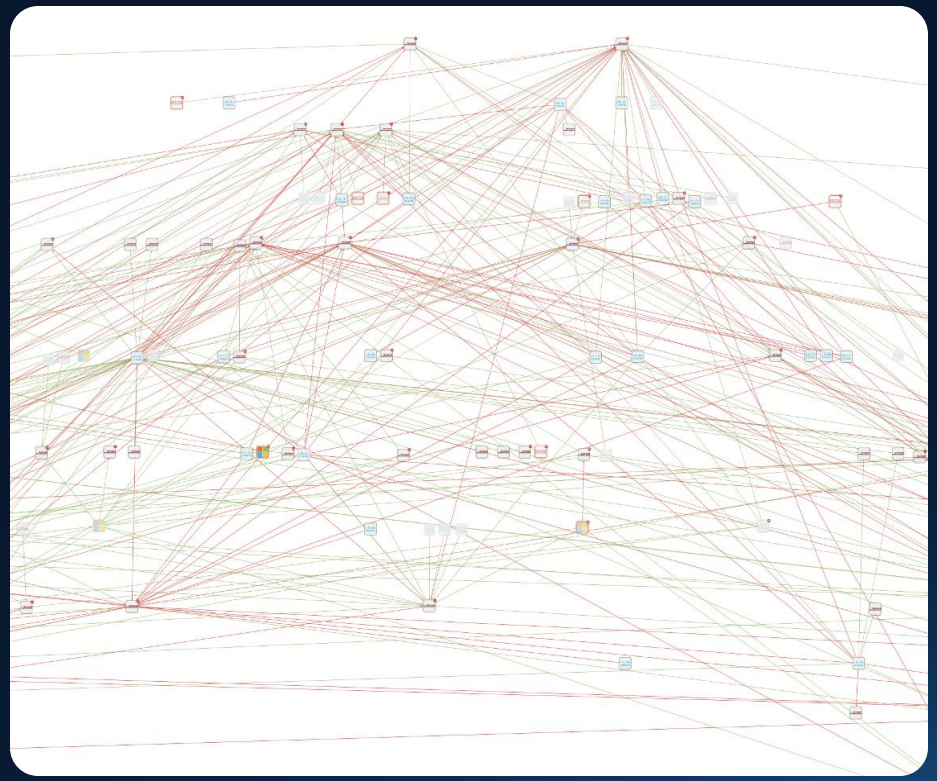
Device vulnerabilities
Risk scoring

Operational Insights

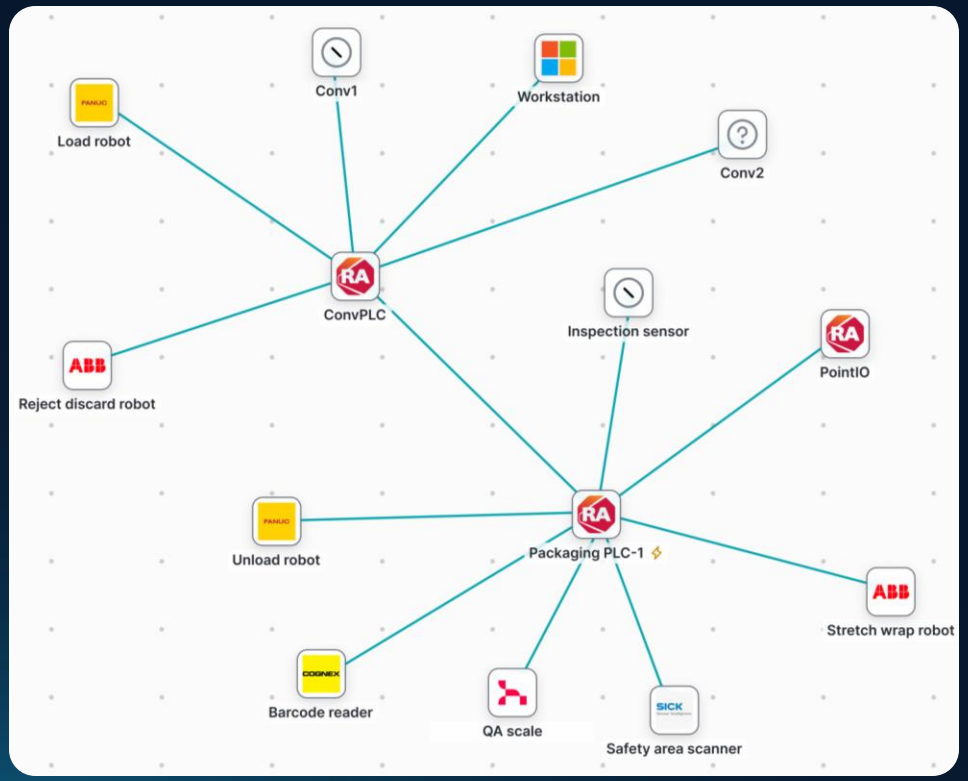
Track process/device modifications
Record control system events



Introducing AI-Based Clustering for Segmentation



OT asset inventory projects highlight flat, unsegmented networks



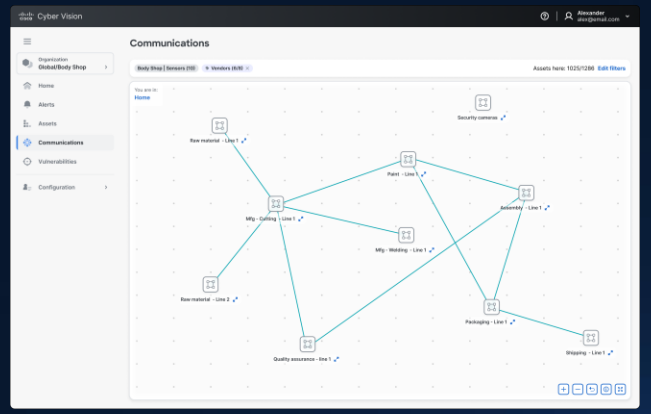
Cyber Vision AI-driven auto-grouping automatically creates security zones to drive network segmentation using Firewalls or NAC

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

RADIUS

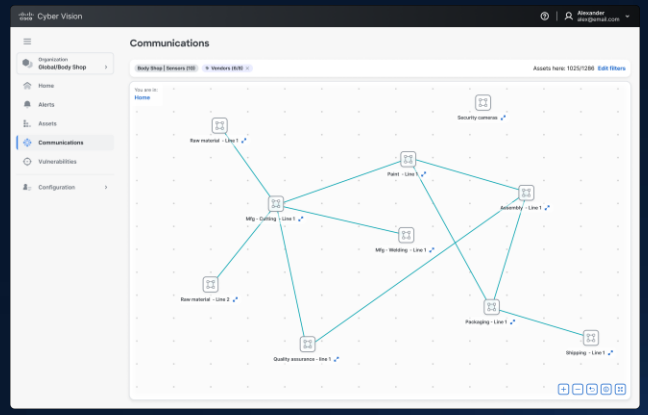
Zero downtime with OT controlled adaptive access policies

Visibility Driven Perimeter Defense With Secure Firewall

Grouping assets
in Cyber Vision

Drives TrustSec
Auth policy in ISE

Segmentation enforced by
switches and routers

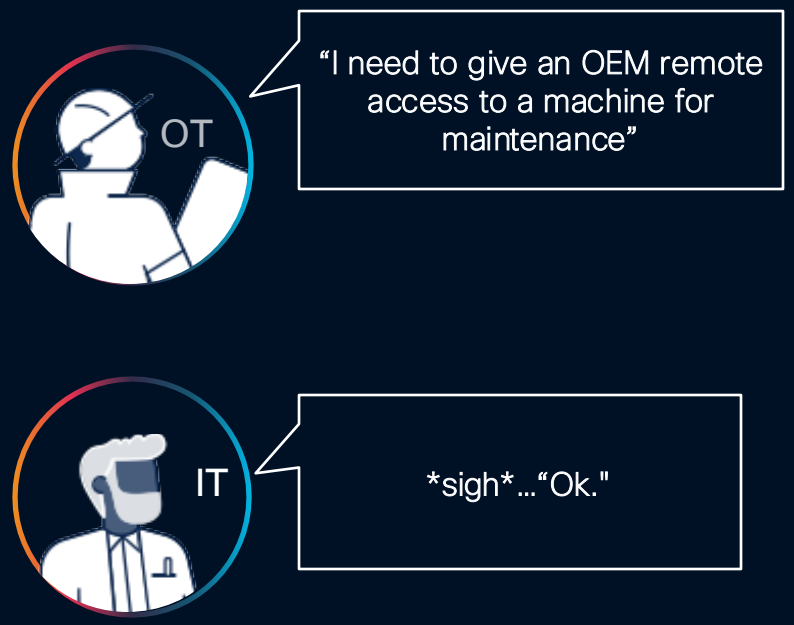


PxGrid

RADIUS

Zero downtime with OT controlled adaptive firewall rules

“Secure” Remote Access Typically Means User Frustration With Cumbersome Experiences



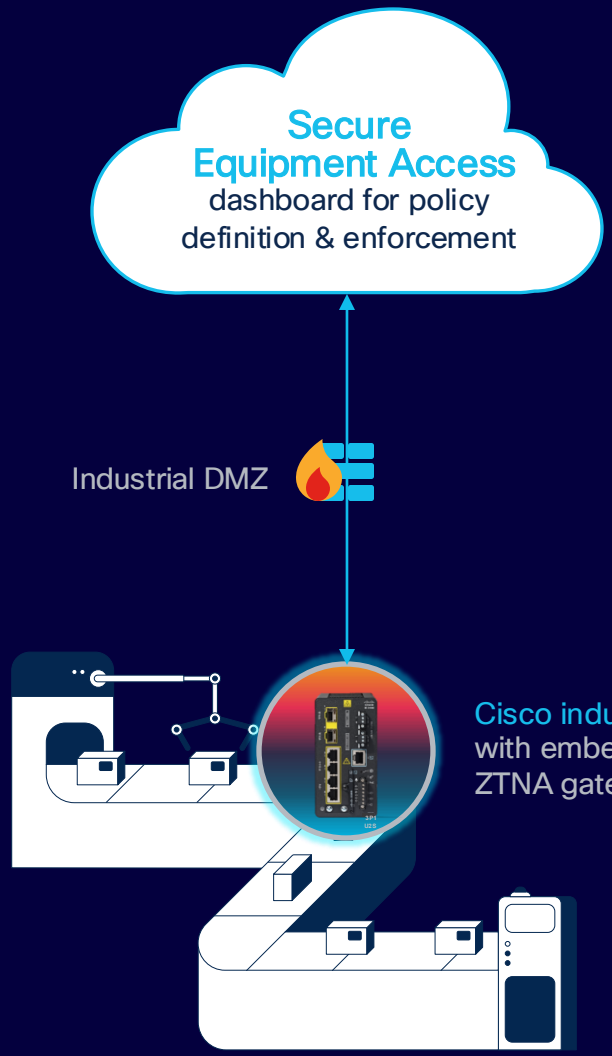
- **Add user account to the VPN**
- MFA is an optional add-on!
- Create policies for VPN user so they cannot access network
- Give user credentials to the jump server
- Add network policies to jump server to stop lateral movement
- Setup WebEx call so I can watch remotely
- Remember to close all policies when session is over

How long does it take you to grant remote access?

Secure Equipment Access

OT self service based on IT defined zero trust remote access

- MFA, SSO, and remote user identity threat detection
- Remote users only see assets you expose to them
- Grant access on-demand or within a scheduled window
- Credentials can be hidden from remote users
- Session recording, monitoring, and kill
- Clientless & Agent-based Access
- Cisco AI assistant for audit trail forensics
- No dedicated hardware required



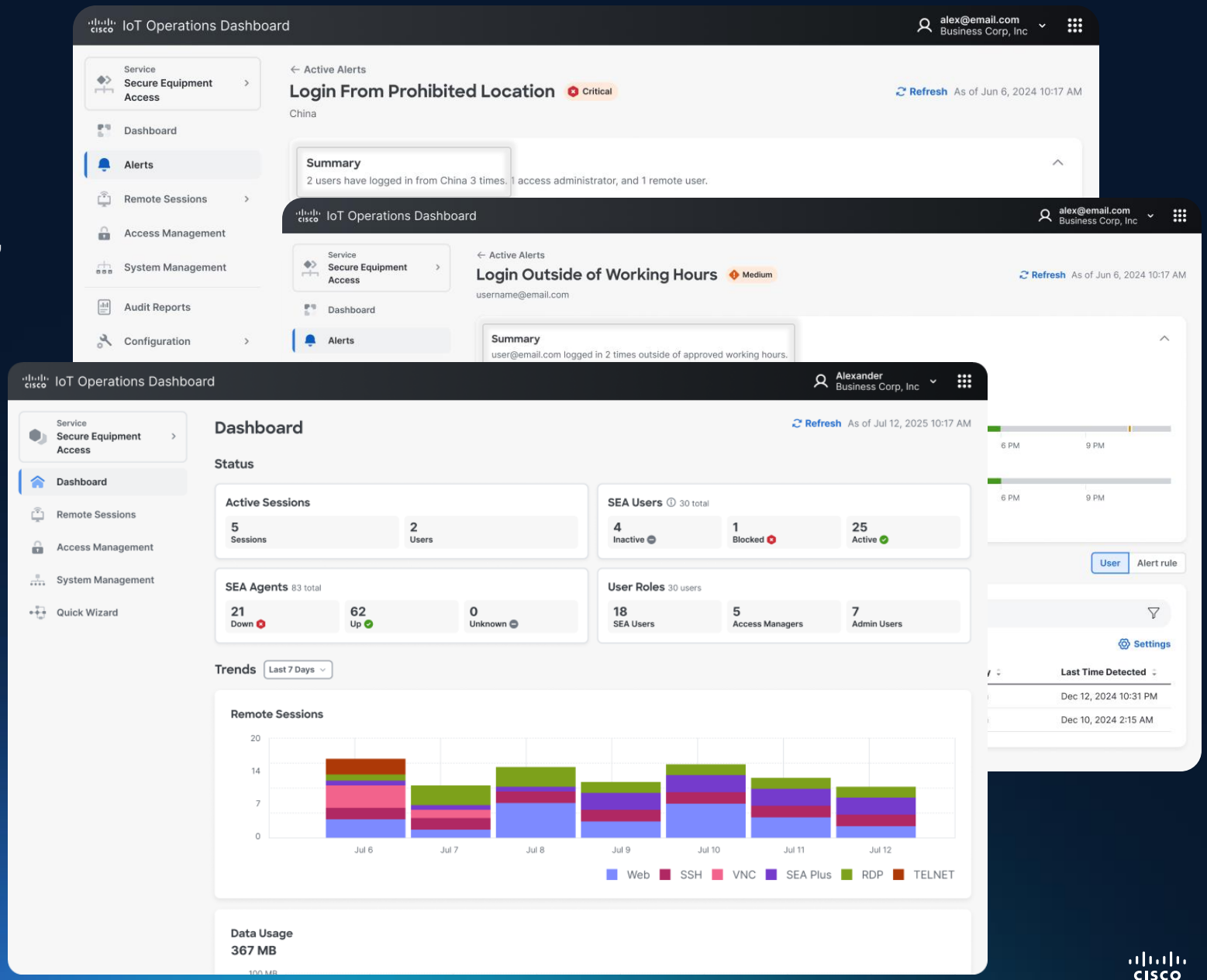
One-click zero trust remote access to any OT asset connected to Cisco industrial network

Remote User Identity Threat Detection

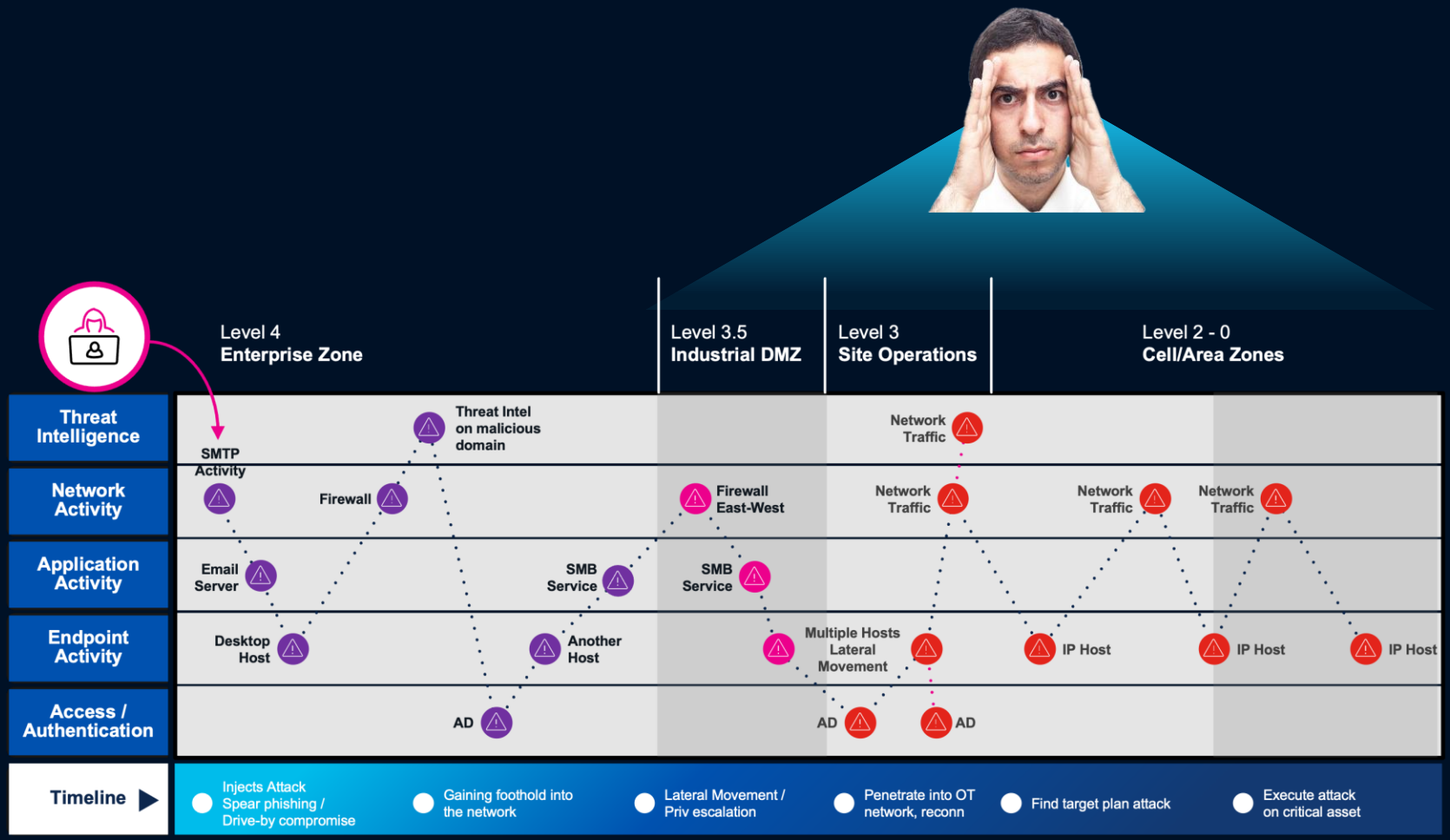
With the rise in remote access activities, remote user identity is becoming a significant attack vector in OT networks

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



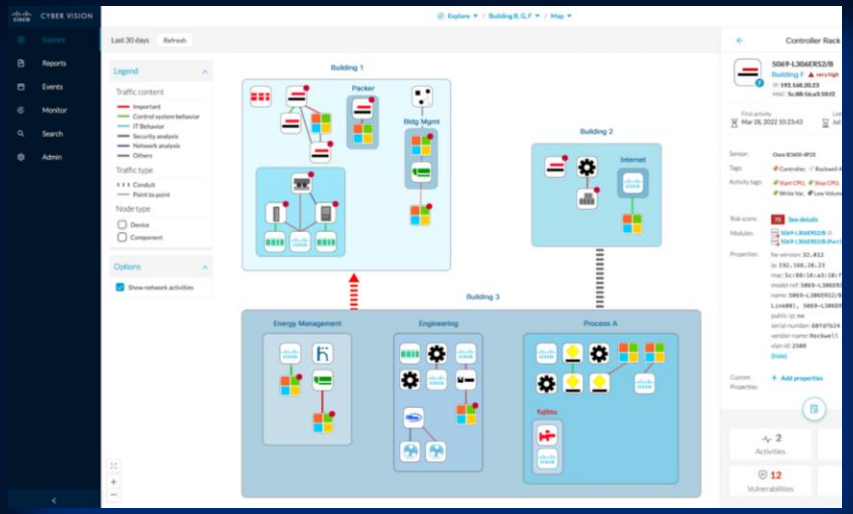
A Siloed Approach Is Not Enough to Secure OT



- With digitization, OT, IT, and Cloud domains are getting increasingly interconnected
- When an industrial company is attacked, it is almost always via corporate tech, e.g. through a phishing email
- Central visibility across interconnected domains is key to detecting and stopping threats

Getting Visibility to OT in the SOC

Cyber Vision



Cyber Vision
Add On for Splunk

Splunk OT Security

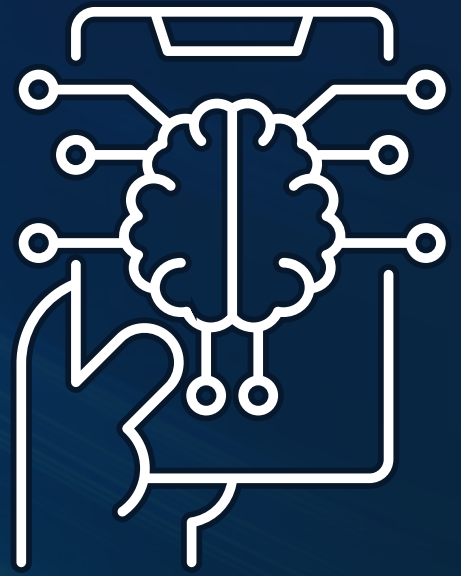
Visibility across the entire attach chain

Splunk OT Security

Detect and remediate threats across IT & OT

- Unified IT/OT security events management
- OT Asset Investigator
- OT Baselining
- Perimeter Monitoring
- Risk Based Alerting
- MITRE ATT&CK ICS correlation rules
- NERC-CIP compliance reports

Secure Devices Purpose-Built for AI



Announcing 19 New Switches Joining Cisco's Leading Portfolio

DIN-rail Portfolio

Cisco IE3100 - Compact

NEW!

4PPoE

Cisco IE3200

Cisco IE3300

Cisco IE3400

NEW!

Cisco IE3500

IP67 Portfolio

NEW!

Cisco IE3100H - Compact

Cisco IE3400H

NEW!

Cisco IE3500H

Rackmount Portfolio

Cisco IE9300 – All Copper

Cisco IE9300 – All Fiber

NEW!

Cisco IE9300 – Mixed Ports

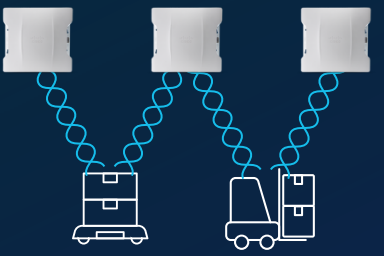
Unified Wi-Fi and URWB Infrastructure

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 CURWB Technology

cisco

Thank you